

R&M Data Center

Handbook



Version 5.0



Convincing cabling solutions

R&M Data Center

Handbook

Preface

Reichle & De-Massari AG (R&M), a manufacturer of high-quality cabling systems for data centers and data networks, presents this handbook as an up-to-date guide for all individuals involved in data center operations – including IT planners, installers, operators as well as employees. The purpose of this handbook is to impart users with the fundamental knowledge required in planning, constructing and operating data centers and to help users identify the numerous challenges encountered in those areas. It is based on the latest version of the relevant standards (as of August 2013), the technical principles involved in implementing 10 Gigabit Ethernet systems and R&M's experience in bringing a number of data center projects to success.

Data centers today are of vital importance in running companies and markets. Regardless of their size, high availability and peak performance are a basic data center requirement, 7 days a week, 365 days a year. High-quality equipment alone is not enough to ensure trouble-free operation. Merely replacing existing components by ones that provide higher performance is also an inadequate solution. Of much greater importance is to carefully determine requirements and provide efficient solutions through an integrated, forward-looking planning process that is based on detailed analyses. A key factor to consider in planning is that data cabling equipment forms the foundation of all communication channels. Planners must therefore devote special attention to the passive infrastructure.

These days, a secure, reliable data center which runs efficiently represents a decided competitive advantage to a company. In addition to fulfilling a company's specific requirements, data center operations are becoming increasingly required to comply with international rules of law as well as regulations on security. Service regulations are also essential for running a data center in an orderly manner. This handbook is designed to provide important information in these areas as well. It will impart its readers with essential knowledge and help them identify the interconnections that exist among the multitude of challenges in the data center.

1.	Introduction to Data Centers	7
1.1	Definition	7
1.2	General Information	7
1.3	Standards and Norms	10
1.4	Availability	10
1.5	Market Segmentation	11
1.6	Cabling Systems	11
1.7	Cabling Management	14
1.8	Network Hardware	14
1.9	Data Center Energy Consumption	14
1.10	The Path to Energy Efficiency	15
1.11	Green IT	17
1.12	Operational Safety and Risk Prevention	18
2.	Planning and Design	23
2.1	Data Center Types	23
2.1.1	Business Models and Services	23
2.1.2	Typology	24
2.1.3	Number and Equipment	25
2.2	Classes (Downtimes and Redundancy)	26
2.2.1	Tier I – IV	26
2.2.2	Classification Impact on Communications Cabling	27
2.3	Governance, Risk Management & Compliance	30
2.3.1	IT Governance	30
2.3.2	IT Risk Management	31
2.3.3	IT Compliance	31
2.3.4	Standards, Norms and Regulations	32
2.3.5	Certifications and Audits	37
2.3.6	Potential risks	38
2.4	Customer Expectations	41
2.4.1	In-House and Outsourced Data Centers	44
2.5	Aspects in Planning a Data Center	46
2.5.1	External Planning Support	46
2.5.2	Further Considerations for Planning	47

3.	Data Center Infrastructure	48
3.1	Standards for Data Centers	48
3.1.1	Overview of Relevant Standards	48
3.1.2	ISO/IEC 24764	50
3.1.3	EN 50173-5	52
3.1.4	EN 50600	53
3.1.5	TIA-942-A	54
3.2	Laying Out Data Centers	55
3.2.1	International Standards	55
3.2.2	Room Concepts	57
3.2.3	Security Zones	57
3.3	Network Hierarchy	59
3.3.1	Two & Three Tier Networks	59
3.3.2	Access Layer	60
3.3.3	Aggregation/Distribution Layer	60
3.3.4	Core Layer	61
3.3.5	Advantages of Hierarchical Networks	62
3.3.6	Data Center Fabrics	63
3.3.7	Software Defined Networking	64
3.4	Cabling Architecture in Data Centers	66
3.4.1	Top of Rack (ToR)	66
3.4.2	End of Row (EoR)	68
3.4.3	Dual End of Row	69
3.4.4	Middle of Row (MoR)	69
3.4.5	Two Row Switching	70
3.4.6	Other Modules	71
3.5	Data Center Infrastructures	75
3.5.1	Power Supply, Shielding and Grounding	75
3.5.2	Cooling, Hot and Cold Aisles	77
3.5.3	Hollow/Double Floors and Hollow Ceilings	80
3.5.4	Cable Runs and Routing	81
3.5.5	R&M <i>inteliPhy</i> – Intelligent Infrastructure Management	82
3.6	Active Components and Network Hardware	83
3.6.1	Introduction to Active Components and Network Interface Cards	83
3.6.2	IT Infrastructure Basics (Servers and Storage Systems)	84
3.6.3	Network Infrastructure Basics (NICs, Switches, Routers & Firewalls)	88
3.6.4	Connection Technology and Interfaces (SFP, SFP+, QSFP+, CFP)	90
3.6.5	Energy Requirements of Copper and Glass Fiber Interfaces	94
3.6.6	Trends in Network Technology	96

3.7	Virtualization	97
3.7.1	Server/Storage/Client Virtualization Basics	97
3.7.2	Converged Networks, Effect on Cabling	99
3.7.3	Trend toward Virtualization and Cloud Computing	100
3.8	Communication Protocols	101
3.8.1	Implementation (OSI & TCP/IP, Protocols)	101
3.8.2	Ethernet IEEE 802.3	104
3.8.3	Fiber Channel (FC)	108
3.8.4	Fiber Channel over Ethernet (FCoE)	110
3.8.5	iSCSI, InfiniBand and Remote Direct Memory Access	111
3.8.6	Protocols for Redundant Paths	116
3.8.7	Data Center Bridging	118
3.9	Transmission Media	119
3.9.1	Glass Fiber Cables (Fiber Optic)	119
3.9.2	Multi-mode, OM3 / OM4	120
3.9.3	Single-mode, OS1 / OS2	120
3.9.4	Plug Connectors for Glass Fiber Cables	121
3.9.5	Coax and Twinax Cables	126
3.9.6	Twisted Copper Cables (Twisted Pair)	126
3.9.7	Plug Connectors for Twisted Copper Cables	129
3.10	Implementations and Analyses	132
3.10.1	Connection Technology for 40/100 Gigabit Ethernet (MPO / MTP®)	133
3.10.2	Migration Path to 40/100 Gigabit Ethernet	138
3.10.3	Power over Ethernet (PoE / PoEplus)	146
3.10.4	Short Links	151
3.10.5	Transmission Capacities of Class E _A and Class F _A Cabling	155
4.	Appendix	166

All the information provided in this handbook has been presented and verified to the best of our knowledge and in good faith. Neither the authors nor the publisher shall be liable for loss or damage caused directly or indirectly by the information contained in this book.

All rights reserved. Dissemination and reproduction of this publication, texts or images, or extracts thereof, for any purpose and in any form whatsoever, without the express written approval of the publisher is in breach of copyright and liable to prosecution. This includes copying, translating, use for teaching purposes or in electronic media.

This book makes use of registered trademarks, trade names and common names. The relevant regulations regarding protection apply even when these items are not indicated as such.

1. Introduction to Data Centers

According to studies by the market research firm Gartner, new IT services such as cloud computing are reaching a growing number of users. These technologies will alter the market and also determine a number of trends in the economy. By now, it has become the norm for companies to outsource projects, processes and sub-tasks to remote data centers and to obtain IT resources such as software and storage from these providers. Benefits of cost and efficiency are increasingly enticing companies to turn to the cloud for IT services. Server and storage virtualization help organizations to cut down on resources by optimizing and condensing their IT infrastructures.



However, the demands these new trends bring with them are correspondingly high. Servers and data centers must be 100% available around the clock. Downtimes and interruptions or delays in data transmission must be virtually eliminated. At the same time, production processes must be designed to save as energy as possible, to conserve the environment, the climate and raw materials. Today's higher demands even apply to the tiny in-house "service room" still maintained by many companies. Any failure of an IT system risks not only significant costs to a company, but also dissatisfaction on the part of users and customers.

1.1 Definition

Since the market uses different definitions for similar terms, we recommend you clarify exactly what a given supplier, user, planner or technical employee means or understands when a specific term is used.

The terms

data center – data processing center – computer room – server room – server cabinet – collocation center – IT room – etc.

usually describe the room designed to house and operate servers. The term campus is also used for a data center that is spread over a large customer installation.

The term data center as used in this handbook is understood to mean the building or premises in which the central computing technology and the infrastructure required for operations are housed for one or more firms or organizations. This generally consists of a separate room that has its own secure power supply and climate control system. On the basis of this definition, a distinction can be made between a data center and individual server cabinets or individual servers.

1.2 General Information

Data centers are responsible for establishing the technical and structural conditions a company requires for carrying out its business processes. They ensure reliability and security for servers and other components, protect them from external dangers and also provide the infrastructure required for operation. They also provide measures for protecting systems from unauthorized access and fire and other natural disasters. The power supply system – including an emergency power supply system – as well as the climate control system are factors crucial in ensuring reliable system operation.

A targeted planning process geared to optimizing costs and an operational concept geared to future sustainability will ensure that data centers have the ability to meet a company's demands with respect to availability. Since infrastructural requirements in general are continuing to grow, many companies are now choosing to outsource their data center services.

Suppliers of outsourced services provide data center infrastructures in which they manage the hardware as well as the system software. The advantage of outsourcing is that IT costs can be better controlled. Customers also have access to a maximum level of security as well as the latest technology. The first step in outsourcing is to migrate company systems and applications to an external data center. The outsourcing company then assumes operation of these systems and applications. The client company outsourcing services must make sure that a qualified service agreement exists.

The agreement should list the specific services to be provided and define these on some basis of concrete measurability. High operational availability and stability as well as data reliability should be priorities when selecting an outsourcing provider.

The data center must of course also be able to provide expert support for the applications required by the client company as well as the required server types and classes. Note here that due to the rising number of real-time applications, the wide range of server variants is also increasing.

The service provided by a server, or the software that makes this service available:



- May run with other services on the same server;
- May be executed by a separate server computer, or even
- May be distributed over multiple servers.

This last operational model is often found in public web servers, since they frequently need to process an extremely high amount of data traffic. These servers make use of load balancing systems which automatically distribute requests over a number of physical servers.

In general, server services can be divided into the following types:

File Server

A file server makes its directories available to other computers. This allows users to send files to other users or to jointly use the same files. The services provided by file servers are transparent, and their directories are presented to the user just like the directories on the user's own workplace computer. This makes it all the more important for the file server to provide a precise system for managing access rights so that users only see the files they want to see.

Print Server

Print servers provide users access to one or more printers. Print server administration mainly involves providing individual work stations with access to the correct printer drivers for their operating system so that they can use printers without having to install drivers locally themselves.

Mail Server

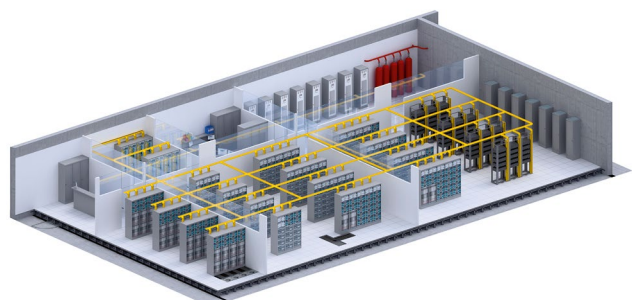
Mail servers handle e-mail communication. These systems may be installed with an Internet provider in the cloud, or even in the local network of a company. An internal company mail server can be advantageous because it provides employees with the ability to communicate with one another via e-mail. It is also useful when access to the Internet needs to be restricted for security reasons. A workstation computer is often not permitted to communicate with an external mail server at all.

Webserver

The primary function of a web server (HTTP server) is to deliver web pages from a network to clients upon request. The network in this case is usually the public Internet (World Wide Web). This form of information transfer is also used in local company networks (intranet). Browser programs allow users to access web pages as well as the hyperlinks contained in them, which are links to other web pages and documents.

Network Structures and Availability

Designing a network so that it is redundant greatly increases its availability. Redundancy means that multiple network connections are used to link together server systems and storage systems as well as network components. In case one system fails, this configuration ensures that an interface, or connection, will remain between each component so that data between components can still be exchanged.



Classifications have been defined to describe the level of reliability provided by data centers. These classifications are discussed in greater detail in section 2.2.

Connection of Remote Users

Many companies in the process of extending their local networks also choose to provide connections for remote users. These users are permitted to access company resources either from a remote company location or mobile from their home office. A virtual private network (VPN), a so-called site-to-site or site-to-end scenario, is generally used for this purpose.

VPN Connections

Since users require fast, secure access to systems, VPN connections must be routed through an automatically created VPN tunnel. It must therefore be possible to prioritize these packets with respect to the other traffic on the system. These requirements can be met through the use of high-end routers. Redundancy can be implemented for these systems as well to increase reliability.

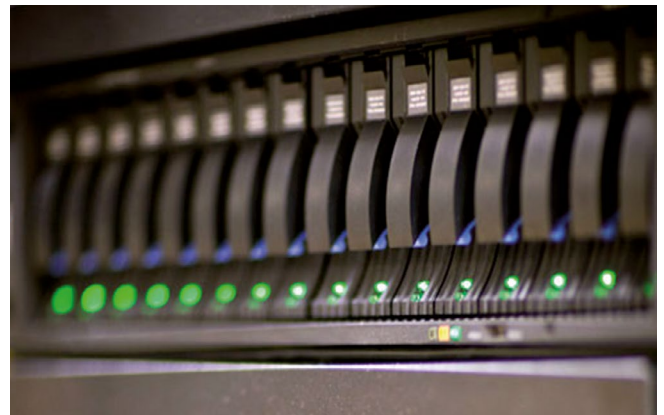
Storage Architectures

Storage servers are normally equipped with a defined number of local hard disk drives (direct attached storage/DAS). Since modern servers with multiple RAID controllers (redundant array of independent disks) can effectively control several dozen disks, even a large number of disks pose no technical problems for these systems.

A current trend towards storage consolidation in data centers is leading to the creation of storage networks (storage area network/SAN). These systems contain one or more storage systems onto which servers store all data.

Storage-consolidated environments provide the following advantages:

- Easier administration
- Higher availability
- Extended functions



SAN, NAS, iSCSI

The following technologies enable access to central storage resources:

- **SAN:** Storage area network, a general term that stands for all forms of storage networks, regardless of technology, and is synonymous with Fiber Channel SAN. Fiber Channel is currently the most widely used technology for storage networking. This technology is discussed in greater detail in section 3.8.3.
- **NAS:** Network attached storage is a file server storage system that is connected directly to an existing LAN. Since file shares cannot support block level access (these are exclusively allocated storage areas), database files may not be stored there.
- **iSCSI:** The Internet Small Computer System Interface makes block level access possible over storage resources available in the network. Since professional NAS systems support iSCSI access, the storage areas of these systems can also be used by database servers. This process can be carried out server-side using conventional network interface cards. Section 3.8.5 covers this technology in greater detail.

1.3 Standards and Norms

Recognized standards (US standard TIA-942-A, international standard ISO/IEC 24764, European standard EN 50173-5) have been established that standardize the basic data center infrastructure. These standards include classifications of data centers on the basis of different availability classes as well as cabling variants, 19" technologies, power supply, climate control, earthing etc.

A detailed comparison of the different standards is provided in section 3.1.

1.4 Availability

The general dependence on digital systems as well as their complexity and computing power have increased to such an extent that continuous availability of IT equipment and services is indispensable for most business processes. Equipment failures that only last a few hours already have dramatic consequences for organizations, and the failure of a key IT system that lasts for several days can actually threaten the existence of a company. Data center availability can be divided into 4 classes:

Tier	Introduction	Explanation
Tier I	1960s	Single power supply path, single cooling supply system, no redundant components, 99.671 % availability
Tier II	1970s	Single power supply path, single cooling supply system, redundant components, 99.749 % availability
Tier III	End of 1980s	Multiple power and cooling distribution paths but only one active redundant component, concurrently maintainable, 99.982% availability
Tier IV	1994	Multiple active power and cooling distribution paths, redundant components, fault-tolerant, 99.995 % availability

Source: US Uptime Institute: Industry Standards Tier Classification

Data center reliability, or availability, is a crucial focal point for companies whose goal is to provide reliable operation. And as every company has different requirements, reliable operation itself is a concept which each company must specifically define for themselves. Development, enhancement and regular review of IT system concepts are required in order to precisely shape and dimension the capacity a company requires, and in turn the safety requirements which will dictate the maximum IT downtimes a company can tolerate. See the overview in section 2.1.2 for more details on classifications, including those from the Uptime Institute, BSI, BITKOM etc.

Growing requirements of availability also require that the ambient conditions and supply of resources required by a data center are continuously maintained. Redundancy concepts must therefore also be provided for climate control systems and power supply systems, such as a double power feed and uninterruptible maintenance systems.

Factors that influence planning do not only include designing technical components to meet required availability goals, but also a thorough risk analysis. Selection of the location of a data center is also essential so that risk factors such as accidents due to air traffic, floods and conflicts as well as neighboring risk factors such as gas stations or chemical storage plants can be avoided. Attention must also be paid to internal, human-based risk factors (resulting from employees, visitors, service providers, etc.).

Availability concepts do not only involve the technical solution, but also the organizational structure. For example, data center operators must provide trained service personnel as well as replacement parts and maintenance contracts. Proper conduct in the event of system faults or emergencies must be announced and practiced.

The term "availability" therefore denotes the probability that a system is functioning as planned at any given point in time.

1.5 Market Segmentation

Without a doubt, the data center market can be described as extremely large and many-sided. Market researchers agree that the demand for services provided by data centers continues to grow. R&M has repeatedly made note of these impressive developments in its customer magazine Connections.

Google provides a good example of what data centers must provide in terms of performance: With over a billion search queries each day, Google is the world's most-visited website. The corporation must operate 13 data centers so it can respond to these search requests, and in less than a second. According to estimates, Google owns approximately 1 million of the world's 33 million computer servers. By comparison, confirmed reports indicate large company combines such as Microsoft, Intel, Amazon and HP/EDS each operate 100,000 to 380,000 servers located in stationary data centers. The largest of these data centers are located primarily in North America, Europe and Asia.

In addition, a subtly differentiated market exists for small and mid-sized data centers which are operated by companies themselves or by professional providers of IT services and other services. The data center market also offers modular container systems. Well-known international company groups also make ready use of these variants for their projects. Other names for these data center types include:

Modular container-sized data center – scalable modular data center (SMDC) – modular data center (MDC) – cube – black box – portable modular data center (PMDC) – ultra-modular data center – data center-in-a-box – plug-and-play data center – performance-optimized data center – etc.

The segmentation of data centers in Germany is shown below as an example to illustrate typical orders of magnitude: The German Federal Environment Agency has recorded the following size classes:

Data center type	Server-rack	Server-room	Small center	Medium center	Large center	Total
Total installed Servers	160,000	340,000	260,000	220,000	300,000	1,280,000
Percentage of server clusters over Total number of servers	12.5 %	26.6 %	20.3 %	17.2 %	23.4 %	100 %
Number of data centers	33,000	18,000	1,750	370	50	53,170
Percentage of total number of data centers	62.0 %	33.9 %	3.3 %	0.7 %	0.1 %	100 %

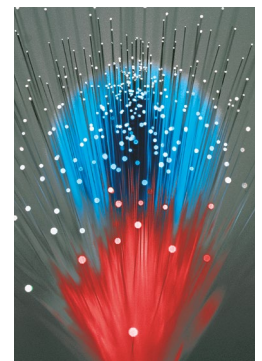
Data Center Inventory in Germany, as of November 2010

See section 2.1.2. for additional data center types.

1.6 Cabling Systems

Communications cabling of vital importance to availability. Data exchange would not be possible at all without the passive infrastructure (layer 1). IT applications, servers, switches, routers and storage media all communicate via cabling. The quality of the materials used for cabling and the systems design of each network component play an important part in planning, expanding and re-organizing data centers. These components must maintain high standards which include:

- High channel densities
- High, error-free transmission speeds
- Consistent software distribution
- Hot-swappable hardware changes
- Ventilation requirements
- Customer-friendly support



Data center planners and operators must use prudence and foresight when structuring and planning their communications cabling systems. This is because passive infrastructures must also meet typical auditing and compliance requirements in accordance with the relevant principles established by bodies of rules and monitoring bodies. Worthy of note are (based on a list provided by Compliance magazine) the Sarbanes-Oxley Act (SOX), Basel II, HIPAA, NERC and PCI DSS. Aligning the infrastructure as closely as possible with business and operational requirements (validation) is also a key consideration when designing data center capabilities to meet current as well as future needs. This means determining the business requirements of operators and of users to see what services and what level of availability must be eventually provided.

Selection

Rising data transmission rates along with extremely high requirements of availability are causing data centers to in turn make extremely high demands of quality on cabling components. An emphasis on quality pays off in the selection of systems and a full-cost analysis when the following aspects and criteria are taken into consideration:

- Cable design
- Bandwidths
- Insertion loss and return loss budgets for fiber optic systems
- EMC immunity for copper systems
- Ability of system to migrate to next higher speed classes
- 19" cabinet design and cable management

Cabling units may also be ordered pre-assembled and ready for operation. These systems make it possible to implement "plug and play" installations. In the view of R&M, pre-assembled solutions offer the following advantages: Reproducible quality, controlled quality, best transmission characteristics, high operational reliability, transparent documentation and simple logistics.

Shielded systems are the best choice when copper is selected as a transmission medium, since they – depending on physical conditions – better fulfill high demands of availability and interference resistance. Class EA copper cabling is the minimum requirement for data centers. Criteria when selecting suppliers include: Product quality, reliability, experience, competence and sustainability.

Structure

It is recommended that a cabling infrastructure be designed so that it is clearly laid out, transparent, and decoupled from the current architecture. This avoids the need to modify the cabling system every time a device is added or replaced. Ideally, the infrastructure should connect given equipment locations together by means of a uniform, consistent structure. Such a structure will allow the data center arrangement to grow with future requirements.

Data center layouts and cabling architectures are discussed in sections 3.2 and 3.4 respectively

Security and Redundancy

Data center infrastructures are normally designed to be redundant so as to ensure availability and interruption-free operation, e.g. when hardware needs to be replaced or when a cable link fails. In R&M's experience, a cabling platform that is modular, congruent and designed in a uniform manner fulfills this requirement better than other solutions. Such a system can consistently ensure, for example, that bending radii are maintained and the required performance delivered. Such a system also allows for reliable installation of components during continuous operation and also offers a few other advantages.

Cabling systems that are pre-assembled at the factory can contribute to increasing availability. This is because using pre-assembled units reduces the time spent by installation personnel in the security area of the data center. This in turn reduces potential malfunctions and increases operational safety. In addition, data centers must ensure that all products meet general as well as customer-specific requirements in terms of quality. Such compliance must be reviewed and documented in a quality management system.

The redundancy principle also applies to systems outside a local computer room. Connections from one data center to another (i.e. between redundant data centers or backup data centers) as well as connections to a basic data backup system at a different location must be designed in a redundant manner. The same applies for connections to MAN and WAN provider networks.

Installation and Quality Assurance

Only those technicians who have specialized training and knowledge in cabling system specifications should be used for cable installations and patching. Manufacturers like R&M are based on a comprehensive system of quality assurance throughout the entire value chain – from the manufacturing of components, through professional installation and implementation up to professional maintenance of the cabling system.

The use of modular, factory-assembled cabling systems is also advantageous when it comes to installation. Such designs save time, and in turn costs, when cabling systems are set up. Pre-assembled solutions allow passive infrastructures to be adapted more quickly during migrations and also when capacity is increased or hardware is upgraded.



Regardless of the data center performance you desire or require, we recommend implementing a system solution that consists of a distribution cabinet system and cable management system based on the typical 19-inch format. Depending on the application requirements, cabinet systems that are 600 mm or at least 800 mm wide should be used, as closed systems or open frame system, in lightweight construction or a robust design. These systems allow for installation of a uniform cable management system in the vertical and horizontal direction. Cabinet depth is determined by the passive and active components to be installed. A cabinet depth of 1000 mm to 1200 mm is recommended for the installation of active components.

A modular server cabinet provides appropriate security characteristics at reasonable costs. It can also be dismantled or modified if necessary and used at a different location. Finally, it is also suitable for expansions that implement new housing solutions or climate control concepts.

Modern high-performance server systems and storage solutions with high packing densities as well as self-contained power supplies require a high degree of stability from server racks. These racks must exhibit capacity loads of up to 1,000 kg. Cabinet floors and sliding rails must therefore also be designed to meet these high loads.

Cable entries are an important consideration as well. It is very useful when the installation and maintenance side ensures reliable bending radii and allows easy access to all cable bundles. Power and data cables in copper cabling systems must be routed separately from one another in order to minimize interference between the two.

Increasing server performances and higher packing densities in racks require sophisticated ventilation designs that will ensure the heat produced by these devices will be drawn off. Appropriate solutions include perforated doors and partitions between the warm and cold areas in racks, as well as contained cold aisles and hot aisles.

Documentation and Labeling

An accompanying system of documentation provided for managing the cabling system will ensure planning of conversions or expansions will run smoothly. A number of tools are available for creating and maintaining such documentation – from standalone Excel lists up to software-based documentation tools like R&M *IntelPhy*. When all is said and done, it is absolutely essential that this documentation system be kept up-to-date and it reflects the cabling that is actually installed at any given point in time.

One essential component contributing in a living, breathing document management system is cable labeling; this should be unambiguous and easy to read even when lighting conditions are poor. Manufacturers offer a number of identification systems in this area as well, including labels that contains bar codes. Maintaining one uniform naming convention that is consistent throughout the company is critical. A responsibility-based system for managing this documentation must also be provided for purposes of quality assurance.

1.7 Cabling Management

Precise plans for laying data cables and energy cables must already be completed well before cable systems are actually installed or migrated. Locations where cables are to be laid must be precisely documented so that future changes in concept or new requirements can be accommodated quickly.

Cables must be laid properly, in cable trays or cable runs. Laying cable in double floors brings certain advantages, since this results in fewer obstacles when computer rooms are renovated or maintenance work is carried out. Further information on cable installation appears in sections 3.5.3. and 3.5.4.

Cable penetration seals are one weak area in this regard. As these components must fulfill all requirements of safety (fire/gas/water protection), they must also be designed to be appropriately durable. At the same time, however, they must be flexible enough to accommodate upgrades and changes in cable installation.

1.8 Network Hardware

Modern data centers must contend with the trend towards virtualization, and thus require that special attention be placed on themes involving networking. The virtualization of servers and storage systems continues to spread rapidly. Client/server concepts are increasingly made available through cloud computing solutions. Business processes are being run more and more frequently over data links which also have the ability to supply energy to terminal devices via technologies like Power over Ethernet (PoE). Along with the increasing importance of network technology in ensuring uninterrupted business operations, security requirements are growing in this area too.

Network technology falls back on requirements that are comparable to those demanded by servers:

- The rack as a framework for the infrastructure,
- Network cabinets on the same platform, since active components must also be standardized to 19 inches
- Comparable requirements also prevail with regard to stability, fire protection and access control.

Network cabinets may be seen as a long-term investment, similar to the network infrastructure installed in buildings that is generally designed to last for at least 10 years. By contrast, accessories must focus on flexibility so that they have the ability to easily accommodate future developments in technology.

One consequence of the frequent switchovers that occur at network component connection points (ports) is that new cables need to be installed more frequently in network cabinets than in server cabinets. Allowing cables to be easily inserted into roof sheets and base make upgrades easier and also provides for short cable runs. Cable ducts and guiding plates ensure clean, fine distribution in the rack. This process, just in terms of cable management, requires a particular focus on component stability. The minimal bending radii of cables must also be considered here.

Since network cabinets continue to generate more and more waste heat, climate control is another factor which is rapidly gaining in importance in this area. Options for expanding climate control systems should already be planned on even before network cabinets are installed. Typical solutions include passive cooling via roof panels, venting devices, double-walled housings over ventilators, roof cooling units and cooling units between racks.

Further information on network hardware and virtualization can be found in sections 3.6 and 3.7. respectively.

1.9 Data Center Energy Consumption



The dramatic increase in the data volume and IT service demands placed on data centers naturally translates into an increase in their energy requirements. According to predictions by the environmental organization Greenpeace, the annual power consumption of all data centers in the world will triple within ten years, to a figure of 1,963 kilowatt hours by 2020.

According to a study by the market research firm Gartner, data centers will reach their limits with respect to energy consumption and space requirements in the next three years. The result will be a further consolidation of performance. This, however, will only further increase the power requirements for operation and cooling.

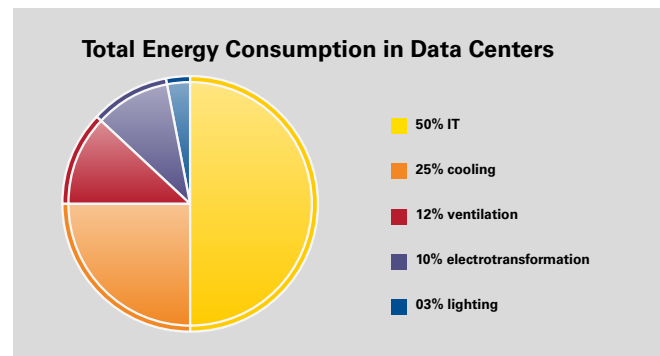
These high power consumption forecasts are primarily for existing data centers that use obsolete technologies. As much as 70% of the energy consumed by these data centers is output just for cooling purposes

Processors typically show energy consumption on the level of 140 watts, with that of servers at approx. 500 watts and blade servers approx. 6,300 watts. Each watt of computing power can require cooling power of up to 1 watt. The power consumed by supply technology and energy technology is a factor as well. The following table provides an overview of sample values. The conclusion: A savings of 1 watt in IT power consumption translates into an overall power savings of 3 watts.

Energy consumption at server level	1.00 watt
DC/DC conversion	+ 0.18 watt
AC/DC conversion	+ 0.31 watt
Power distribution	+ 0.04 watt
Uninterruptible power supply	+ 0.14 watt
Cooling	+ 1.07 Watt
Switchgear for power distribution	+ 0.10 watt
Total energy consumption	2.84 watts

This remarkable trend can also be comprehended by examining average power consumption per server cabinet. This value was at 1.7 kW in 2003, rose to 6.0 kW by 2006 and was 8.0 kW in 2008. By now, server cabinets at full capacity consume approximately 15 kW, and even 20 kW for cabinets which house blade servers.

The graphic to the right demonstrates how the total data center energy consumption is distributed over the various areas of the center.



Source: EYP Mission Critical Facilities Inc., NY

1.10 The Path to Energy Efficiency

It is safe to conclude from the previous section that data centers today must focus on energy efficiency so they can produce in a more sustained manner. In other words, green IT is the order of the day. Energy-efficient operation can be best achieved by starting at the very beginning of the chain of cause and effect. This chain starts with applications, continues with IT hardware and ends with systems for power supply and cooling. Applications and servers that are no longer required should be switched off whenever possible. This will reduce losses in the uninterruptible power supply as well as cooling load.

Becoming More Efficient through Virtualization

From a technological point of view, virtualization is a highly effective tool for running a cost-efficient, green computing solution. Expanded server farms can thus be made smaller, by transferring physical servers onto virtual machines. In spite of this, server utilization can still be increased. Because this approach is so effective, some energy suppliers are already offering corresponding discounts.

Virtualization allows for power savings to be increased threefold or even fivefold. Even further savings can be achieved if modern multi-processor systems are also used for consolidation.

Saving on Cooling



Among the greatest challenges faced by a data center are its cooling requirements. The continuous rise in processor performance is resulting in a growing demand for energy, which in turn is leading to higher and higher cooling loads. One essential task involved in cooling is segmenting and delimiting off different sections of data centers. Climate control for these sections can then be provided more efficiently, depending upon the heat generation involved.

Only an integrated overall concept which brings performance requirements of power, availability and operational reliability in line with energy-efficient utilization of hardware can lead to data center operation that is economically efficient. We must point out the possibility of re-using waste heat via heat exchangers or block heating and generating plants. Operational efficiency can be improved even further through such measures.

In terms of functionality and energy efficiency, water cooling and liquid cooling systems are greatly preferable to thermal cooling systems. Due to the construction of hot aisles and cold aisles, these latter systems show significantly higher space and volume requirements. Liquid cooling is 3,000 times more efficient than air cooling. Cooling is further discussed in section 3.5.2.

Key Efficiency Benchmarks



A number of approaches can be used to quantitatively measure the efficiency achieved in data centers. The approach established by the Green Grid organization uses two key indicators:

- Power Usage Efficiency (PUE) determines the efficiency of energy use as calculated from the total energy used and the power of IT devices
- Datacenter Infrastructure Efficiency (DCIE) evaluates the efficiency of the energy used and determined in the data center. It is calculated from the quotient of energy of IT devices to the total energy in the data center.

The DCIE value is the reciprocal value of the PUE. The DCIE thus equals $1/PUE$ and is expressed as a percentage. The table below shows how these performance indicators are assessed:

PUE	DCIE	Level of efficiency
3.0	33%	Extremely inefficient
2.5	40%	Inefficient
2.0	50%	Average
1.5	67%	Average
1.2	83%	Extremely efficient

If an IT department uses only a third of its energy requirements, this would translate into a DCIE value of 30%, which corresponds to a PUE value of 3.3. The more closely the PUE value approaches the number 1, the more efficiently the data center will operate.

The following items are included in the total energy balance:

- Energy for switchgear
- Uninterruptible power supply (UPS)
- Batteries
- Cooling
- Air conditioning system
- IT devices such as computers, storage systems, communications devices and peripherals.

In addition to this, the industry association called The Green Grid introduced two new performance indicators at the beginning of the first quarter of 2011, geared to providing guidance to IT departments and data centers:

- Carbon Usage Effectiveness (CUE) describes the amount of greenhouse gas emissions generated from the IT gear in a data center facility.
- Water Usage Effectiveness (WUE) describes the amount of water required to operate an IT installation.

Helpful Initiatives



Initiatives and associations in industry and research as well as lawmakers around the world are making great efforts to improve energy efficiency in the IT industry and its data centers. The Green Grid is an American industry association of suppliers of supercomputers and chips, dedicated to the concept of environment-friendly IT, also called green IT. This consortium was founded by AMD, APC, Cisco, Dell, Hewlett Packard, IBM, Microsoft, Silicon Graphics International (formerly Rackable Systems), Sun Microsystems and VMware. The Green Grid develops standards (IEEE P802.3az Energy Efficient Energy Task Force), and measuring systems and processes to lower energy consumption in data centers.

The European Code of Conduct (COC) on Data Centres Energy Efficiency was introduced by the European Commission in November 2008 with a similar goal, to curb excessive energy consumption in data center environments. The code comprises a series of voluntary guidelines, recommendations and examples for improving energy efficiency. Data centers and equipment suppliers implementing an improvement program recognized by the EU Commission may use the code's logo. Quantitative minimum requirements will also be defined over the medium term. R&M takes part in this program as an endorser.

The SPEC Server Benchmark Test of the U.S. American Standard Performance Evaluation Corporation (SPEC) is also of importance in this area. The association sponsors IT manufacturer efficiency competitions in which companies are encouraged to construct and test configurations that provide maximum efficiency.

1.11 Green IT



Green IT is a general term that encompasses a variety of approaches for conserving energy and raw materials in the IT industry. The concept centers on reducing operational costs while at the same time enhancing computing performance and identifying measurable, short-term results. Data center efficiency is a top priority in these considerations.

With power costs rising significantly over the past few years, business and industrial sectors have been paying increasing attention to obtaining their computing power needs from "green" IT sources. This also translates into birth of a new type of market demand.

Along with the automotive and real estate industries, information and communication technologies and sectors (ICT) are one of the key starting points for the improvement of climate protection. According to a study¹⁾ by the Gartner group, ICT accounts for 2 to 2.5 percent of global CO₂ emissions, about the same as the aviation industry. A quarter of these emissions originate from data centers. In office buildings, IT equipment often consumes over 20 percent, in some offices over 70 percent, of the total energy used.

However, in addition to the measures described above, green IT also involves evaluation of the materials and means of production used in manufacturing and in using hardware. In particular, this involves materials which may harm humans and the environment if improperly used, if used continuously, if used during natural disasters or when disposed. The RoHS guideline of the UE (Restriction of Hazardous Substances) is the final word in this area. This directive should be taken into consideration when planning and evaluating data centers and also in day-to-day operations.

¹⁾ Gartner (2007) "Gartner Estimates ICT Industry Accounts for 2 Percent of Global CO₂ Emissions"

1.12 Operational Safety and Risk Prevention



Data centers have very different requirements with regard to operational safety and risk prevention than other structures. This section provides information on what areas and risk factors need to be taken into account when planning data centers. In many countries, legislation stipulates that IT systems are an integral part of corporate processes, and are therefore no longer just tools to advance a company's success, but elements that are bound by law and in themselves part of the corporate purpose. It goes without saying that security requirements must be considered as a whole and extend far beyond firewalls, virus protection and storage concepts. They include the entire building and its surroundings as well as physical risks.

Regulations such as the German Supervision and Transparency in the Area of Enterprise Act (KonTraG), the international Basel II Accord or the Sarbanes-Oxley-Act (SOX) in the United States require that a company's own IT systems are integrated virtually 100% into its main corporate processes. As a consequence, IT managers see themselves exposed to significant liability risks. Customer claims for compensation, productivity losses and the importance of IT to the corporate image are among the typical challenges companies and organizations must head off by means of security measures and preventive measures.

The first step in planning is to identify and analyze weak areas in IT structures in order to determine the actual need for IT security. Planning must also consider any potential external risks. Essential elements in security planning include information and data on room allocations, transport routes, ceiling heights, cable paths, double floors, energy supply systems and telecommunications systems. Exact specifications must be provided for all for these installations.

Security solutions can be designed gradually and in modular fashion, and should be geared to needs. Economic issues must also be taken into consideration in planning. Pragmatic solutions can be scaled flexibly and give the company the ability to grow. However, solutions should also always be kept comprehensive in order to ensure the exact protection required is in place in the event of any hazard situation.

The following hazards and risk factors may physically impair data center operations and may even bring about new challenges: Fire, smoke, dust, water, energy supply system failures, air conditioning and access control, explosions, future structural and technological changes, migration and growth, faults in maintenance and remote surveillance.

Fire



Fires generally arise outside of the IT infrastructure, e.g. in energy supply systems or air conditioning systems. Only about 20 percent of fires occur in server rooms or in their immediate vicinity. Computer rooms are provided with systems that can detect fires at a very early stage (EFD systems) as well as fire alarm and fire extinguishing systems. These systems are fully automatic and can be implemented redundantly so as to avoid false alarms.

EFD systems draw air out of the racks they protect and can detect even the tiniest particle of smoke.

These systems must exhibit an adequate level of detection sensitivity. These systems are also equipped with filters and intelligent signal processing algorithms which detect disturbance variables. Some manufacturers offer combination fire alarm systems which fit into 19" racks and take up little space.

Firefighting measures should result in as little additional damage as possible. Non-poisonous extinguishing gases allow for firefighting even at an early ignition phase. Extinguishing gas works much faster than foam, powder or water, causes no damage and leaves no residue. Typical gases used include FM-200, noble gas (e.g. argon), nitrogen, Inergen and carbon dioxide. These chemicals smother fires through an oxygen removal process. There are also extinguishing gases which put out fires by absorbing heat.

Instruments for oxygen reduction (called inertization) can be used in addition to extinguishing gases. The inertization process involves constructing an air decomposition system that splits ambient air into its individual components in order to reduce the level of oxygen in the air. Low oxygen content has a preventive effect and works to smother fires faster. Another advantage of such gases is that employees may continue to remain in the data center, since the reduction in oxygen is generally not harmful to humans.

Fire in the Data Center

In the evening of March 1, 2011, a fire broke out in the high-performance data center in Berlin. For security reasons, all servers were shut down shortly after that time and the entire space was flooded with CO₂ to smother the fire!

German Red Cross

Smoke

IT systems can be affected even if a fire occurs outside the data center. Flue gases can get into the computer room through ventilation systems and cause serious damage. For example, burning plastics such as PVC create poisonous, corrosive smoke gases. Burning one kilogram of PVC releases approx. 360 liters of hydrochloric acid gas, producing to 4500 cubic meters of smoke gas. IT personnel and equipment are in danger if this gas penetrates into the data center. The "mean time between failures" (MTBF) is lowered quite significantly. MTBF is the average predicted elapsed time between inherent failures of a system during operation.

Only hermetically sealed server rooms are protected from such dangers. EN 18095 tests should be used to ensure smoke gas resistance. IP categories are used in Switzerland and Germany. At a minimum, a data center should have IP 56 protection.

Dust

Dust particles in indoor air can get deposited onto ventilation systems and electronic components and significantly reduce their service life. Dust can enter through natural ambient air, and also while installation and maintenance work is being carried out or renovations and upgrades are being implemented in computer rooms. Dust-free conditions are among the top safety objectives when planning and operating data centers. Data centers should always meet grade 1 dust-tightness requirements in accordance with EN 60529, IP 56 (see water risk). High-quality filter systems can also minimize the penetration of dust. Dust levels should be continuously monitored.

Water



Water can penetrate into the data center through pipe leaks in the cooling system or air conditioning system, or through firefighting measures. Unfortunately, this risk factor is frequently ignored. Damage through fire is often less than that caused by the water used to extinguish it. This risk factor of water and/or liquid plays a role especially when liquid cooling systems are used in server cabinets.

Computer rooms must be sealed watertight over the entire time firefighting measures are carried out and must also be made secure from flooding. High-availability systems should be able to withstand flooding for up to 72 hours. Water tightness should be proven and independently certified to be EN 60529-compliant.

Power Supply

Ideally, uninterrupted power supply systems that are permanently operated (online UPS systems) should be used to supply IT equipment in computer rooms. Offline UPS systems that only start up in the event of a power failure require that a switchover or activation process first take place in the event an emergency occurs. This brief switchover period brings additional risk factors, including switching time delays and voltage-based component failures.



Online UPS systems supply consumers directly via their circuits. Their batteries can comfortably bridge fluctuations in the power grid as well as longer power failures. These devices provide perfect sinus voltage.

EN 50091-3 and EN 62040-3 VFI standards define classifications for UPS systems. Data centers should choose devices with the highest VFI-SS-111 quality rating of 1 in order to ensure reliable failover protection. UPS systems fall into the category of either single-phase or multi-phase 19" inserts, or stand-alone units of different performance classes. Some systems can be expanded and upgraded during operation.

Emergency power systems (EPS) must be activated in the event of data center accidents that are more severe or last for a longer period of time. These devices are self-sufficient emergency power generators that can provide data centers with all the power they require. These units are generally based on diesel engines. In some cases, these engines can also be operated as block heating and generating plants and burn fuels made of renewable raw materials (e.g. vegetable oil). This approach contributes to reducing CO2 emissions from data centers and to achieving additional revenue from power production.

Long-term planning must include considerations of whether fuel cell technologies are possible as power sources for emergency power systems. Fuel cells are expected to have a long service life and favorable total cost of ownership (TCO). Other advantages of fuel cells include shorter backup times and response times, lower sensitivity toward temperature fluctuations and climate-neutral operation.

Air Conditioning



As the performance of data centers and servers increases as described above, additional heat is inevitably generated. Cooling capacities and air conditioning systems must therefore also become more high-performance. A typical "sound barrier" exists at thermal loads of 800 W/m². Climate control devices on the ceiling or wall are generally sufficient if the actual load is less than this value. Floor-mounted air-conditioning units must be used in case higher loads are maintained. These systems blow cold air into the raised floor.

Ventilation and climate control equipment are positioned inside and outside the data center as needed, on the basis of the center's space situation and structure. Indoor cooling systems can focus on rack-based cooling or hot spot cooling. The use of liquid-cooling packages is also an option for cooling hot spots in data centers. These packages extract the hot air that is emitted along the entire length of the cabinet then discharge into a cold water network or a cooler by means of an air and water heat exchanger.

This targeted cooling system reduces operating costs. However, in return one must accept the greater noise levels that occur in the server room as well as the need for maintenance personnel to work in sensitive areas. Other advantages of an indoor cooling solution include protection from third-party access, avoiding additional breakthroughs for pipelines or sliding valves.

Risks decrease when climate control equipment can be positioned out of doors. This is because the fire load factor does not apply here. Maintenance personnel do not have to enter the computer room, saving space. The air conditioning system can be supplied directly with fresh air.

The climate control system is also subject to requirements of continuous operation. In most cases, for reasons of cost, secure redundancy as provided under tier III and IV (see section 2.2.1.) is only required for air-conditioning units on walls and ceilings that have a rather low cooling capacity. "N+1 redundancy" as defined under Tier II should be planned when higher capacities, and thus stand-alone units, are required. In this case, a specific number of units run in continuous operation while an additional unit acts as a redundancy reserve.

It is recommended that a stable relative humidity of 40% to 60% be maintained in computer rooms. As a result, the climate control equipment that is used should include humidification and dehumidification systems.

Systems certified by Eurovent, the interest group of European manufacturers of ventilation and air-conditioning systems, have proven to be reliable.

Access



Access to data centers should be strictly regulated, monitored and documented. Only authorized personnel with proper qualifications should receive access to these areas. All operations should be recorded in accordance with relevant regulations on documentation and logging. Access control must correspond to operator specifications exactly.

Protection of the data center must fulfill requirements for protection from third-party access, sabotage and espionage. One basic principle of access control is to allow only specific personnel to enter specified areas of a space, for the purpose of carrying out specifically defined tasks. Data centers can implement resistance class III (RCIII) burglary protection as defined under EN 1627 with little effort. The air conditioning system and electrical equipment can be installed separately from servers, if the area of the data center allows for this. This reduces the need for maintenance personnel to access sensitive zones.

A variety of technical solutions and security levels are available in the selection of an access control system. Biometric systems raise the level of security and can be combined with other systems such as magnetic card readers. Vein recognition technology guarantees the highest level of security. The level of precision they offer makes it easier to implement security processes. The false acceptance rate provided by these systems lies under 0.00008, with a false rejection rate of 0.01 percent. They also provide hygienic advantages, since no contact with these recording units is required.

Video surveillance systems also provide for transparency, monitoring and reliability. Thanks to modern sensor technology and the related software, up to 1,000 cameras can be managed centrally, regardless of the cameras' manufacturers. Video surveillance can also control and record alarm conditions.

Explosion

A conscientious data center planner will also take explosion risk factors into consideration. Data centers can be exposed to terrorist attacks or natural disasters that can lead to explosions in the area of the building and server rooms. If possible, high availability, or at least fast recovery, should be ensured in these situations as well. Data centers with SEAP standard certification have shown they can successfully withstand an explosion test.

Pressure-resilient wall panels should be installed in data centers that require a high level of security. These walls make it possible for the data center to withstand explosion pressure and thus provide protection for IT systems. Other measures must then be provided to protect IT systems from debris and vandalism. In short, buildings and rooms should be provided with all-around protection.

Future Viability



Potential changes in structure and technology, even when these changes are not yet foreseen, should be taken into consideration already at the planning and installation stage. This will ensure that the data center remains capable of growing with future needs. History shows, without a doubt, that such changes can occur at any time.

Product life cycles are becoming shorter and shorter, while demands on IT systems are growing higher and higher. Data center operators are often faced with the question of whether they should enlarge a data center, make it smaller or possibly even move it to a different location. These and similar issues must be taken into consideration already by the planning stage. Professional project partners support operators right from the start of a project, and continue to provide later support in day-to-day data center operations.

It is important to keep in mind that network technology will continue to undergo significant further development in the future. Highly condensed cabling systems and parallel optic connection technology will shape these developments, since the introduction of 10 gigabit Ethernet and later 40/100 gigabit Ethernet demands these infrastructures. New applications and upcoming trends like virtualization, cloud services and SaaS require network architectures that are capable of growing along with the future.

Efficiency

Data center operators expect their investments to be efficient, secure, and economically viable over the long term. At the same time, data centers must be flexible enough to grow at any time and adapt themselves to current market conditions. These issues must play a part in the selection of planners, suppliers and other project partners and also in the evaluation of components. Certification from independent testing organizations can give planners orientation in this regard. Building work should be inspected both during the construction phase and afterwards. This will provide a firm foundation for data center operations that are reliable, efficient and profitable.

Infrastructures that are scalable and modular are advantageous because they can be easily adapted to new demands. A data center designed in this way can then grow gradually and on the basis of its tasks. System migrations can be managed without complication, and investments remain manageable. This also contributes to increasing the efficiency of the data center. Planning and evaluation stages should focus on those suppliers who have a proven ability to fulfill such requirements.

Another aspect to efficiency is to search for pragmatic solutions which ensure high availability. For example, data center units can be maintained in a decentralized manner and distributed over available building and office areas. This reduces dependence on a single centralized unit and in turn the risk of a total system failure. In some cases, this concept even saves operators from having to construct a new installation.

Decentralized structures do not have to be more expensive. For example, modular security systems exist which provide efficient support for such decentralized structures. A concept of modularity makes it possible to integrate existing structures cost-effectively and without a problem. If necessary, system expansions, changes or moves can be managed without frictional losses or interruptions to operation. Similarly, security rooms or server locations can often be rented or leased, making it relatively easy and efficient to carry out short-term extensions as well.

Maintenance



Regular inspections of and maintenance to IT systems and other data center components can help to reduce risks and dangers and detect these at an early stage. In all cases, maintenance by professional, qualified technicians will reduce the likelihood of a system failure. Maintenance work should be carried out at defined intervals and should also be thoroughly documented. This work should be based on a long-term servicing concept that is implemented on a continuous basis, and not just when a system failure has just occurred.

Servicing concepts can be adapted to the specific needs of a data center operator, so that the servicing order only contains the maintenance work that is actually required, but the operator still achieves the highest possible operational safety.

Servicing concepts and service agreements must provide coverage for all areas including cabling, air conditioning, fire alarm/early fire detection system, UPS/emergency power systems, and monitoring/access control systems. Provisions in these documents should cover all tasks and requirements up to and including warranty claims.

Regulations on the type and scope of the services provided can be created on the basis of each individual data center and should be oriented to the objectives of the given company and/or data center operator. These regulations may be basic annual check-ups, or extend all the way to full technical customer service including 24/7 availability and a chain of alerts.

Remote Surveillance

Remote surveillance measures make it possible for data center operators to increase operational safety and system availability. Special monitoring programs and sensors have the ability to control all data center functions and selectively trigger alarms in the event of an emergency. They sometimes even have the ability to analyze faults immediately and transmit appropriate instructions for responding to them. Third-party personnel, e.g. security service employees, can then intervene faster and more effectively, with measures targeted to the specific fault. It is essential that an appropriate alarm sequence plan be prepared and practiced.

The alarm can be activated according to defined routines, and consist of visual and/or acoustic signals. The alarm can also be sent immediately as a text message through appropriate interfaces to operators, administrators, call centers and security services.

Not only servers, but also other data center components like fire extinguishing systems can be easily controlled from a remote location. Rescue measures can likewise be implemented and coordinated through the use of remote monitoring tools. Appropriate tools even provide the ability to continuously monitor the status of each individual plug connection or each active device in the data center's data network. Finally, visual displays are a good means for obtaining a quick overview of the status of all systems.

Integrated Approach

Planning must always be based on a comprehensive, integral examination of all operational and security requirements. Only such an approach will allow risks and dangers to be eliminated right from the very start. This planning must also include a consideration of the entire corporate structure of a company. The overall examination should also include a risk analysis which records the conditions of the building and its location, and assesses these in a completely neutral manner.

Supplier bids for data center planning, construction and equipment provision services should include the overall examination with the risk analysis as well as the resulting technical specifications or satisfactory responses to the corresponding questions. The goal in this process is to always find the optimal solution for constructing and operating a safe, secure data center that meets all needs. The process for selecting partners and suppliers and evaluating products and components should be geared to this objective as well. Preference should be given to those partners and suppliers who are qualified to provide support in all necessary areas, and who can demonstrably prove they fulfill the related quality requirements. Only such an approach will guarantee that all the risks and impact factors discussed above are taken into consideration. This will then ensure that IT structures are made secure as dictated by needs, basic conditions and the budget situation.

2. Planning and Design

Data center infrastructures require proper, professional planning that will lay the foundation for high availability, profitability and the ability of the data center to grow and meet future needs. However, the expectations, goals and other basic conditions surrounding the data center must first be defined before the technical details of the infrastructure can even be planned. This section describes the issues that need to be taken into consideration in infrastructure planning and design.

2.1 Data Center Types

A multitude of terms exist that describe the business models, applications and services associated with data centers. The following explanations are provided to shed light on these terms.

2.1.1 Business Models and Services

The term "data center" alone does not allow for any clear conclusions to be drawn with regard to the business model used. As a result, the terms

Housing – hosting – managed services – managed hosting – cloud services – outsourcing – and others

describe just some of the services for which providers furnish and maintain a data center infrastructure. Other providers put IT services on the market, but do not actually operate their own data centers. A variety of different business models exist in this sector as well, including:

- Fixed rentals of larger areas in third-party data centers
- Rentals by need
- Resellers for data center services

Housing refers to the provision of space, including cabling. Customers provide their own servers, switches, firewalls, etc. and manage these components themselves or through contractual partners.

Hosting refers to IT services based on servers, storage media, Internet connections, etc., in particular:

- Web hosting
- Share hosting
- File hosting
- Free hosting
- Application service provider (ASP)
- Internet service provider (ISP)
- Full service provider (FSP)
- Cloud computing provider, etc.

Managed services and **managed hosting** means that contractual parties make specific arrangements for just those services that are required. Typical variants include:

- The data center runs customer servers
- The data center makes servers available

Cloud services come in even a wider variety of forms. Many companies offer cloud services in line with this current trend. These services include:

- SaaS (Software as a Service),
- IaaS (Infrastructure as a Service),
- PaaS (Platform as a Service) and
- S+S (Software plus Service).

Purely housing services fall under the category of outsourcing. Moving all company IT operations to third-party premises would also be considered a form of outsourcing.

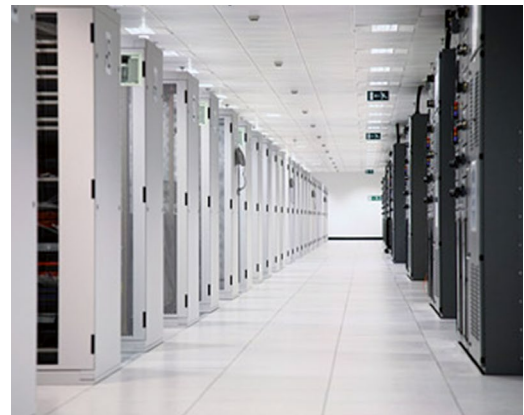
Space

The terms

Collocation – open collocation – cage – suite – room – rack – cabinet – height unit – and others

refer to either the areas of space in a data center that can be leased, or the leasing business model.

- **Collocation**, or collocation spaces, house the IT equipment owned by a given user. In **open collocation**, several customers make use of the same space.
- **Cage – suite – room** refers to a separate room or sealable section in a data center in which customers may house their IT equipment. Customers can even make their own decisions regarding cabling in these spaces, if the operator of the premises so agrees.
- **Rack – cabinet** are synonymous terms for the housing unit in which devices and distributors are housed. The customer and the data center normally make flexible arrangements regarding what model, types of use and/or equipment, and height units can be selected.



2.1.2 Typology

Neither experts nor industry associations have defined clear specifications on data center types and sizes. At this point, we provide, on the basis of existing classification models, a differentiation of data center types, especially with regard to their purpose:

Statistical Approach

This typology was used mainly with respect to data center energy consumption (see US-EPA 2007, TU Berlin 2008, Bailey et al. 2007). US-EPA uses terms like: server closet, server room, localized data center, mid-tier data center, and enterprise-class data center.

The German Federal Environment Agency refined this typology approach further, in an inventory it carried out to determine resource and energy consumption. This approach is based on the following figures.

Availability as Criterion

A primary characteristic for measuring the quality of a data center is its reliability or availability. Different classifications work using this criterion (BSI 2009, Uptime Institute 2006, BITKOM 2009, and many others).

Here are some examples: These include different specifications for data centers:

BSI DE Availability Classes	VK 0	~59%	Approx. 2-3 weeks/year	No requirements
	VK 1	99%	87.66 hours/year	Normal availability
	VK 2	99,9%	8.76 hours/year	High availability
	VK 3	99,99%	52.6 minutes/year	Very high availability
	VK 4	99,999%	5.26 minutes/year	Maximum availability
	VK 5	99,9999%	0.526 minutes/year	Disaster-tolerant
Tier Classes US Institute	Tier I	99,671%	28.8 hours/year	
	Tier II	99,749%	22.0 hours/year	
	Tier III	99,982%	1.6 hours/year	
	Tier IV	99,995%	24 minutes/year	

BITKOM DE Data Center Categories	A	72 hours/year
	B	24 hours/year
	C	1 hour/year
	D	10 minutes/year
	E	0 minutes/year

Classification by Purpose

In many cases, data centers are classified on the basis of the underlying business model, e.g. housing and collocation data centers, high-performance data centers, and others.

Operator Type

Operators can also be classified by their type and branch of industry: Banks, automobile, research, telecommunications, public authorities and companies. The characteristics of corporate data center and Internet data center are also used to classify operators.

- Corporate data center (internal data center of a company)
Data centers which provide IT services for a company and to which these services are also assigned, whether the data center is a separate company, a department within the company, etc.
- Internet data center (service provider)
Data centers that furnish services for third parties. These include services of housing, hosting and collocation and well as managed services and exchange services.

Corporate data centers may also be offered on the market as Internet data centers or service providers. This is especially true of public utilities.

2.1.3 Number and Equipment

The above-mentioned study by the German Federal Environment Agency included a classification for the German market. Figures and data in the following table were taken from that study.

Data Center Type	Server Cabinet	Server Room	Small Date Center	Mid-Sized Data Center	Large Data Center
Size		x			x
Ø Number of servers	4,8	19	150	600	6,000
Ø Total power	1,9 kW	11 kW	105 kW	550 kW	5,700 kW
Ø Space	5 m ²	20 m ²	150 m ²	600 m ²	6,000 m ²
Ø Network					
Copper	30 m	170 m	6,750 m	90',000 m	900,000 m
Fiber optic		10 m	1,500 m	12,000 m	120,000 m

Number of Data Centers in Germany						Total
2008	33,000	18,000	1,750	370	50	53'170
Extrapolation for 2015						
"Business as usual"	34,000	17,000	2,150	680	80	53'910
"Green IT"	27,000	14,000	1',750	540	75	43'365

2.2 Classes (Downtimes and Redundancy)

The Uptime Institute, founded in 1993 and based in Santa Fe, New Mexico, is responsible for establishing specifications for the best-known classifications for data centers. These classifications define the availability of both physical structures and technical facilities. Tier classes I to IV describe the probability that a system will be functional over a specified period of time.

SPOF (Single Point of Failure) refers to that component in a system whose failure will cause the entire system to collapse. High-availability systems may not possess a SPOF.

2.2.1 Tier I – IV

The tier classification is based on all the components that are essential in a data center infrastructure, as well as some other factors. The lowest value of a specific component (cooling, power supply, communication, monitoring, etc.) determines its overall evaluation. Note that the classification also takes into consideration the sustainability of measures, operational processes and service processes in the data center. This is particularly evident in the transition from Tier II to Tier III, where the alternative supply path allows maintenance work to be performed without interfering with the operation of the data center, which in turn is reflected in the MTTR value (Mean Time to Repair).

Main Requirements	TIER I	TIER II	TIER III	TIER IV
Distribution paths power/cooling	Mutual	Mutual	1 active / 1 passive	2 active
Redundancy Active components	N	N+1	N+1	2 (N+1)
Redundancy Backbone	No	No	Yes	Yes
Redundancy Horizontal cabling	No	No	No	Optional
Double floor	12"	18"	30"–36"	30"–36"
UPS / Generator	Optional	Yes	Yes	
Continuous servicing	No	No	Yes	Yes
Fault-tolerant	No	No	No	Yes
Availability	99.671%	99.749%	99.982%	99.995%

N: Need (required)

Source: Uptime Institute

Tier I

This class corresponds to the requirements of smaller companies. At this level extranet applications are not yet required, and use of the Internet is more passive. Availability is considered a secondary factor.

A Tier I data center operates with non-redundant capacity components and single non-redundant distribution networks. These centers do not require emergency power supply systems, uninterrupted power supply systems or double floors. Maintenance and repair work are based on schedules. Faults may paralyze operations.

Tier II

This second level corresponds to requirements of companies that are already processing business processes online during business hours. Delays where the data center is not available on occasion are acceptable. However, data losses may not occur. Delays should not be business-critical (non-time critical backups).

A Tier II data center has redundant capacity components (N+1) and single non-redundant distribution networks. An uninterruptible power supply as well as double floors is required.

Tier III & IV

These higher levels correspond to requirements of companies that use their IT installations for internal and external electronic business processes. IT systems must be ready for operation and available around the clock. Times for maintenance and shutdowns must not lead to delays, operational interruptions or data loss. Tier III and IV requirements are the standard for e-commerce, electronic market transactions and financial services. High failure safety rates and security backups must be ensured at all times for organizations of these types.

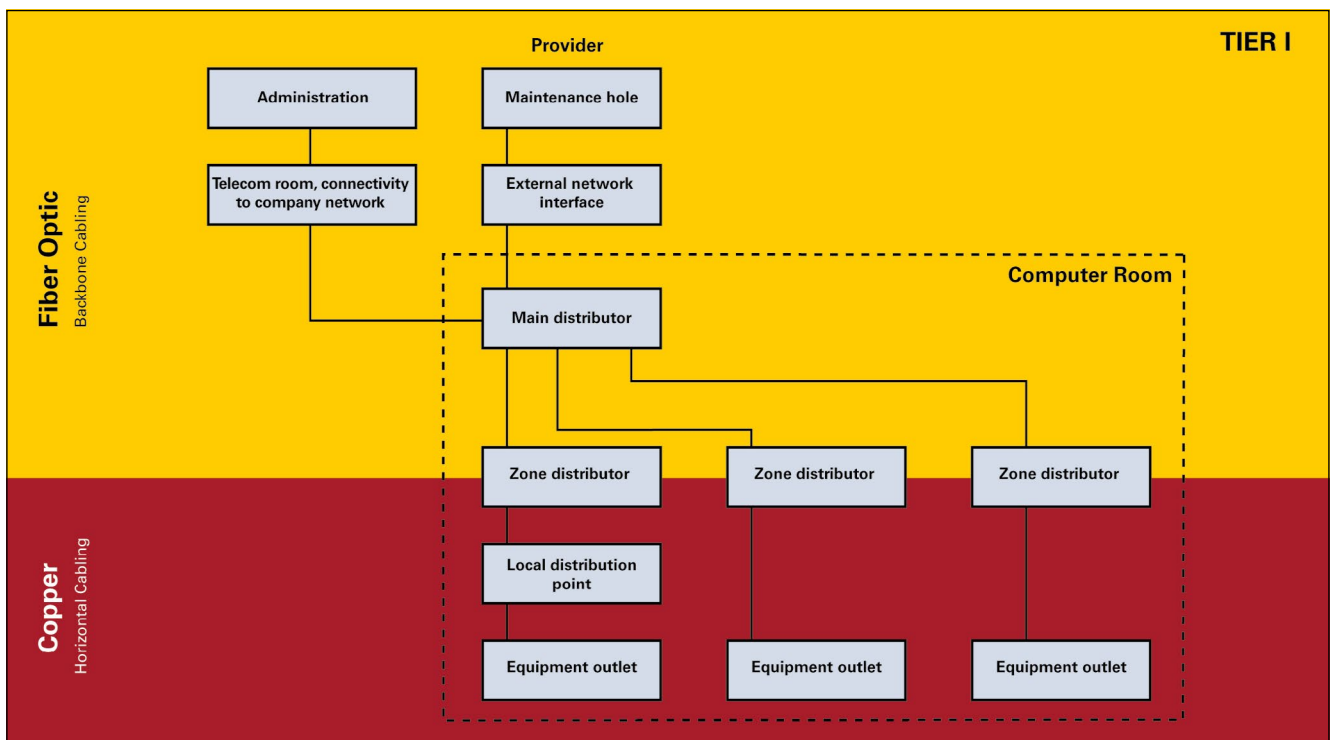
A Tier III data center operates with redundant capacity components and multiple distribution networks. In general, only one distribution network supports servers at any one time.

A Tier IV data center must also possess so-called fault tolerance. It operates using redundant building components. Multiple distribution networks support servers simultaneously. All servers are dual powered and installed properly so as to be compatible with the topology of the site's architecture.

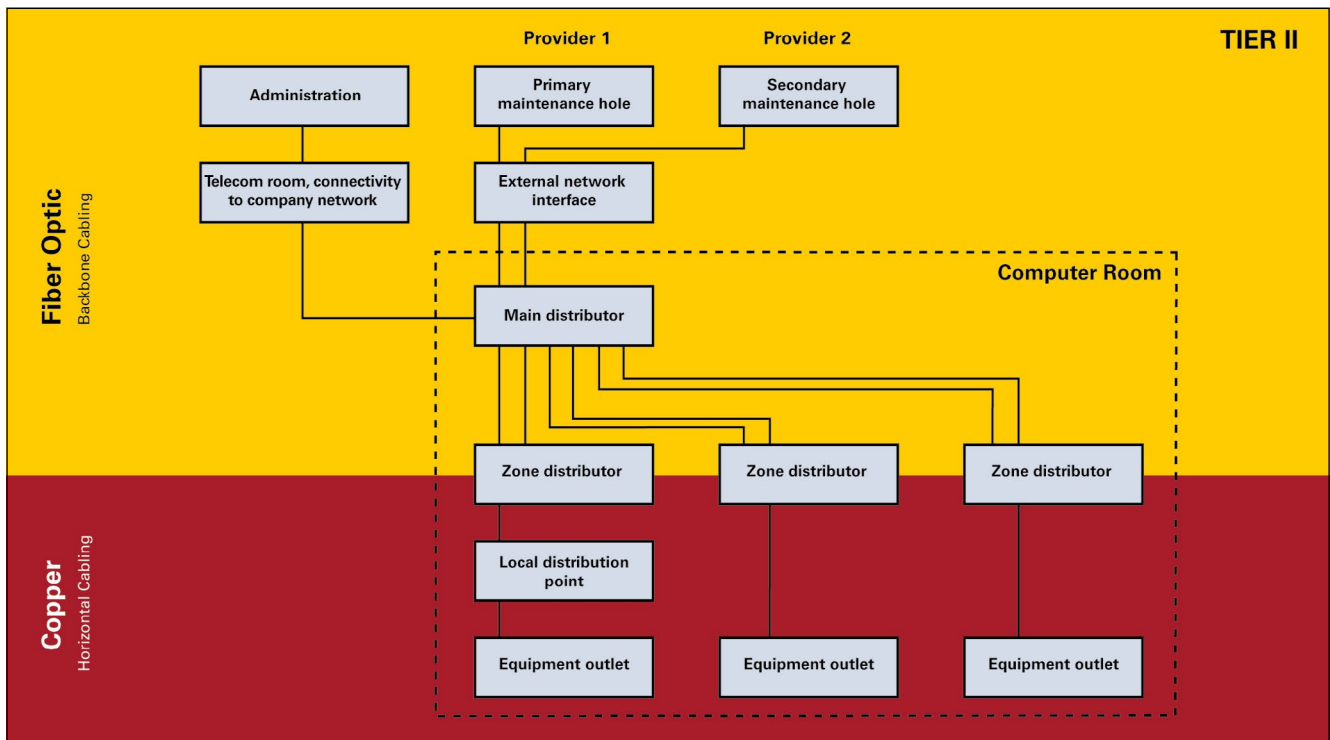
2.2.2 Classification Impact on Communications Cabling

Regardless of the corresponding tier level, cabling systems must be configured redundantly. This ensures availability and failure safety of the communication network in the data center. The following charts illustrate principles of cabling.

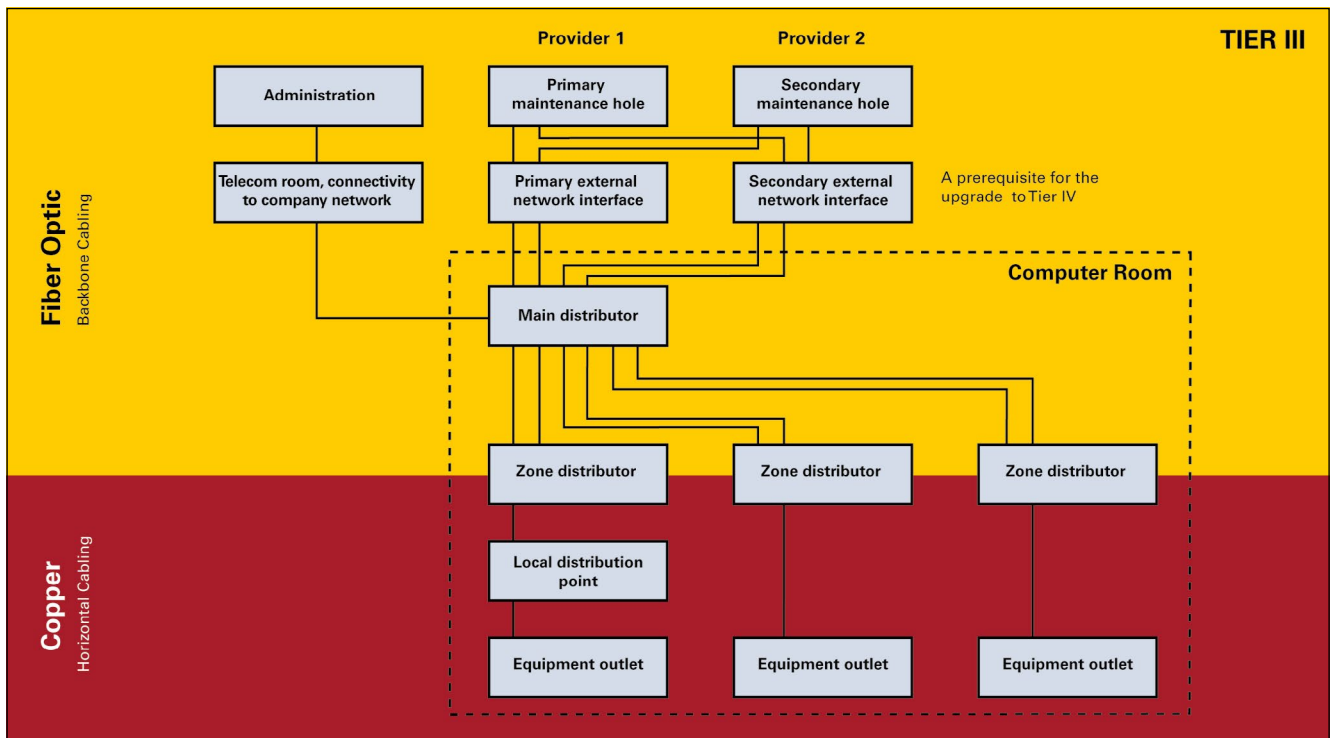
Data center layouts and cabling architecture are discussed in sections 3.2. and 3.4. respectively. The transmission media (copper and fiber optic) used for the specific areas are discussed in section 3.9.



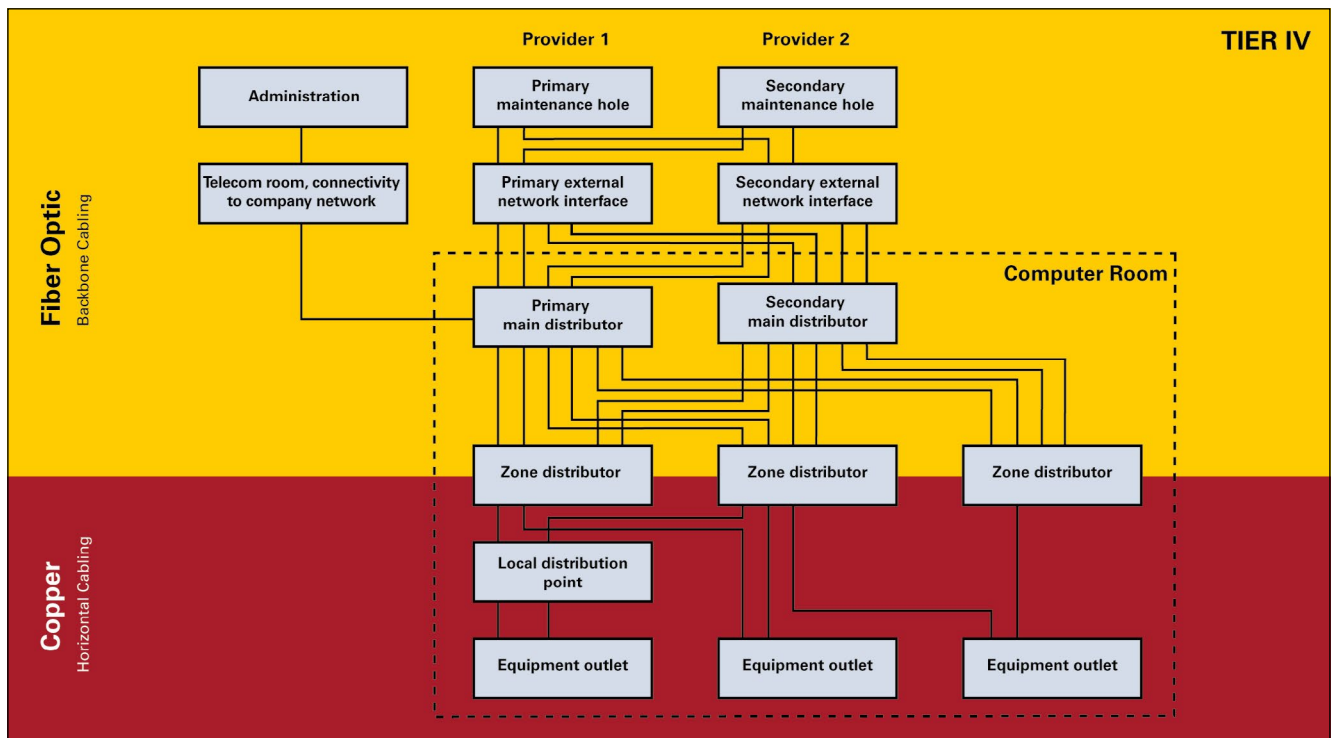
A simple star topology or structured cabling system fulfills Tier I requirements. Neither backbone cabling systems, horizontal cabling systems nor active network components are redundant. Network operation may be interrupted. However, data integrity must be ensured.



Backbone cabling and horizontal cabling at the Tier II level are also in a star topology and not redundant. Redundancy must be planned for active network components and their connections. Network operation may only be interrupted at specified times or only minimally during peak hours of operation.



Backbone cabling and active network components are configured redundantly in a star topology at the Tier III level. Network operation must be maintained without interruption within specified times and during peak hours of operation.



The Tier IV level requires that backbone cabling and all active components as well as the uninterruptible power supply and the emergency power generator are redundant, 2 x (N+1). Horizontal cabling may also be configured redundantly if desired. Systems and networks must operate free of interruption. 24/7 operation is an absolute requirement. This means that the data center runs around the clock, on all days of the week. It must be planned to be fault-tolerant, without a SPOF (single point of failure). Maintenance and repair work may be carried out during continuous operation but must not lead to downtimes.

In conclusion, note the difference between the scientific classification and standard. The Tier classification of the Uptime Institute is based on a comprehensive analysis of a data center, from the point of view of the user and the operator. By contract, a Tier classification per TIA-942-A is more a checklist for designing data centers. IA-942-A specifies Tier classes using Arabic numbers, whereas the Uptime Institute uses Roman numbering.

In addition, the costs and time periods that are to be expected for implementing a Tier I and Tier IV data center may be of interest to planners and investors. The following table from the Uptime Institute gives an overview of sample values.

Implementation Time and Investment Costs

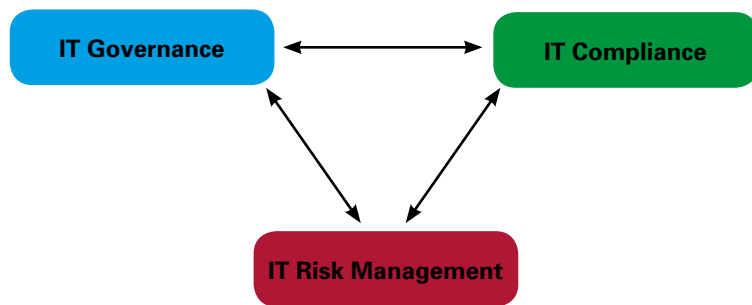
	TIER I	TIER II	TIER III	TIER IV
Implementation time	3 months	3 - 6 months	15 - 20 months	15 - 20 months
Relative investment costs	100 %	150 %	200 %	250 %
Costs per square meter	~ \$ 4,800	~ \$ 7,200	~ \$ 9,600	~ \$ 12,000

Source: Uptime Institute

2.3 Governance, Risk Management & Compliance

Most business processes for organizations, companies as well as public authorities, are becoming increasingly dependent on information and communication technologies. Their data centers must function reliably under all circumstances. Data center operators, through suitable corporate management, appropriate risk management and clear regulations, can take appropriate precautions to ensure their IT systems operate in a stable manner. This section provides an introduction to the action areas that are relevant in this regard.

Governance, risk management and compliance, or GRC, is an umbrella term that covers an organization's approach across these three areas.



"GRC is an integrated, holistic approach to organization-wide governance, risk and compliance ensuring that an organization acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness." This scientifically established definition of GRC was published in 2010, and validated by GRC experts (Racz et al. 2010).

Governance

Governance refers to corporate management that is carried out on the basis of prescribed guidelines. These guidelines include the definition of corporate goals, the planning of the necessary resources to accomplish them and the methods applied to implement them.

Risk Management

Risk management refers to an organization's identification of known and unknown risks through the use of pre-defined analyses. Companies must begin to continuously examine these risks at an early stage and develop strategies through which these risks can be minimized. In the event a risk or loss occurs, the company must then implement preventive measures and create a buffer through which these losses can be delayed or minimized.

Compliance

Compliance is considered the observance of internal and external standards that regulate the provision and processing of information. The following issues, among others, are involved in compliance:

- Directives from standardization drafts,
- Data access regulations
- Legal bases for their use.

Each of these three action areas involves special consequences for company IT departments and systems. The explanations presented below focus on IT.

2.3.1 IT Governance

IT governance refers to the organization, control and monitoring of a company's IT infrastructure and IT processes by company management. The main components of IT governance include:

- **Strategic Alignment:** The continuous alignment of IT processes and structures with strategic enterprise objectives and processes, and supporting the company in achieving its corporate goals.
- **Resources Management:** Responsible, sustainable use of IT resources.
- **Risk Management:** Identification, evaluation and management of IT-related risks
- **Performance Measurement:** Measurement of how well IT processes and services perform, including reporting functions.
- **Value Delivery:** Monitoring and evaluating the worth IT contributes to the business.

A number of processes support and regulate the implementation of IT governance, such as:

- Control model, focusing on financial reporting: **COSO** (Committee of Sponsoring Organizations of the Treadway Commission)
- Corporate Governance in IT: **ISO/IEC 38500:2008** Corporate Governance in Information Technology
- Control model for IT management: **Cobit (Control Objectives for Information and related Technology)**
- **Implementation of IT Service Management**: ISO 20000, ITIL (Information Technology Infrastructure Library)
- Information security: **ISO/IEC 27002** and basic **IT protection catalogs**

2.3.2 IT Risk Management

The purpose of IT risk management is to ensure that company business runs smoothly.

- In this case, risk is understood to mean any negative deviation from planned values,
- Whereas chance refers to any positive deviation.

An IT risk management system is implemented for legal, financial and/or operational reasons:

- Legal aspects
 - Conscientious management (see SOX, KonTraG, RRG)
- Economic aspects
 - Ensuring a company's existence by reducing errors and failures in IT systems
 - Negotiating advantage with potential customers by enhancing their trust in the ability to supply
 - Advantage in rating assessment of banks for credit approval
 - Premium advantages with insurance policies (e.g. fire and business interruption insurance)
- Operational aspects
 - Wide range of applications and saving options

One normally falls back on four strategies to counter a risk:

- Avoidance
- Mitigation
- Transfer
- Acceptance

IT risks fall into the following categories:

- Organizational risks
- Legal and economic risks
- Infrastructural risks
- Application and process-related risks

2.3.3 IT Compliance

In compliance, everything involves keeping to regulations, including legal requirements, internal company rules, contractual provisions and typical industry regulations. Corporate management is obligated to comply with these rules. This also applies for IT areas, especially information security, availability, data storage and data protection.

Managing directors and boards in listed companies and companies with limited liability can be made to be personally liable for complying with regulations. In many cases, customers or even competitors require that specialized standards or good practices be followed in addition to legal regulations.

Compliance must be viewed as a continuous, permanent process. The corresponding analyses, evaluations, documentation and necessary modifications in the area of IT must be carried out on a continuous basis.

2.3.4 Standards, Norms and Regulations

Below is an overview of the most important standards for managing IT security and risk in data centers. The table is based on the compass provided by the German industry association BITKOM (version 4.0, August 2009). The table is followed by a brief explanation of the five standard areas described in the table.

Enterprise type	Banks/insurance companies	Public authorities / administration	Consulting	HW/SW manufacturers	IT service providers	Public health system	Law firms	Skilled trades and industry	Service providers	International orientation
Information Security Management System (ISMS)										
ISO/IEC 27001	●	●	○	∅	●	●	●	∅	∅	●
ISO/IEC 27002	●	●	○	∅	●	●	●	∅	∅	●
ISO/IEC 27006			∅		∅					●
IT-GS (DE)	●	●	●	●	●	●	●	●	●	∅
Security Measures and Monitoring										
ISO/IEC 18028	∅	∅	∅	∅	∅	∅	∅	∅	∅	●
ISO/IEC 24762	∅	∅	∅	∅	∅	∅	∅	∅	∅	●
BS 25777:2008	∅	∅	∅	∅	∅	∅	∅	∅	∅	●
Risk Management										
ISO/IEC 27005	∅	∅	∅	∅	∅	∅	∅	∅	∅	●
MaRisk / MaRisk VA	●				∅					
Relevant Standards										
COSO	●	●	●	∅	●	●	∅	●	●	●
ISO/IEC 38500	●	●	●	∅	●	●	∅	●	●	●
Cobit	●	●	●	∅	●	∅	∅	●	●	●
ITIL	●	●	●	●	●	●	○	●	●	●
IDW PS 330 (DE)		●	∅	∅	∅	●	●	●	●	
SWISS GAAP FER (CH)		●	∅	∅	∅	●	●	●	●	
Regulations										
KonTraG (DE) / RRG (CH)	●	○	○	○	∅	○	○	∅	∅	∅
SOX / EURO-SOX	∅	○	○	○	○	○	○	∅	∅	●
Basel II/III	●	○	○	○	∅	○	○	∅	∅	∅
Solvency II	●	○	○	○	∅	○	○	∅	∅	∅
Federal Data Protection Act (BDSG, Germany) / Data Protection Act (DSG, Switzerland)	●	●	∅	●	●	●	●	●	●	●

Relevance: ● = high, ∅ = partial, ○ = low

I. Information Security Management System (ISMS)

- **ISO/IEC 27001**
This standard emerged from the British standard BS 7799-2 and describes basic ISMS requirements within an organization (company or public authority). The standard makes use of a process approach to include ISMS requirements. The standard primarily addresses company managements and IT security managers, and secondarily parties responsible for implementation, technicians and administrators. The ISMS implementation can be audited by internal and external auditors..
- **ISO/IEC 27002**
This information security management guide also emerged from the British BS 7799-1. It is normally used in areas that require information security. Target group: IT security managers..
- **ISO/IEC 27006**
This standard describes requirements for bodies that provide audits and certifications for information security management systems.
- **IT-Grundschutz (IT-GS)**
IT-GS is a German regulation. Since 1994, the Federal Office for Information Security (BSI) in Germany has been issuing the IT Baseline Protection Manual, which provides detailed descriptions of IT security measures and requirements for the IT security management. Today it is fully compatible with ISO/IEC 27001 and also incorporates the recommendations specified in ISO/IEC 27002.

II. Security Measures and Monitoring

The following standards are used as a basis for improving IT network security. These standards are not just limited to internal corporate networks, but also cover security for external network access points

- **ISO/IEC 18028 (in the future 27033)**
The objective of this standard is to focus on IT network security by specifying detailed guidelines aimed at different target groups within an organization. The standard covers security aspects involved in working with IT networks, security involved in maintenance work and continuous operation, and relationships between networks as well as external connections.

The standard comprises five parts:
 1. Guidelines for network security
 2. Guidelines for the design and implementation of network security
 3. Securing communications between networks using Security Gateways
 4. Remote access
 5. Securing communications between networks using Virtual Private Networks (VPN)
- **ISO/IEC 24762**
This standard provides guidelines on the provision of information and communications technology disaster recovery (ICT DR) services. It includes requirements for implementing disaster recovery services and provides information on installations, including emergency workstations and alternate processing sites.
- **BS 25777:2008**
The purpose of this standard is to establish requirements for IT continuity management.

III. Risk Management

- **ISO/IEC 27005**

Guidelines for systematic, process-oriented risk management. Supports compliance with risk management requirements established by ISO/IEC 27001.

- **MaRisk / MaRisk VA**

This is likewise a catalog of risk management requirements specific to Germany. It was originated by the German Federal Financial Supervisory Authority (BaFin) and contains The Minimum Requirements for Risk Management (MaRisk). The standard lays out explicit requirements for IT security and disaster recovery planning. A second version of the standard is directed at insurance companies, leasing and factoring companies (MaRisk VA).

IV. Relevant Standards

- **COSO**

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed this framework for internal monitoring systems. It includes:

- o A methodology for implementing the primary components of an internal control system, e.g. the control environment in a company
- o Risk evaluation procedures
- o Specific control activities
- o Information and communication measures in a company and
- o Measures required for monitoring of the control system

COSO is the basis of reference models like Cobit and facilitates their introduction.

- **ISO/IEC 38500**

The standard "Corporate Governance in Information Technology – ISO/IEC 38500" recommends six key principles for corporate governance in IT:

- o **Responsibility:** Adequate consideration of IT interests by top management
- o **Strategy:** Corporate strategies must be extended to include considerations of potential areas in IT and to align IT strategies with corporate principles.
- o **Acquisition:** A rigorously demand-oriented IT budget plan, based on transparent decision making
- o **Performance:** Align IT services with the requirements of corporate areas and departments
- o **Conformance:** IT systems must comply with all applicable laws, regulations and internal and external standards, etc.
- o **Human Behavior:** The needs of internal and external IT users are taken into account in the IT concept.

The standard assigns three functions to each of these principles:

- o **Assessment:** Continuous assessment of IT performance
- o **Management:** Guiding IT measures so they are aligned with business requirements
- o **Monitoring:** Systematic monitoring of IT compliance and IT systems productivity

- **Cobit**

The ISACA formulated Cobit as a comprehensive control system that encompasses all aspects of information technology use, from planning and even up to disposal of IT equipment. The goal of the standard is to provide support for management and all departments involved for carrying out their responsibilities in accordance with IT governance. ISACA stands for Information Systems Audit and Control Association, while Cobit means Control Objectives for Information and Related Technology. Here are the Cobit elements and their respective target groups:

- | | |
|---------------------------|---------------------------------|
| o Executive Summary | Senior executives like CEO, CIO |
| o Framework | Senior Operational Management |
| o Implementation tool set | Middle management, directors |
| o Management guidelines | Middle management, directors |
| o Control objectives | Middle management |
| o Audit guidelines | Line management and auditors |

- **ITIL**

ITIL provides a best practices reference model for implementing IT management. This standard is applied especially in IT service management (ITSM). ITIL was originally derived from the term IT Infrastructure Library. The goal of ITIL is to base IT organizations on life cycles. The organization should be continuously process-oriented, service-oriented and customer-oriented. ITIL V3 can be used to better align IT service management with corporate strategy. This will then ensure the management process is compatible with the ISO 20000 IT service management standard.

Experts in IT can acquire ITIL certification. Companies can have their process management certified in accordance with the international standard ISO/IEC 20000 (former BS 15000).

- **IDW PS 330 (Germany)**

Financial auditors in Germany are obligated to look into the IT systems of the company being audited, when these systems are related to accounting. Depending on the complexity of the IT systems in use, comprehensive testing of the IT system in accordance with the IDW Auditing Standard 330 (IDW PS 330), or at least an audit of selected subsystems may be required.

- **SWISS GAAP FER (Switzerland)**

The Swiss GAAP FER focuses on the accounting system of small and mid-sized organizations and company groups operating on a national level as well as non-profit organizations, employee benefit institutions and insurance companies. These organizations are provided with an effective framework for authoritative accounting to provide a true and fair view of the company's net asset, financial position and earnings situation. Other goals include:

- o Promoting communication with investors, banks and other interested parties.
- o Facilitating comparability of annual financial reports across time and between organizations.

V. Regulations

- **KonTraG (Germany)**

The German Act requires financial controls and transparency of listed corporations as well as limited liability companies. Its objectives include:

- o Implementation of a monitoring system for early detection developments that threaten their existence.
- o Requiring management to implement a corporate-wide risk management policy. The act stipulates personal liability of members of the board of management, the board of directors and the managing director.

- **Accounting and Auditing Act (RRG, Switzerland)**

The comprehensive revision of Switzerland's audit legislation in 2008 made risk assessment compulsory. It is now subject to review by the auditing body. Overall responsibility for this lies with the highest decision-making and governing body of the company, while the board of managers is responsible for introduction and implementation. This audit requirement extends to all corporate forms as well as organizations of economic significance.

- **SOX (US)**

The Sarbanes-Oxley Act of 2002 (also called SOX, SarbOx or SOA) is a United States federal law that was enacted on July 30, 2002. Its objective is to improve the reliability of accurate financial reporting by those companies which dominate the nation's securities market. Since the law was implemented, financial auditors and company management must now furnish proof that a functional internal monitoring system exists. Company boards are responsible for the accuracy and validity of corporate financial reports. These provisions apply to all companies that are listed on an American stock exchange, and in certain cases their subsidiaries as well.

- **EURO-SOX**

The 8th EU Directive, also known as EURO-SOX, is aimed at establishing an internationally recognized regulation for the auditing of financial statements in the European Union. It is geared to the SOX model of the United States, but applies to all capital companies. Small and medium-sized companies (SME) are also now required to address issues such as risk management, IT security and security audits. Germany's Accounting Law Modernization Act (BilMoG) applies similarly in that country.

- **Basel II**

The term Basel II refers to the entire set of directives on equity capital that were put forward by the Basel Committee for Banking Supervision. These directives apply to all banking institutions and financial service providers. Initially, Basel II involved internal banking regulations, so bank use the standards today for their customers as well. This results in a direct relationship between terms for raising funds and credit risks. The failure of a data center would significantly increase credit risk, in other words a company with a secure data center can negotiate better terms. In Germany, Basel II rules were implemented through measures including the German Banking Act (KWG), the Solvency Regulation (SolV) and the Minimum Requirements for Credit Management (MaRisk), while in Switzerland, its implementation was carried out by the FINMA. In France, Basel II rules were implemented through the Autorité des Marchés Financiers (AMF), while in the United Arab Emirates its implementation was carried out through the Securities & Commodities Authority (SCA).

- **Basel III**

Basel III refers to the extended set of rules and regulations adopted by the Basel Committee at the Bank for International Settlements in Basel (Switzerland). It continues the previous banking regulations in light of weaknesses uncovered as of the global financial crisis of 2007. The body of rules has been applied in Switzerland since 2013 and is leading especially to stricter capital ratio¹⁾. Implementation within the European Union is being achieved by amendments to the Capital Requirements Directive (CRD) starting in 2014.

- **Solvency II**

Solvency II is the insurance industry's equivalent of Basel II. Solvency II regulations are expected to take effect in companies starting in 2014. The EU Commission has been negotiating over a binding implementation starting in 2016 or 2017²⁾

- **BDSG (DE) / DSG (CH)**

Examples of data protection acts are German's Federal Data Protection Act (BDSG) and the one in Switzerland (DSG). The goal of these acts is the respectful treatment of personal data. From a data center perspective, the technical and organizational measures that might be necessary are of primary relevance, especially those concerning regulations on access control and availability control.

¹⁾ Source: http://de.wikipedia.org/wiki/Basel_III

²⁾ Source: http://de.wikipedia.org/wiki/Solvency_II

2.3.5 Certifications and Audits

Data centers can undergo appropriate certification processes and audits to have their level of performance and security inspected by independent bodies. This certification can then be provided to customers and contracting principals as proof of the quality of the data center. Certification and audit preparations are costly and time-consuming. Possible motivation and reasons for certification include:

- **Differentiation:** Strengthening trust on the part of customers, employees and the public. Differentiating oneself from the competition. Competitive advantages when participating in invitations to tender.
- **Internal benefits:** Identifying and reducing weak areas.
- **Regulations**

Common certifications and audits, as well as the relevant standards for data centers include:

- DIN EN ISO 9001- Quality Management
- ISO 27001 – Information Security Management Systems
- ISO 27001 – IT Baseline Protection
- ISO 20000 – IT-Service Management
- DIN EN ISO 14001 – Environmental Management
- SAS 70 Type II certification – SOX relevant
- IDW PS951 – German equivalent of the American SAS70
- Data Center Star Audit – ECO Association (Association of the German Internet Economy)
- TÜV certification for data centers – (TÜV = Technical Inspection Association, Germany)
- TÜV certification for energy-efficient data centers

2.3.6 Potential risks

Very few companies are aware of their own IT risks. In 2010, the IT Policy Compliance Group determined that 80% of companies have poor visibility in this area. These companies lack transparency and proper process controls. The following table is provided as a starting point to help identify priorities in this area. It is geared to the laws and regulations that apply in Germany and to typical management structures. This table is provided only as a guideline..

Liability risks

Need for regulation/ Need for action	Responsibilities	Legislation	Potential damage and losses
Strategic tasks	Management / CEO	See regulations	– Losses due to system failure – Insolvency – Increased costs of corporate loans – Loss of insurance cover – Loss of image – Monetary fines
Design-related tasks	Management / CEO Data protection officer Head of IT	See regulations Employment contract	– See strategic tasks – Data loss – Unauthorized access – Virus infection – Loss due to failed projects – Loss of claims against suppliers – Loss of development know-how
Operational tasks	Management / CEO Data protection officer Head of IT Employees	See regulations Employment contract HGB UrhG StGB	– No annual audit confirmation – Taxation assessment – Imprisonment – Corporate shutdown / loss of production – Capital losses – Loss of image – Loss of business partners or data

Excerpt: Liability Risk Matrix ("Matrix der Haftungsrisiken"), Bitkom, as of March 2005

In addition, contracts with managers and managing directors may contain provisions to regulate issues of liability issues. Companies frequently include limited liability for negligent behavior in agreements between managing directors and the company. Claims for damages can then be dismissed in certain cases. Note: In the case of listed companies, exoneration of managing directors does not automatically result in a waiver of damage claims.

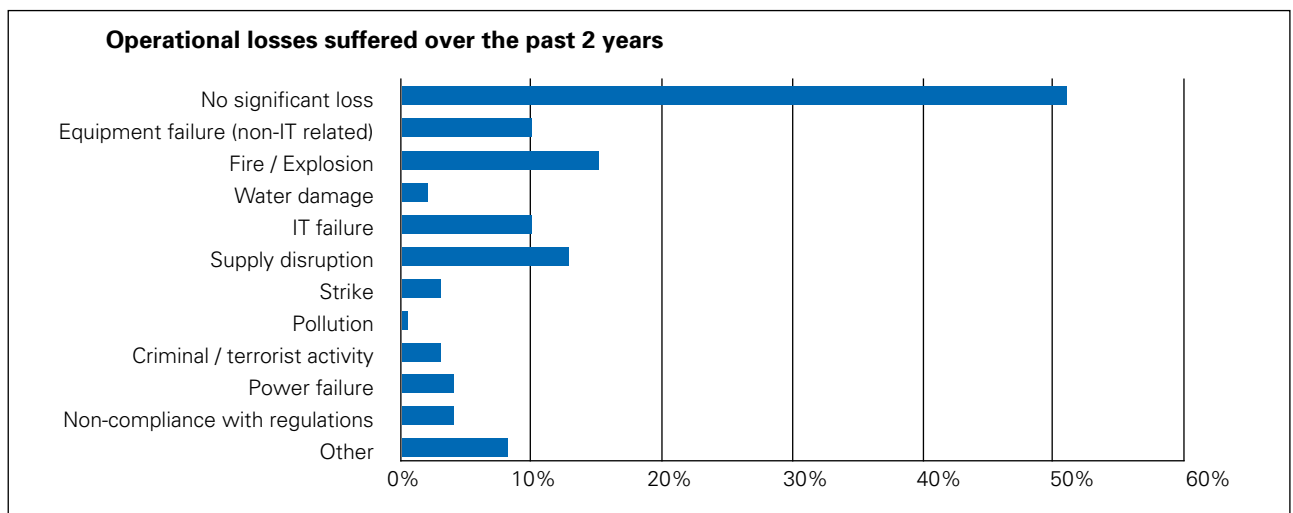
Experience shows:

- ... Managers often fail to see their liability risks
- ... Most managers are unaware of the extent of their liability risk
- ... The risk of being held financially liable for mistakes increases as the use of IT systems and data volume grows
- ... Managing directors and company boards can be held personally liable if they fail to provide sufficient IT security for their companies
- ... The boss is not the only one held liable!

Operational Risks

Operational risks in companies can not only lead to general losses, but also have very serious consequences on IT systems and data centers. These risks can arise through inadequate procedures, system failures, employee mistakes or external events. They can then lead, directly or indirectly, to losses. Due to the efforts of Basel II, organizations now pay particular attention to operational risks of this nature. Areas of focus with regard to operational risks include:

- Information system failures
- IT security policy
- Human resource security
- Physical and environment security
- IT system productivity
- Keeping current systems, procedures and documentation up-to-date
- Information and data of all business operations
- Evaluation and identification of key figures
- Clear, previously drawn-up emergency plan
- Backups of all data

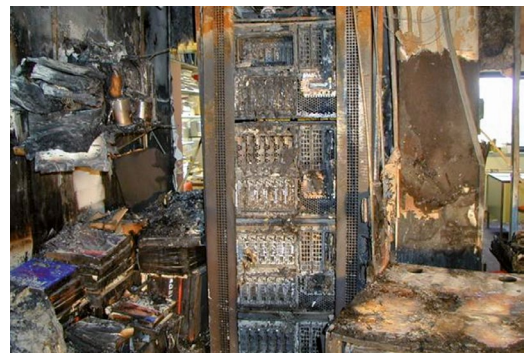


Source: Marsh – business continuity benchmark report 2010 – survey of 225 companies

Typical operational risks include:

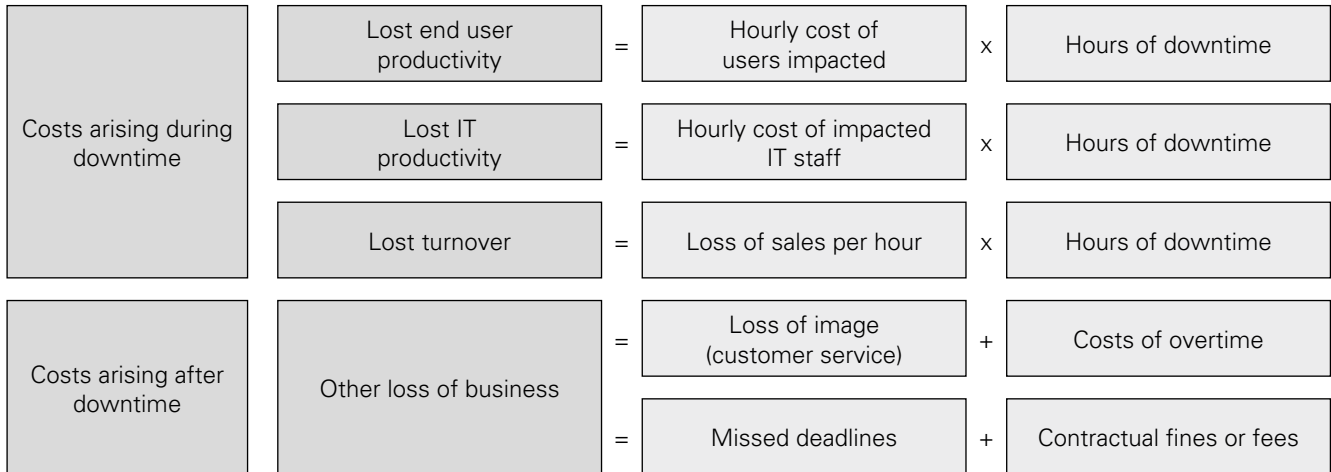
- Natural disasters, acts of God
- Breaches of data and information security
- Fraud, cybercrime, industrial espionage
- Technical failure, loss of business-critical data
- Terrorist attacks, transporting hazardous goods
- Disruption of business processes or the supply chain and disturbances occurring on business partners premises
- Organizational deficiencies, strikes, lockouts
- Official decrees

This statement from a German court describes the true meaning of risk: "Experience tells us you can count on a fire breaking out at practically any moment. When decades go by without a fire, it does not mean that no danger exists, it just means that we've been lucky so far. But the odds are still the same, and a fire can still break out at any moment." This is why, for example, equipment such as fast, reliable fire-detection and extinguishing systems or even a fire prevention system are an absolute necessity for secure data center operation. Incidentally: Water as an extinguishing agent has no business in data centers. Specialty companies offer suitable alternatives as well as automatic extinguishing systems; the installation of this equipment must be carefully planned.



Cost of Downtime

A 2010 study by the market research firm Aberdeen Research determined that only 3% of the data centers operated by companies were available 100% over the past twelve months. Only 4 percent of companies stated the availability of their data center was at 99.999%. Data center failures – even those that only last a few minutes – can result in significant costs. The following diagram shows how to calculate the cost of downtime.



Source: securitymanager 2007

"Avoidable Cost of Downtime", a report from 2010, states that companies require more than eight hours to restore data after an IT system failure. The survey was carried out among 1,800 companies, 202 of which are located in Germany. The German companies attested their systems are at a standstill for a total of 14 hours per year.

According to other studies, IT system downtimes that last three days are considered a threat to the existence of a company. 54 percent of customers switched to a competing firm as a result of an IT system failure (Symantec study, 2011).

2.4 Customer Expectations

What do customers expect from a data center? This key question is still another factor that must be taken into consideration when assessing and analyzing data centers and also in related plans, security measures, performance goals and profit objectives. This section deals with data center considerations in terms of market and customer expectations, and focuses on corporate data centers and themes of availability and costs.

Availability

Availability is a primary customer expectation. Customers and users must be able to make use of a data center continuously and without experiencing delays. To be specific, customers and users expect the following:

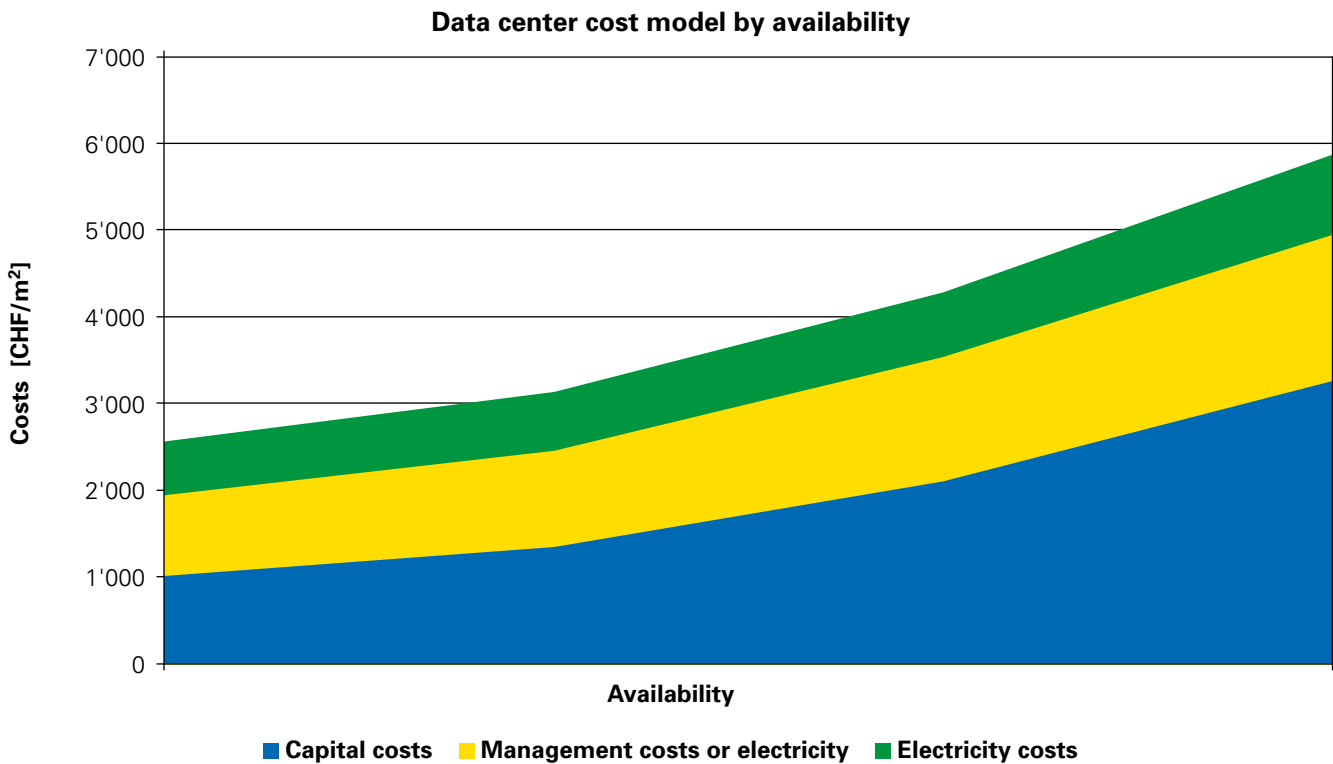
- Hardware and software security, reliable infrastructure, organizational security and general site security
- Continuous IT operation, 24/7 availability, 24/7 monitoring, 24/7 access
- Flexibility in power supply and climate control
- On-demand models that can be displayed
- Structural and technical fire protection
- Security systems such as burglar alarms, access control systems, video surveillance, building security, security personnel, security lighting, central building control systems, etc.
- Redundant connections over multiple carriers
- Continuous cost optimization, profitability
- Sustainability, energy efficiency, green IT
- Fast response times even during system changes and upgrades
- Low latencies to meet e-commerce requirements
- Safe distance between backup sites and/or mirroring sites

Requirements with regard to availability normally receive a high priority, right from the very start of the planning process. All parties want an optimal solution, but the reality is often that costs lie far over expectations.

High availability means: More security measures = greater costs

It is therefore recommended that requirements of availability be considered at the project level if possible, and that alternative concepts (e.g. the 2-location concept) be examined.

The level of availability has an effect on both installation costs as well as operating costs. The Swiss Federal Office of Energy (SFOE) has developed a cost model for transparent analysis. The graphic below is part of it and makes model calculation models possible.



Source: Department of the Environment, Transport, Energy and Communications, Swiss Federal Office of Energy, Oct. 2008

The IBM group determined that, accumulated over 20 years, the operating costs of a data center are 3 to 6 times as high as the original investment. Energy costs make up approximately 75% of all operating costs.

The following table illustrates the utilization rate of data center components on the basis of the Tier levels described in section 2.2.1.

Degree of redundancy	N	N+1	N+1	N+1	N+1	2N	2(N+1)	2(N+1)	2(N+1)	2(N+1)
Configuration	1	1+1	2+1	3+1	4+1	2	2(1+1)	2(2+1)	2(3+1)	2(4+1)
Number of components	1	2	3	4	5	2	4	6	8	10
Utilization Components	100%	50%	66%	75%	80%	50%	25%	33%	37.5%	40%

According to an IBM analysis, the increase in cost between a Tier-III and a Tier-IV installation amounts to 37 percent.

Power Costs

Power requirements of information and communications technology continue to increase on a worldwide basis. As a result, the IT industry must also deal with the corresponding energy costs. The strongest growth was observed in infrastructures, i.e. servers and data centers. Approx. 50% of this energy consumption and resulting CO2 emissions were actually caused by the surrounding infrastructure, such as air conditioning and power supply systems.

Data center operators can lower their energy consumption, not only through innovative technologies, but also by implementing cost-effective action measures such as arranging racks in hot and cold aisles and eliminating obstacles that hinder air circulation. As the following example shows, such investments payoff: A trend analysis commissioned by the German Federal Environment Agency (UBA) determined that if data centers in Germany continue to operate as they have to this point, their energy consumption will increase to 14.2 TWh by 2015. If these centers take advantage of absolutely all the options offered by "Green IT", this figure could be reduced to 6.0 TWh.

Data center types/numbers in Germany	2008	2015 Scenario	
		Business as usual	Green IT
Server cabinet	33,000	34,000	27,000
Server room	18,000	17,000	14,000
Small data center	1,750	2,150	1,750
Mid-size data center	370	680	540
Large data center	50	90	75
Energy consumption in TWh	10,1	14,2	6,0

Most companies have no idea how much of their total energy consumption is required for IT equipment alone. The following figures from Germany are provided as an example: Only 33% of all data center operators employ personnel with responsibilities related to energy efficiency, and 37.5% of operators have no points of contact whatever for electricity costs. Power consumption does not appear as an item in the IT budgets of 31.25% of all operators.

In addition to the indicators listed in section 1.10, the following values can be used to assess the energy efficiency of a data center:

Green Grid (USA)		
PUE	Power Usage Effectiveness	Ratio of power consumed by the entire facility to the power consumed by the IT equipment alone
DCIE	Data Center Infrastructure Efficiency	Ratio of power consumed by the IT-related systems to the power consumed by the entire facility (=1/PUE)
IEP	IT Equipment Power	Energy consumed by IT processing, storage and distribution plus management
TFP	Total Facility Power	The total energy consumed by the data center facility including climate control (cooling), power, surveillance, lighting, etc.
Uptime Institute (USA)		
SI-EER	(Site Infrastructure – Energy Efficiency Ratio)	The ratio of power consumed by the entire facility to the power consumed by the IT equipment alone
IT-PEW	(IT Productivity per Embedded Watt)	The ratio of IT productivity (network transactions, storage, and computing cycles) to the energy required for this purpose
DC-EEP		Value derived by multiplying SI-EER with IT-PEW

The PUE value is the generally-used standard of measurement. However, the data used in calculations are not always comparable to each other. The German Federal Environment Agency used the following PUE values in its 2010 study

Data Center Type	Ø PUE	
	2008	2015 Green IT
Server cabinet	1,3	1,2
Server room	1,8	1,5
Small data center	2,1	1,5
Mid-size data center	2,2	1,6
Large data center	2,2	1,6

Below, expected acquisition costs are compared with energy costs, using a server as example. Costs for floor space, maintenance, monitoring, etc. are not yet considered here.

Server hardware acquisition cost		1,500,00 Euro
Life span	4 years	
Power consumption (during operation)	400 watts	
Hours per year	24 h x 30,5 days x 12 months =	8,784 h
Power consumption per year	8,784 h x 0,4 kW =	3,513,6 kWh
Power costs per kWh in Germany	Price: Industrial customers	0,15 Euro
Power costs per year	3,513,6 kWh x 0,15 Euro =	527,04 Euro

Power costs		1 year	4 year
PUE factor = 3,0	527,04 Euro x 3 =	1'581,12 Euro	6'324,48 Euro
PUE factor = 2,2	527,04 Euro x 2,2 =	1'159,49 Euro	4'637,95 Euro

2.4.1 In-House and Outsourced Data Centers

The need to act with regard to data centers is generally a consideration that can be assessed over the long term. IT departments, being aware of trends and critical time points, can make strategic considerations at an early stage. One question that faces data center operators, for example, is whether they should set up additional in-house resources, just outsource the entire data center, or find combined solutions.

We first take the case where a company decides against completely outsourcing its IT systems, and at best accepts housing and hosting them with external service providers. This approach is considered below: The company must take the following issues into consideration:

- Continuing to develop its own data center further (own)
- Using housing or hosting services from a hosting provider (renting)
- Mixture between owning and renting

The arguments against outsourcing are mostly of a psychological or organizational nature, or are security-related.

Psychological Reasons

A fear of loss of control is the strongest reason for deciding against outsourcing. Typical arguments include:

- Fast responses to system faults are no longer possible
- You do not know who else has access to the computers you use

IT departments might also feel that they would become "less important" within the company since a core activity is now being outsourced.

This misgiving can easily be invalidated through appropriate processes and agreements with external data centers.

Organizational Reasons

Typical arguments against outsourcing from an organizational standpoint:

- Lack of transportation options for IT personnel
- Difficulty of coordinating internal and external staff
- Inability to carry out hardware operations at short notice
- Limited influence on scheduled maintenance work

However, upon careful review, one can see that not every visit into a data center is necessary. Many data center operators employ qualified technical staff on-site who can carry out simple hardware jobs on behalf of the customer. Most work can be carried out remotely. If company personnel themselves need to be on site more frequently, it might be possible to provide a local operator.

If the number of customers in the external data center increase, customer influence on scheduled maintenance operations drops. However, customers do have the option of selecting a higher level of availability and/or service. Higher availability means that maintenance operations can be carried out without downtimes

Security-Related Reasons

Risk-conscious IT managers often point to possible security weaknesses as an argument against outsourcing. However, this misgiving is usually quickly refuted. The following arguments speak in favor of the security provided by an external data center:

- Qualified service providers work in accordance with audited processes that define security in different areas.
- A data center set up on a company's own premises is sometimes exposed to higher risks. A remote location can be more secure.
- External data center operators can make their data center "invisible" to curious eyes and, if desired, guarantee anonymity for their customers
- Access restrictions can be implemented consistently since there are clear delineations between a company's own employees and external company personnel.

Relatively clear decisions can be derived after these arguments are examined in detail, weighted and the related costs compared. It is important, when examining bids from external data centers, to acquire a comprehensive list of all the costs involved. The information centers provide on power costs is often incomplete since these specifications often do not include non-IT equipment (see also PUE).

Combined solutions, where a company maintains its own data center but rents space from an external operator, offers the following advantages, among others:

- Backup concepts can be realized logically.
- Capacity bottleneck situations can be quickly isolated and resolved.
- The required flexibility (on demand) can be defined by contract.
- A higher security level can be achieved.

The bottom line is that there is no decision for outsourcing that is right in all cases; every concept has advantages and disadvantages. The important thing is to examine all aspects of the situation in light of your own specific requirements.

2.5 Aspects in Planning a Data Center

Areas on which to focus in preliminary planning include:

- The analytic phase, including an accurate determination of your current situation
- Definition of requirements
- Conception

These phases should also include estimation of the costs of constructing the solution as well as future operational costs. The following items in particular should be included in the preliminary planning process:

- Corporate strategies
- Requirements resulting from IT governance policy
- Requirements resulting from IT risk management policy
- A realistic determination of performance specifications

In addition, answers to critical issues must be provided at an early stage:

- Construction of an entirely new data center, or expansion of the existing one or
- Outsourcing (housing, hosting, managed services, cloud services) or
- Some alternative data center concept

Two factors are of vital importance when selecting a site for your data center:

- Power supply
- IP connection

Selection of a data center location must of course also include a consideration of general economic conditions, available resources and requirements of physical security. These last should include:

- Potential risks due to activities carried out by neighboring companies
- Risks due to natural hazards (water, storms, lightning, earthquakes)
- Protection from sabotage

2.5.1 External Planning Support

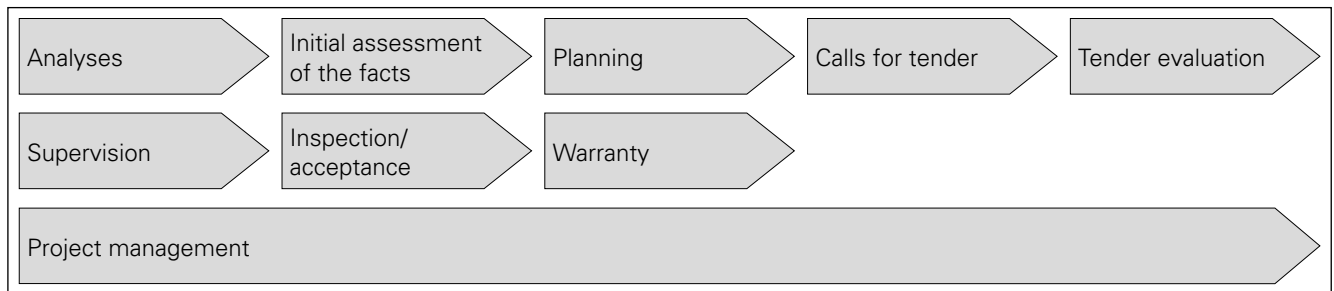
Planners and consultants are frequently brought into the planning process too late. Companies are often of the belief that server parks, phone systems and complex information systems can be realized without the help of specialized planners, or at least without professional consultants. The industry-wide experience these specialists bring to the table makes it possible for data center planner to avoid and/or resolve a number of deficiencies and risks before they arise. It is therefore advisable that external partners providing support in the planning process themselves be evaluated at an early stage.

A perfect flow of communication between all project members is another requirement for project success; these parties must all speak the "same language". As a result, the project leader must act as a focal point to tie together and integrate all the different area heads and trade groups. These parties include:

- Management
- IT and infrastructure experts
- Electrical and climate control engineers
- Supply technicians
- Architects
- Safety experts
- Network specialists, etc.

Consultants should meet with all project members to help them work out analyses and later requirements and technical specifications. This especially includes management, the IT department and infrastructure experts.

The conventional responsibilities of a data center planner include the following:



In Switzerland, offers for planning work are generally submitted in accordance with SIA guidelines (Swiss Engineer and Architects Association), and those in Germany in accordance with the HOAI (Fees Regulations for Architects and Engineers).

The demand for data center planners is constantly increasing, and the industry continues to show growth. Every planner brings a very different portfolio of services; they range from general contractors, who provide all services from planning up to final completion of the data center, up to experts who specialize in specific sub-tasks, as well as trade groups. The best way for a company to select the right planner is to focus on their own particular ideas and requirements, or the specific needs of the client. Companies are sometimes able to build upon their own experiences, in which case they might only need to invite certain trade groups to tender, or engage an expert assessor for quality assurance purposes.

2.5.2 Further Considerations for Planning

As data centers are often installed within the structure of a corporation, campus, production facility or building, areas in planning that go beyond mere infrastructure planning are gaining in importance. Such fields include structured building cabling as well as application-neutral communications cabling (also see EN 50173, EN 50173-5 and EN 50174).

These integration tasks are often still not entrusted to data center planners. Experts estimate that more than 70% of all IT failures are based on faults in the cabling system infrastructure. Internal and external network are being required to transport increasing amounts of data. As a result, it is all the more essential for planners not to ignore how a data center is linked to the rest of the networked world.

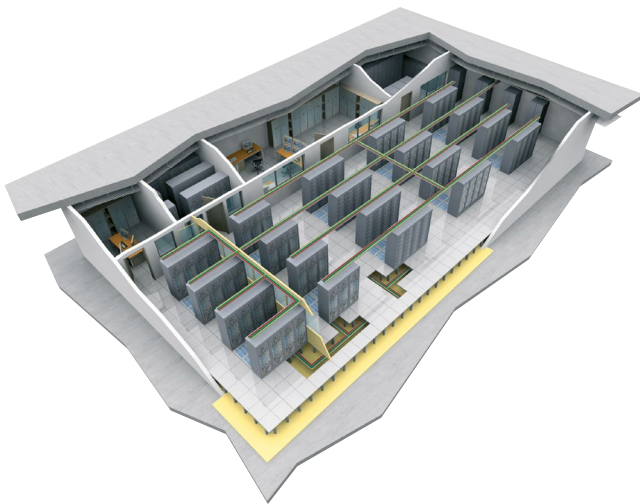
From a data center standpoint, the following issues are essential to include in network planning:

- Security, availability
- Energy consumption, energy efficiency
- Redundancy
- Installation and maintenance efforts and/or costs
- Delivery times
- Flexibility for changes
- Productivity

3. Data Center Infrastructure

The requirements for planning and operating a data center involve a number of different areas. The purpose of this section is to provide an overview of the relevant standards and prevailing technologies. We will start our discussion from the outside then work our way in: From rooms and spatial conditions to data center layouts, infrastructures and zones and finally up to hierarchies and components. This section will also cover communication protocols and media as well as topics on hardware and virtualization. Finally, for the purpose of providing planners, operators and managers with an overall view of the topic of infrastructure, we also provide an introduction to current and upcoming cabling architectures and LAN technologies. We pay special attention to the upcoming evolution from 10 Gigabit Ethernet to 40/100 Gigabit Ethernet that is expected over the next few years, a development that requires a long-term perspective and well-thought-out planning, primarily in the area of glass fiber cabling. This handbook includes a few proven migration paths that will allow this upgrade to be carried out smoothly.

3.1 Standards for Data Centers



Because of trends like cloud computing and virtualization and the increasing tendency of companies to outsource data center operations, requirements in terms of space are growing more complex. Functions must be defined and assigned to separate rooms. This leads to room structures that must be specially designed.

A typical data center is divided into an access area, computer room and work area for administrators. UPS batteries, emergency power generators and the cooling system are each located in separate rooms. Areas in the premises must also be made available for access control, video monitoring and alarm systems. And last but not least, sufficient space must be maintained for data cabling. Every area affects other areas. When planning how to divide up space, key goals are always to provide for smooth administration of the data center, to facilitate quick recoveries in the event of system faults, and to make it possible for the data center to be expanded and migrated as necessary – and all this without great administration overhead.

The data center layout, hierarchical structure and individual zones as well as their functions are described in detail below.

3.1.1 Overview of Relevant Standards

National as well as international committees have worked out standards that define data center structures as well as characteristics of the cabling systems that must be furnished for them. The three most important organizations in this area are:

- ISO/IEC (International Organization for Standardization / International Electrotechnical Commission), responsible for developing international standards
- CENELC (*Comité Européen de Normalisation Électrotechnique*), responsible for developing European standards
- ANSI (American National Standards Institute), responsible for developing American standards.

The following bodies of standards relate to data center cabling:

- ISO/IEC 24764
- EN 50173-5
- EN 50600-2-4
- TIA-942-A

Though these four standards focus on different areas, they all center on the structure and performance of cabling systems. Their goal is to provide a flexible, scalable and clearly laid out structure for cabling systems. This will allow for rapid isolation of faults as well as system changes and expansions.

Delimiting Different Standards

These standards take into account the variety of the data center types as well as the demands that are expected to result from future communication protocols and data rates. However, the different standards all treat these requirements, as well as interfaces to other system types, in a different manner. CENELEC will introduce the EN 50600 series as an overall standard in Europe. The Committee is already in the process of working out further standards.

Data center cabling planners must examine a variety of different parameters as a whole. These parameters include: For example space requirements, climate control, power consumption, redundancy, failure safety and access control. It is recommended that the different bodies of standards be applied as required and as they are appropriate to the given purpose at hand.

The following table provides an overview of the most important parameters covered by the relevant standards, as well as their areas of focus.

Criteria	ISO/IEC 24764	EN 50173-5	TIA-942-A
Structure	✓	✓	✓
Cabling performance	✓	✓	✓
Redundancy	✓	✓	✓
Grounding/equipotential bonding	IEC 60364-1	EN 50310	TIA-607-B
Tier classification	✗	✗	✓
Cable routing	IEC 14763-2 ¹⁾	EN 50174-2 /A1	✓ ²⁾
Ceilings and double floors	IEC 14763-2 ¹⁾	EN 50174-2 /A1	✓ ⁶⁾
Floor load	✗	✗	✓
Space requirements (ceiling height, door width)	IEC 14763-2 ¹⁾	EN 50174-2 /A1 ³⁾	✓
Power supply / UPS	✗	✗	✓
Fire protection/safety		EN 50174-2 /A1 ⁴⁾	✓ ⁴⁾
Cooling	✗	✗	✓
Lighting	✗	✗	✓
Administration/labeling	IEC 14763-1 ⁵⁾	EN 50174-2 /A1 ⁵⁾	TIA-606-B
Temperature / humidity	✗	✗	✓

¹⁾ not data center-specific, ²⁾ cable separation is covered in TIA-569-C, ³⁾ door widths and ceiling height only,

⁴⁾ refers to local standards, ⁵⁾ refers to complexity level, ⁶⁾ refers to TIA-569

TIA-942-A is the standard that focuses most consistently on the data center world. ISO/IEC and EN are more general, and work with additional documentation for key terms and concepts and their descriptions. Sections of IEC documents no longer describe the latest state of technology and also use different terminology.

The terms used below are either from the ISO, as the organization with an international scope, or, in the event the ISO offers no equivalent terms, from ANSI.

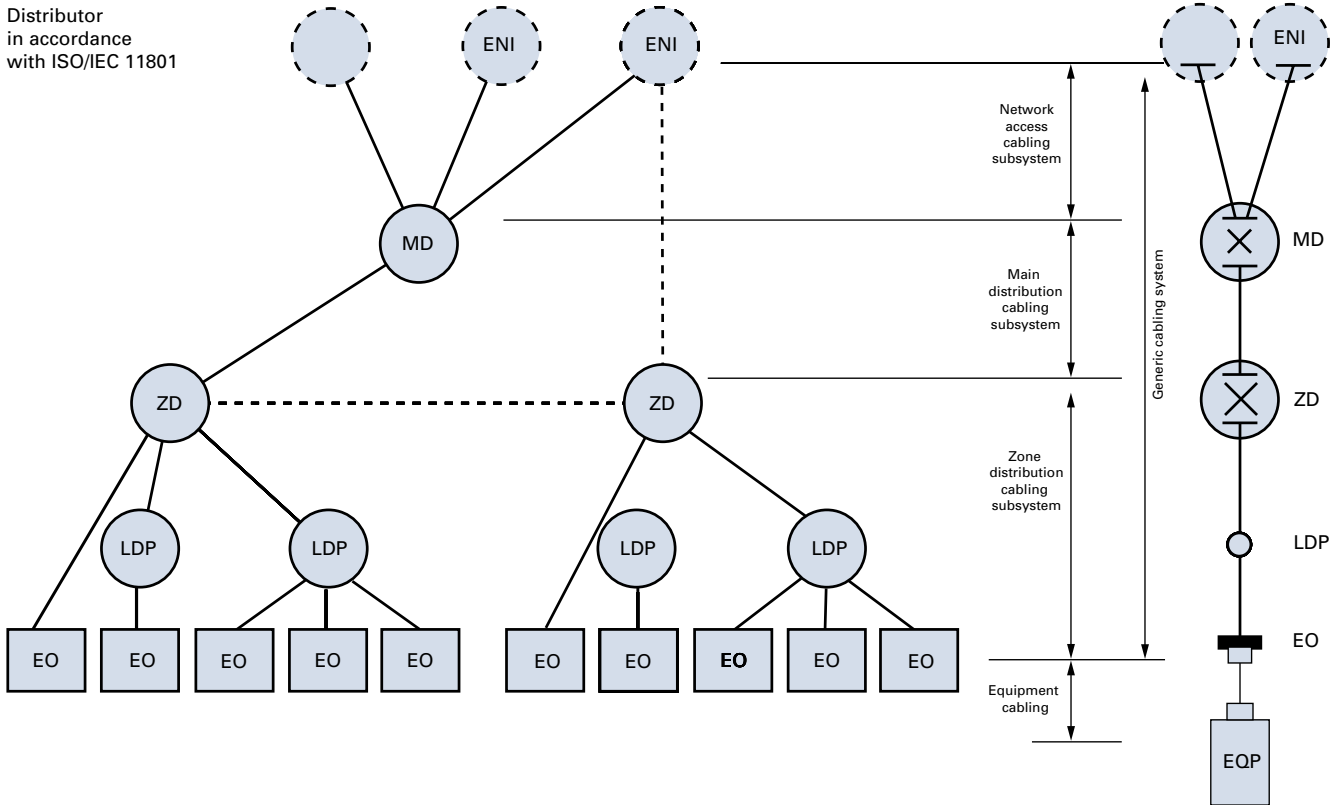
3.1.2 ISO/IEC 24764

Installations implemented in accordance with ISO/IEC 24764 require compliance with the following standards:

- Configuration and structure in accordance with ISO/IEC 24764 and/or ISO 11801
- Copper cabling tests as defined under IEC 61935-1
- Glass fiber cabling tests as defined under IEC 14763-3
- Quality plan and installation guidelines as defined under IEC 14763-2

IEC 14763-2 makes reference to ISO/IEC 18010 in matters of cable routing. This standard not only contains descriptions for cable routing, but also various information on failure safety measures. Note, however, that data center requirements are not explicitly covered in either IEC 14763-2 or ISO/IEC 18010

The tree structure concept, that makes use of a single central distributor, determines the structure of the cabling system. This concept allows for point-to-point connections in exceptional cases, when active devices in the immediate vicinity are arranged together or when communication via a structured cabling setup is impossible. The cabling systems in a local ISO 11801 distributor and at the interface to external networks are not considered part of this structure.



ENI: External Network Interface MD: Main Distributor ZD: Zone Distributor
 LDP: Local Distribution Point EO: Equipment Outlet EQP: Equipment

Section 3.2 describes the data center layout as well as its individual zones and their functions.

The concept of spatial separation of the different areas of the data center is applied to its layout. The network structure in the data center must be separated from the building cabling system. A separate distributor connects the internal network. This must also be physically separated from the data center. The connection to the external network (ENI) can be established either within the data center or outside of it. All other functional elements should be permanent elements of the data center and should be accessible at all times.

The standard does not cover cabling components, patch cords or connection cables, or distributors of the building network itself.

Planners should note that ISO 11801 und ISO/IEC 24764 use different terminologies, as illustrated in the following table:

ISO/IEC 24764	ISO 11801
External network interface (ENI)	Campus distributor (CD)
Network access cable	Primary cable
Main distributor (MD)	Building distributor (BD)
Main distributor cable	Secondary cable
Area distributor (AD)	Floor distributor (FD)
Area distributor cable	Tertiary/horizontal cable
Local distribution point (LDP)	Collection point (CP)
Local distribution point cable	Collection point cable
Device connection (DC)	IT connection (ITC)

A data center must include at least one main distributor. However, the functions of different distributors may be combined together, depending on the size of the data center. The standard does not explicitly stipulate any requirements with regard to redundancy. However, for purposes of improving failure safety, it does provide information on options for redundant connections, cable paths and distributors. The local distribution point (LVP) should be housed within the ceiling or a raised floor. Patch cabling is not used in this area, since cables are through-connected.

ISO/IEC 24764 makes references to ISO 11801 with regard to matters of performance. The latter standard contains further details on characteristics of transmission links and components. These standards differ in terms of their definitions of the minimum requirements for primary cables and area distributor cables.

Cabling classes for the network access connection correspond to the applications listed in ISO 11801.

Cabling infrastructure:

- Copper cable: Category 6A, category 7, category 7_A
- Copper transmission path: Class E_A, class F, class F_A
- Multi-mode optical fiber cable: OM3, OM4
- Single mode optical fiber cable: OS2

Plug connectors for copper cabling systems:

- IEC 60603-7-51 or IEC 60603-7-41 for category 6_A for shielded and unshielded respectively
- IEC 60603-7-7 or IEC 60603-7-71 for category 7 and 7_A respectively
- IEC 61076-3-104 for category 7 and 7_A

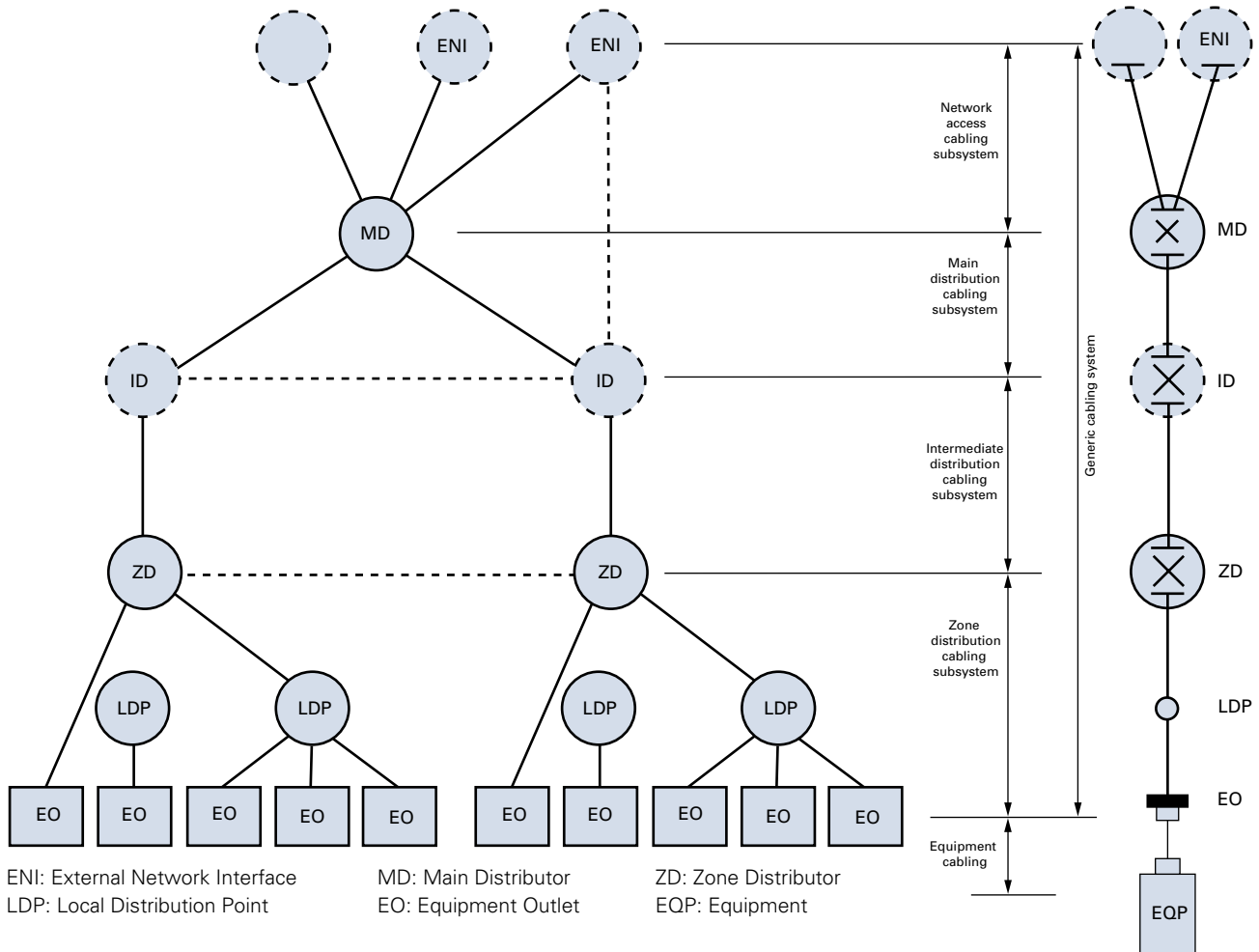
Plug connectors for optical fibers:

- LC duplex per IEC 61754-20 for GA and ENS
- MPO/MTP® multi-fiber connectors per IEC 61754-7 for 12 or 24 fibers

ISO/IEC 24764 makes reference to ISO 14763-2 with regard to issues of multi-fiber connections. Keep in mind here that for the sender and receiver to be connected correctly, connection polarities must be strictly observed.

3.1.3 EN 50173-5

EN 50173-5 shows only minor differences from ISO/IEC 24764. Amendment 2 contains the latest changes. Planner should read EN 50173-5 and EN 50173-5/A2 as well as the other standards in the EN 50173 series. The hierarchical structure defined in EN 50173-1 & -2 also applies in EN 50173-5. One significant enhancement is the amendment is the additional distributors provided for structuring larger data centers.



Section 3.2 contains a detailed description of the data center layout as well as its individual zones and their functions.

A standards-compliant installation must comply with

- The EN 50173 series,
- The EN 50174 series,
- Their respective amendments and
- EN 50310 for earthing and equipotential bonding systems for cabling systems.

Additional information on the following data center topics was added in EN 50174-2/A1:

- Design proposals
- Cable routing
- Separation of power and data cables
- Double floors and ceilings
- Use of pre-assembled cables
- House interconnection point
- Room requirements

In contrast to ISO 11801, EN allows for optical fiber classes of not only OF-300, OF-500 and OF-2000, but also OF-100 through OF-10000. EN 50173-1 and EN 50173-2 establish requirements for cabling performance.

Minimum requirements for data center cabling are also established in these standards. EN 50173-5 provides for a cabling class for the network access connection in accordance with ISO 11801 applications.

3.1.4 EN 50600

EN 50600 was developed to adapt the contents of the TIA-942-A standard to European conditions. CENELEC divides the contents of TIA-942-A over a number of standards. EN 50600-1, as the first part of the series, bears the title: "Information Technology - Data Center Facilities And Infrastructures - Part 1: General Concepts". Its contents include:

- Risk assessment
- Building design
- Classification of data centers

The EN 50600 series is to include the following standards:

EN 50600-2-1	Building construction
EN 50600-2-2	Power distribution
EN 50600-2-3	Environmental control
EN 50600-2-4	Telecommunications cabling infrastructure
EN 50600-2-5	Physical security
EN 50600-2-6	Management and operational information

3.1.5 TIA-942-A

The encompassing body of standards TIA-942-A lays the foundations not only for cabling, but also for the building to house the data center, selection of the surrounding area and the geographic location, and more. One important building block is the availability classes, or "Tiers", defined in the body (see section 2.2.1). Planners and operators should also take note of addenda TIA-942-1 and TIA-942-2.

TIA-607-B covers topics of grounding and equipotential bonding. TIA-606-B describes administration. TIA- 569-C describes measures for separating telecommunications cables and power cabling. Cabling is the common theme that runs throughout all the data center standards listed above. TIA-942-A makes reference to the EIA/TIA-568 series for performance-related issues; here, minimum requirements for cabling system performance capacity were adapted to ISO/IEC 24764 and EN 50173-5.

TIA provides for an intermediate distributor between the MDA (main distribution area) and HDA (horizontal distribution area). If data center plans include a second entrance room, the cabling system will be better structured through use of an IDA (intermediate distribution area).

Delimitation of TIA from ISO/IEC:

- In TIA-942, the interface to the external network exists outside of the computer room.
- ISO/IEC 24764 and EN 50173-5 set stricter boundary values for category 6A ($\neq 6A$).
- The application determines the length of the fiber optic cable.

In addition, TIA-942-A establishes the following criteria for data center cabling:

Cabling infrastructure:

- Copper cable: Category 6 – 6A
- Copper transmission path: Category 3 – category 6A (category 6A is recommended; TIA is not aware of classes)
- Multi-mode optical fiber cable: OM3, OM4 (OM4 recommended)
- Single-mode optical fiber cable: 9/125 μm , OS2
- Coaxial cables: 75 ohm

Plug connectors for copper cabling systems:

- ANSI/TIA/EIA-568-B.2

Plug connectors for optical fibers:

- LC duplex per TIA -604-10 (for ≤ 2 fibers)
- MPO/MTP[®] multi-fiber connectors per TIA-604-5 (for ≥ 2 fibers)

Summary

Since no standard is complete in itself, all relevant standards should be consulted as the planning process begins. The most demanding and most advanced standard should then be used, in light of the given requirements and the technical area under development. Example: In the case of cabling performance, the standard with the highest performance requirements for cabling components should be used as a basis for planning. The same applies for other parameters.

Recommendation:

The relevant standard should be listed in the technical specifications in order to ensure requirements are clearly defined!

3.2 Laying Out Data Centers

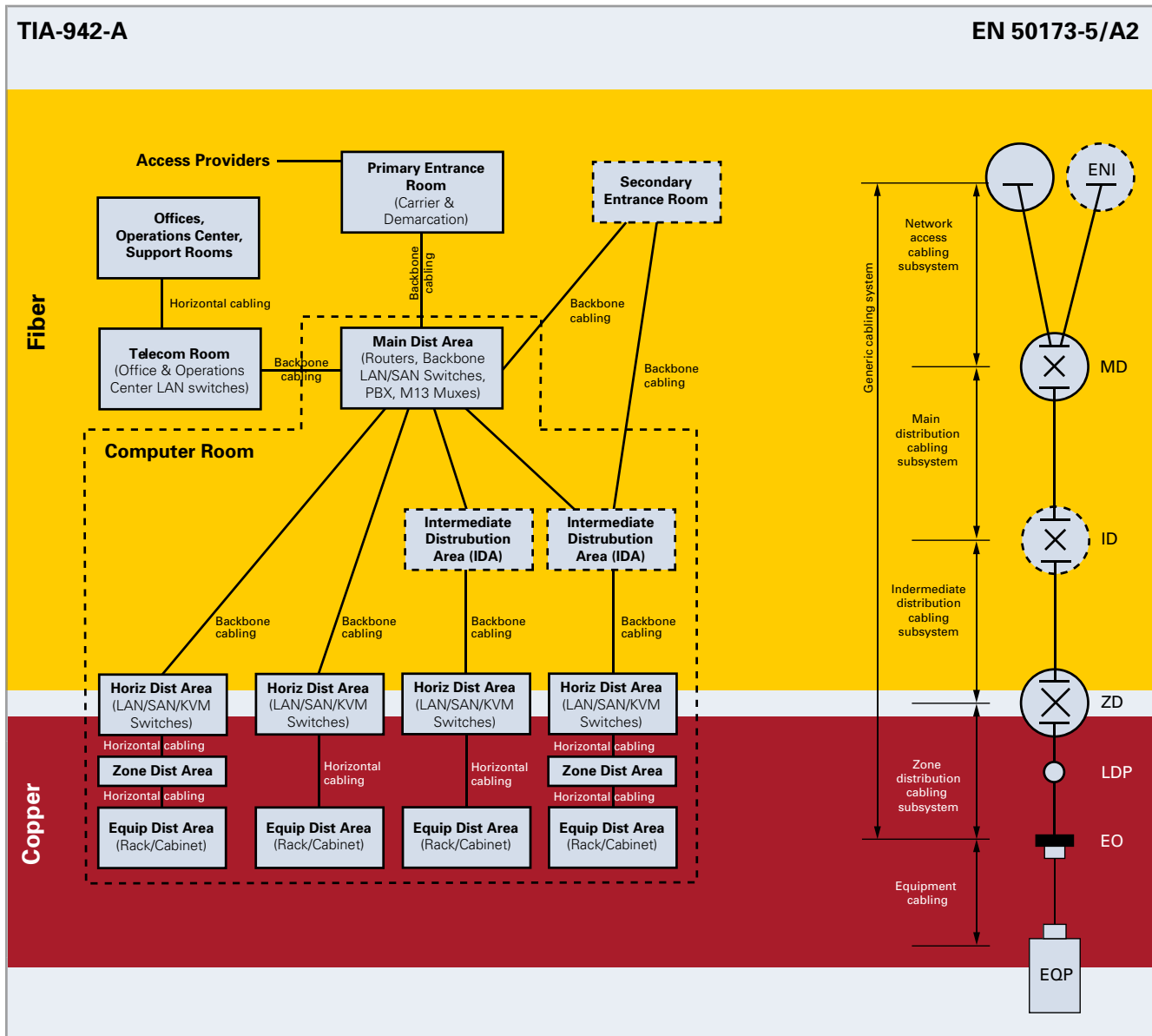
Data centers that have already been installed are still not spared from current developments in technology. Just trends toward cloud computing, virtualization and outsourcing as well as rising needs for bandwidth, performance and storage volumes make multiple re-designs of data centers over the medium term necessary. Basic rules that specify data center layout provide invaluable support in the development of appropriate layout concepts.

3.2.1 International Standards

International standards on data center cabling differ from their European counterparts due to their areas of focus (also see section 3.1). One important thing to note is that the terms used to describe functional elements differ between international standards and European standards. A comparison of these terms appears in the following table:

ISO/IEC 24764	ISO 11801	TIA-942-A
External Network Interface (ENI)	Campus Distributor (CD)	ENI (External Network Interface) ER (Entrance Room)
Network Access Cable	Primary Cable	Backbone Cabling
Main Distributor (MD)	Building Distributor (BD)	MC (Main Cross Connect) MDA (Main Distribution Area)
Main Distributor Cable	Secondary Cable	Backbone Cabling IC (Intermediate Cross Connect) IDA (IntermediateDistributionArea)
Area Distributor (AD)	Floor Distributor (FD)	HC (Horizontal Cross Connect) HDA (Horizontal Distribution Area)
Area Distributor Cable	Tertiary/Horizontal Cable	Horizontal Cabling
Local Distribution Point (LDP)	Collection Point (CP)	CP* (Consolidation Point) ZDA (Zone Distribution Area)
Local Distribution Point Cable	Collection Point Cable	Horizontal Cabling
Device Connection (CA)	IT Connection (ITC)	EO (Equipment Outlet) EDA (Equipment Distribution Area)

CP* = LDP (Local Distribution Point)



Functions are assigned to rooms. Note, however, that TIA-942-A focuses on the areas of the data center and not its functions. However, the topology on which that standard is based is the same as that in ISO/IEC 24764 and in EN 50173-5. The individual areas of a data center are assigned the following functions:

- **Entrance Room:** Entrance area to the data center network. Access to the public network (Internet provider) is established at this point. This access may be a redundant connection, depending upon the "Tier" level. In smaller networks, the External Network Interface can be connected directly to the Horizontal Distribution Area (Area Distributor).
- **Main Distribution Area:** This is the core of the data center. It should be made secure through the implementation of redundant connections and components. Also known as **Core Layer**, since all data traffic is managed from this point. The **Aggregation Layer** (or Distribution Layer) is part of this layer. It forwards bundled data traffic from the access layer on to the core, via aggregation/distribution switches.
- **Intermediate Distribution Area:** An IDA can be used to structure the MDA and HDA (main/horizontal distribution area) in larger data centers. Network operation may be interrupted. A second entrance room can be connected directly for purposes of redundancy.
- **Horizontal Distribution Area** This area in the network is known as the **Access Layer**. Data traffic from access switches is passed to the aggregation layer between the backbone and horizontal cabling in the HDA.

- **Zone Distribution Area:** Used for intermediate distribution outside the **Equipment Distribution Area**. Is implemented for reasons of space, and placed in the double floor, for example. The Raised Floor Solution from R&M that was developed for this purpose provides up to 288 connections per box in a double floor segment format. It is freely configurable, thanks to its modular design concept.
- **Telecom Room:** Room for connection to the internal network.
- **Operation Center, Support Room** and **Offices** are available as work rooms for data center personnel.

Cable type selection is a critical factor in determining the ability of the data center cabling system to grow with future needs. Definitions therefore exist both for possible communication protocols and the corresponding maximum transmission rates (see section 3.8) for various cable types. Fiber optic cable is usually the preferred medium for backbone cabling, while copper cable is used for horizontal cabling. Transmission media are described in greater detail in section 3.9.

Selection of the cabling architecture determines a number of factors, including scalability of the data center. It affects both network availability as well as rack arrangement. Section 3.4 describes typical cabling architectures such as "End of Row" and "Top of Rack" in greater detail, as well as their advantages and disadvantages. Additional designs for the physical infrastructure of a data center are described in section 3.5.

3.2.2 Room Concepts

The layout of a data center can be based on a number of different room concepts. The room-in-room concept separates equipment rooms from IT security rooms. This concept includes double floors, a suspended ceiling if necessary, active and passive fire protection and a cooling system.



A module container concept is based on the use of high cube containers. The systems for climate control and power are housed in separate containers. Servers, storage devices and network equipment are housed in an IT container.

The data center, including its own block heating and generating plant, represents a mobile, self-contained outdoor infrastructure.

A mini-data center is a compact, automated data center. A complete, fully redundant data center, including its infrastructure with high-performance servers, is contained within a single housing unit. Because of its high power densities, this platform is especially suitable for private cloud computing.

3.2.3 Security Zones

Data center security comprises data in addition to systems and processes. A primary task for security concepts is to provide for early risk detection and evaluation. This means that the security concept must implement measures that ensure an enterprise remains operational.

Room concepts have a big effect on physical security: Appropriate selection of locations for functional IT areas and assignment of functions to rooms can reduce or even eliminate security risks.

Issue of Location and Functional Areas

A company's data backup concept is key, as it also represents the starting point for designing its IT infrastructure, IT functions and their physical locations, performance and availability. An optimal location for a data center will also take into consideration a company's data backup concept.

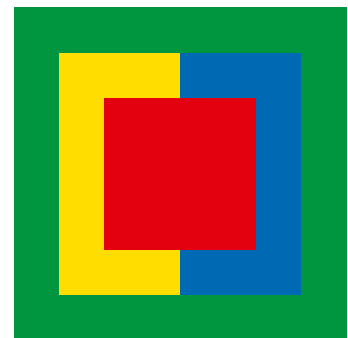
The following criteria are relevant to the physical security of a data center location:

- Adjacent areas or functions and neighboring uses should not involve risk.
- Media lines, supply lines, building tremors or chemicals should be eliminated in order to ensure the physical security of IT systems.
- Natural hazards (water, storms, lightning, earthquakes) should be eliminated or averted. Planning must take into consideration the particular features specific to the given region.
- Installation of the data center as a separate, independent functional area.
- Selection of a "protected" location to provide protection from sabotage.
- The social position of the company should be examined with regard to potential risks.

Risks can be eliminated and costs minimized in the design phase. This phase must therefore include an examination of all risk factors as well as company-specific framework conditions.

Planners and operators should have already come to a decision on the arrangement of the different functional areas of the data center by the time design and planning begins. Requirements of security for each data center function as well as their significance for functional IT integrity are the deciding criteria in this regard. Division of functional areas:

Security Zones	Function	Marking (example)
1	Site	White
2	Semi-public area, adjacent office spaces	Green
3	Operating areas, auxiliary rooms for IT	Yellow
4	Technical systems for IT operation	Blue
5	IT and network infrastructure	Red



Arrangement of Security Zones

The graphic to the right depicts the schematic arrangement of security zones. The IT area (red) is housed in the center of the site. The adjacent zones 3 and 4 (yellow/blue) protect the interior section. Security zones 1 and 2 (white/green) serve as an outer protective layer.

Strict access control must be provided for sensitive areas to provide protection from sabotage and for similar purposes. So, for example, a maintenance technician for air conditioning systems should only have access to the technical areas (blue) and not to the IT area (red).

IT infrastructure security and availability can only be achieved if one single overall security concept exists. This concept should describe the locations for the different functional areas of the data center, and also establish the necessary security zones.

3.3 Network Hierarchy

In order to optimize network administration, scalability and performance, these tasks are divided up into smaller functions. This results in a modular network design. Defined functions are contained in discrete layers. The network is thus presented as a hierarchical design sub-divided into individual layers.

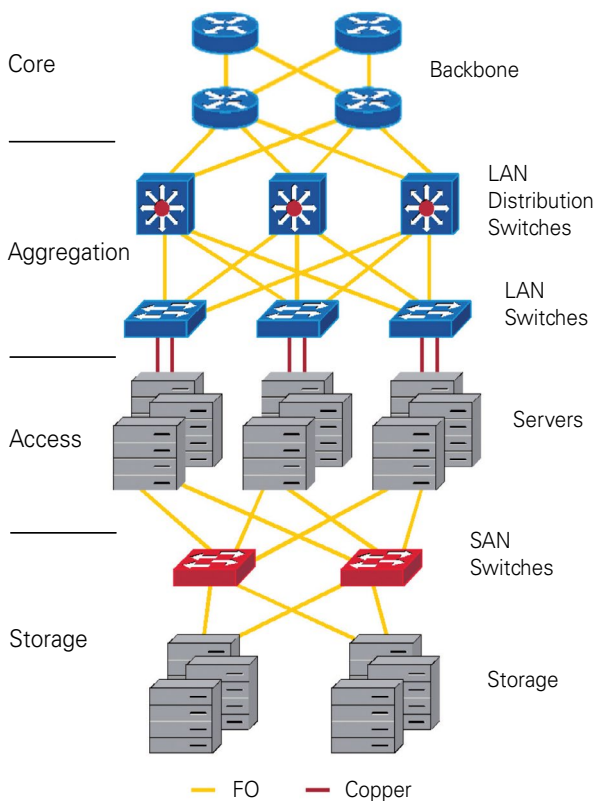
3.3.1 Two & Three Tier Networks

Three-tier networks consist of:

- An access/storage layer: This layer includes switches for desktop computers, servers and storage resources.
- Aggregation/distribution layer: Switches combine streams of data from the access layer and protect these with components such as firewalls
- Core switch layer: Regulates the traffic in the backbone

The European and American standards for physical cabling structures in data centers use the following terms for these logical layers:

Logical architecture	EN 50173-5	TIA-942-A
Core & Aggregation Layer	Main Distributor (MD)	Main Distribution Area (MDA)
Aggregation Layer	Zone Distributor (ZD)	Horizontal Distribution Area (HDA)
Access & Storage Layer	Local Distribution Point (LDP)	Zone Distribution Area (ZDA)
	Equipment Outlet (EO)	Equipment Distribution Area (EDA)



Today's three-tier networks extend the capacity of conventional two-tier networks. They implement an additional bundling (aggregation) layer for this purpose. The spanning tree protocol (STP) manages switching traffic. The IETF (Internet Engineering Task Force) has introduced the so-called TRILL protocol (Transport of Information over Lots of Links) as a replacement for STP, though the new protocol still covers STP. TRILL was introduced to make use of layer 2 connections more effective.

Section 3.8.6 contains a detailed description of network protocols for redundant paths.

Though multi-layer networking concepts have been developed for static applications, today's dynamic applications and data traffic patterns require additional developments. For example, the current trend of server virtualization results in network data traffic that has a number of different facets and is more complex than it was previously.

A flat architecture can replace or extend conventional concepts, this solution is implemented as a fabric of equal nodes. Additional cross-connections can then be added between nodes in to the fabric to increase performance. Section 3.3.6 describes various data center network fabrics and dynamic processes for their implementation.

A dramatic increase in the performance of virtualized servers was achieved through the systematic implementation of SR-IOV (single root I/O virtualization). This technology allowed potential I/O performances of 20 to 30 Gbit/s to be achieved. Server blades that have the ability to support this technology must also be equipped with 2 x 10 GbE connections for them to make use of their full potential. Since blade systems can support up to 8 blade servers, this means planners must provide for 100 GbE network connections.

Up to this point, the performance required for the next highest layer in the hierarchy could be easily achieved through 10 GbE connections or aggregation through multiple connections. Servers just had to be fitted with 1 GbE LAN interfaces, and could be connected to top-of-rack switches over 1 Gbit/s. These days, however, congestion in uplink ports can quickly result given server performance increases to 10 Gbit/s and aggregation processes running in blade systems and transmitting in the core direction with 40 or 100 Gbit/s. This problem is solved with two-tier concepts. The two-tier architectural approach also reduces latency times, since data traffic flows through fewer switches (see section 3.3.5). When virtualization is implemented with blade servers or rack servers, the servers themselves are responsible for access switching functions.

Low latency times are absolutely essential for modern real-time applications such as voice over IP (VoIP), unified communication (UC), video conferencing, video on demand (VoD) and high frequency trading. These applications must support broadcast, multi-cast and unicast traffic and therefore require calculable performance as well as a defined quality of service (QoS). And other technologies like cloud computing and virtualized data center require an end-to-end delay of less than 10 microseconds.

3.3.2 Access Layer

The access layer is responsible for establishing the connection to terminal devices and access to the rest of the network. This layer consists of routers, switches, bridges, hubs and wireless access points for wireless LAN.

The access layer manages device connections as well as communication between network devices. Demands made of the LAN switches in this layer, often called edge switches, include port security, VLANs, Power over Ethernet (PoE) and other necessary functionalities.

Access switches may be stacked into one virtual switch. One master unit then manages and configures the stack as one object.

Low latency switches provide one solution for I/O consolidation in the access layer, and simplify tasks of cabling and management. In addition, these components lower power consumption and regular costs. These switches even support the use of Fiber Channel over Ethernet (FCoE), thus allowing for creation of a data center fabric. A data center fabric is a platform that manages server and storage network together in a unified manner, a key requirement for virtualization.



Product example from Cisco

3.3.3 Aggregation/Distribution Layer

The aggregation layer or distribution layer receives data from access layer switches, combines them together and passes them on to the core layer. The data are then delivered to their final destinations from that point.

The routing functions between VLANs (virtual LANs) are defined in the access layer. Routing is performed in the aggregation layer since aggregation switches possess higher processing capacity rates than access layer switches. In so doing, that layer also manages network data on the basis of defined guidelines. The layer is also responsible for mapping broadcast domains. Aggregation switches assume routing functions for core switches as well.

VLANs use a switch to distribute data over different subnetworks (subnets). This allows the data in a single company to be distributed to its individual departments.

Aggregation switches are also responsible for managing ACLs (access control lists). An ACL defines the data types that are to be permitted or rejected by a switch, and thus allows for control of the communication between network devices. Since a switch must check each individual packet to see whether it meets one of the ACL rules defined on the switch, ACL functions are extremely processor-intensive. As such, ACL functions are carried out on the aggregation layer since this layer already has the necessary processing capacities. Administrative overhead is lower in the aggregation layer.

Combining data lines together is an ideal solution for preventing bottlenecks. This process is important just in the aggregation layer alone. Combining multiple switch ports together increases data throughput by a multiple factor (e.g. $8 \times 10 \text{ Gbit/s} = 80 \text{ Gbit/s}$). This combining process is also known as link aggregation (IEEE 802.1ax). By contrast, the manufacturer Cisco Systems uses the term EtherChannel, while some other providers call the process trunking.

The high load on aggregation switches is the result of the many functions these components must provide. Failure of an aggregation switch has significant consequences for the network and especially the access layer. Because of their importance to the network, aggregation switches should always be installed redundantly, so as to ensure the network remains 100% available. Switches that operate using redundant, hot swappable power supplies are a good option for this implementation.

Aggregation switches must be able to support quality of service (QoS). This allows data arriving at QoS-capable access switches to be managed on the basis of defined priorities.



Product example from Cisco

3.3.4 Core Layer

The core layer is the backbone of the network. Demands of high availability and redundancy are naturally much higher at this level. This layer must ensure connectivity between all the devices on the aggregation layer. Since the core layer combines together the data from all aggregation devices, it needs to transport large volumes of data at higher speeds. The core layer can also be connected directly to Internet resources. In smaller networks, the aggregation and core layers can be bundled into one layer (reduced core model).

A high forwarding rate is a key criterion when selecting core switches. Core switches must support link aggregation so that they have the ability to provide aggregation switches with sufficient bandwidth. Ideally, the fans used at the core layer are hot swappable. Due to the higher demands made on them, core switches tend to run at higher operating temperatures and as such must be continuously cooled down.

As with other components, the issue of quality of service (QoS) is an important factor in the selection of core switches as well. Core switches can be a big factor in a company's ability to make cost-effective, varied and optimal use of available bandwidth. This is one way of avoiding the high bandwidth expense associated with accessing high-speed WANs. Higher QoS guarantees should be given for business-critical and time-critical data such as back-up data and voice services than for less critical data like e-mail.



Product example from Cisco

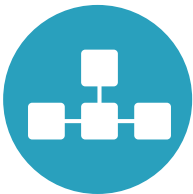
3.3.5 Advantages of Hierarchical Networks

The advantages of a hierarchical network design lie in its

- Scalability
- Performance
- Ease of administration
- Redundancy
- Security
- Maintainability

The ease of maintenance of hierarchical networks results from their modularity and scalability. In certain other network topologies, maintenance expense increases along with the size of the network. Growth is also limited in other network design models.

A hierarchical model allows the switches for each layer to be easily selected on the basis of their functions. However, this can lead to bottlenecks in other layers in the case where additional switches were added to a given layer. Switch functions should be selected so they are appropriate for the given layer. So, for example, more cost-effective switches can be implemented in the access layer than in the aggregation or core layers. By contrast, in a completely meshed topology, it must be possible for every switch to carry out all functions. In other words, this topology requires that high-performance components be implemented everywhere.



A key parameter for planning is network diameter. This refers to the number of devices that a data packet must pass in order to reach its recipient. The larger the number of stations or switches, the larger the diameter of the network, and the more critical latency becomes. Latency is understood to mean the time a network device requires processing a packet or a frame. This process lasts for only fractions of a second, but summed over a large number of legs in the path of the data transfer, the effect will lead to noticeable delays.

The performance capability of switches must be examined in a differentiated manner. Large volumes of data for server/server data and client/server data are routed over data center switches. These components must show significantly higher performance than switches for terminal devices. Active network components are described in greater detail in section 3.6.

Up to this point, a variety of needs-based, installed high-speed technologies have been used for network architectures in data centers. For example, memory traffic (SAN) runs over Fiber Channel (FC), client-server communication over Ethernet and server-server communication over InfiniBand. 10 gigabit Ethernet technology can replace concepts like these. It also paves the way to use of 40/100 gigabit Ethernet, which can be used in both the core and aggregation layers and also in top of rack switches.

Ethernet technology is described in greater detail in section 3.8.2, and the related migration process in section 3.10.2.

3.3.6 Data Center Fabrics

The dynamic load distribution process used in virtualized environments and cloud environments automatically distributes virtual servers over a number of different hosts. This results in a load configuration that can overtax networks based on conventional structures. This is because in some cases data communication between virtual machines travels constantly over multiple networks nodes and layers. One solution to this problem is to slowly start replacing conventional north-south architectures (vertical communication) with east-west architectures (horizontal communication).

This goal can be achieved through the use of data center fabrics. This will allow established three-layer networks to be eliminated and in turn allow for implementation of a simplified network model. A network of this type is also easier to manage. This new model can be viewed as one single, very large switch. This switch, however, is not actually installed physically but modeled logically.

All devices connected to the network are assigned the logical switch as a single access point through which system communication runs. This means it is no longer relevant on what physical host a virtual machine runs, or whether the virtual machine is moved onto a different host. The server always communicates with its partners over the one node, both before and after the migration. Using this approach for network design allows operators and planners to go forward with a virtualization concept that supports dynamic load distribution.

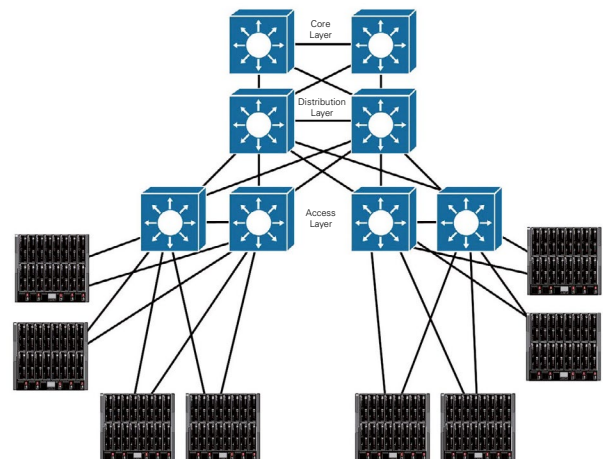
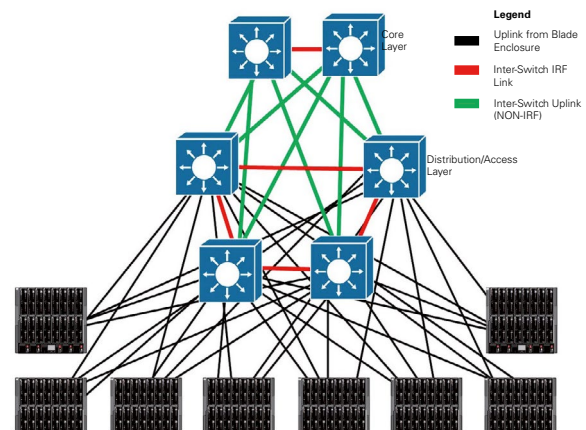
Another advantage of combining components into a single logical object in this way lies in its simplified management. The switch is configured only over a single interface and at a single location. All switches that are combined together can be reached through a single administration access point. This greatly simplifies network analysis, querying of statuses and monitoring.

In addition, a single fabric is easier to scale. If you need more ports, you just add another fabric switch, which then adds itself into the existing combine of switches and is automatically configured from the top-level fabric.

Network virtualization and IRF (intelligent resilient framework) technologies significantly improve the availability of high-performance data center networks. The IRF technology creates a resilient virtual switch fabric (RVSF) that provides a high 99.999% level of availability as well as transparent redundancy. As a result, IRF can be used to virtualize multiple switches which then run as a single switch. This simplifies the overall network architecture, since an aggregation layer is no longer required.

Special features of IRF include:

- Part of the switch operating system (Comware)
- HPN switch virtualization platform for all network layers (core/distribution/edge)
- Stacking solution
- Uses regular Ethernet connections
- Implemented only partially over HPN products



www.insearchoftech.com

The following manufacturers have put fabric solutions for network virtualization on the market:

- Avaya, Virtual Services Platform (VSP)
- Brocade, Virtual Cluster Switching (VCS)
- Cisco, Unified Computing System
- Extreme Networks, Open Fabric
- Juniper, QFabric

A common characteristic shared by all these solutions is the dynamic network connections they provide. Communication paths are configured in the data center fabric.

3.3.7 Software Defined Networking

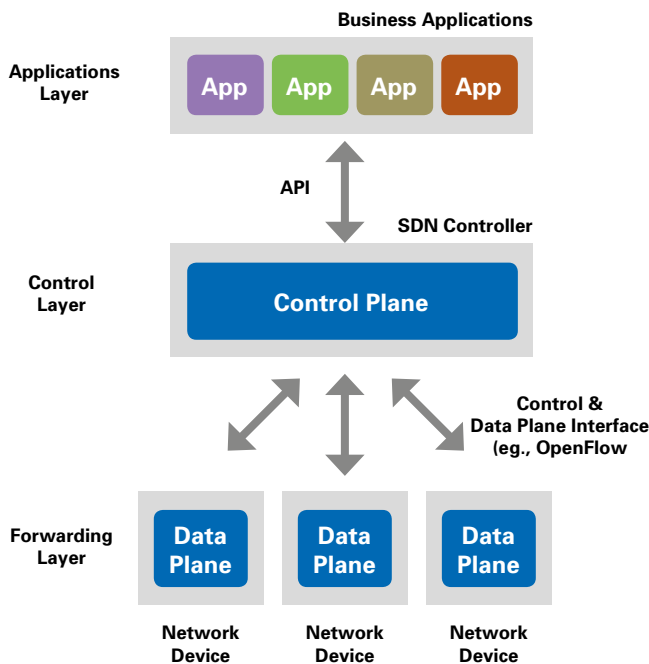
Software-defined networking (SDN) is a new model which provides for flexible packet control within a network. SDN's distinguishing feature lies in its separation of control and data paths – in other words, separation of the control plane from the data plane.

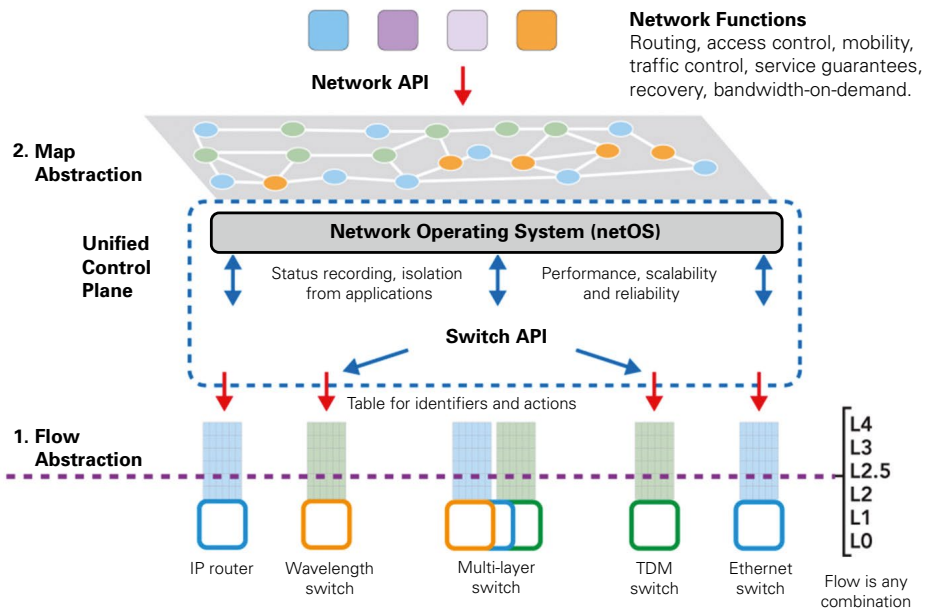
The control plane is responsible for configuring switches and routers and programming data paths. SDN moves the control plane into a separate system, so to speak, i.e. the SDN controller. This process also makes it possible to implement flexible tables, so-called flow tables.

This results in a single point of management for the entire infrastructure, with the controller regulating traffic in the entire network. The SDN controller can be installed as a physical server, virtual machine or hardware appliance. It specifies how the data plane is to handle data packets (priorities, destination ports, etc.).

The data plane in turn forwards these rules onto the application-specific integrated circuits in the switch or router. Software defined networking therefore separates out the decisions which affect the routing of packets and rules (policies) from the network topology and transport layer.

The controller and data plane communicate primarily via OpenFlow, a special protocol developed at Stanford University in California. Standardized application programming interfaces (APIs) provide a method for linking applications together. So that the switches and routers in an SDN infrastructure can understand the OpenFlow used by the SDN controller, new systems that provide the appropriate interfaces must be implemented if necessary.





Source:
Stanford University

All established switch manufacturers are working to upgrade their SDN-capable switches. However, some manufacturers like Cisco Systems are using proprietary approaches: Its Open Network Environment platform (Cisco ONE) includes APIs, agents, controllers and components for overlay networks.

Conclusion

Software defined networking offers a high degree of flexibility as well as improved options for adapting network infrastructures to special application requirements, such as bandwidths or quality-of-service parameters. This flexibility is extremely important in private clouds or hybrid clouds as well as growth-oriented data centers. However, SDN must first prove its advantages and manageability in more complex installations. In addition, the range of devices that support OpenFlow must grow.

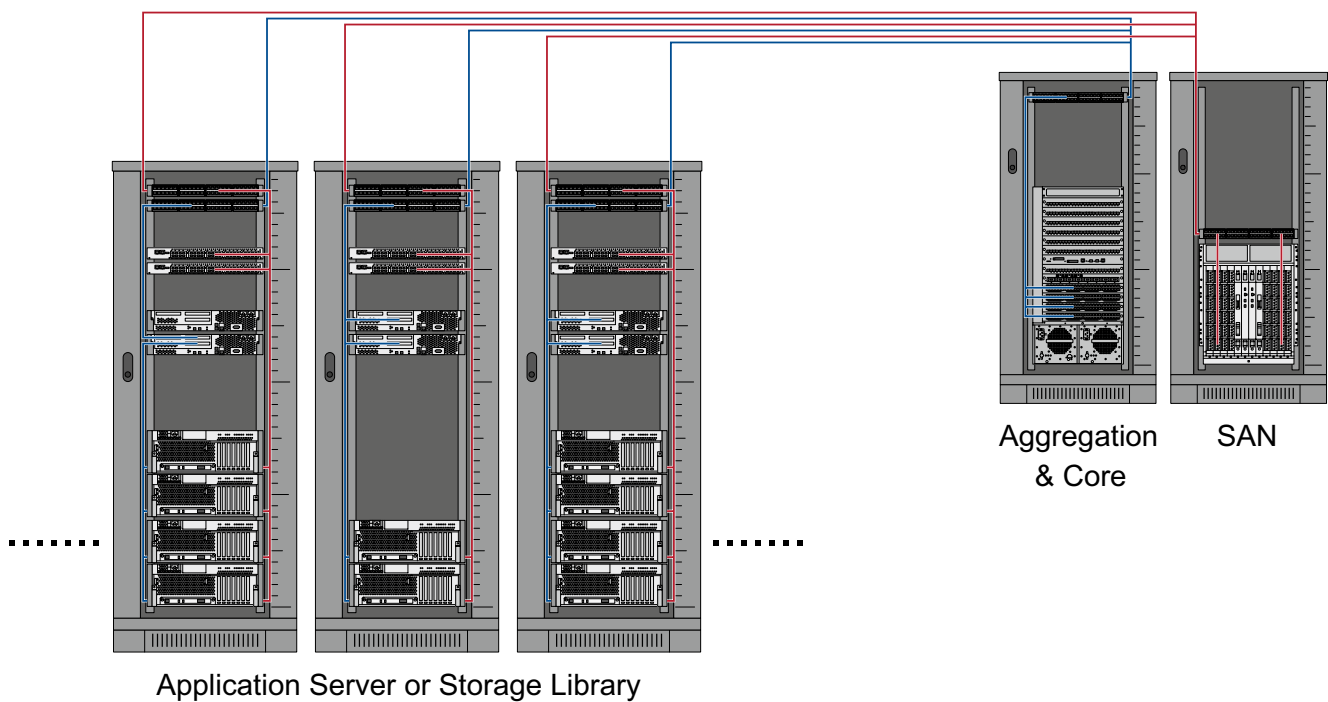
3.4 Cabling Architecture in Data Centers

A number of cabling architectures are available for selection when planning a data center. The purpose of this section is to present the most important concepts in this area – top of rack, end of row and middle of row. Each server in all these concepts is normally integrated using three ports, 1 for the LAN, 1 for the SAN and 1 for KVM. In the event redundancy is required, a total of five connections must be provided, i.e. 1 additional port for both LAN and SAN. The technologies and media used for these connections are typically:

- **LAN:** Ethernet over copper or fiber optic cables (1/10/40/100 Gigabit)
- **SAN:** Fiber Channel (FC) over fiber optic, or Ethernet-based over fiber optic or copper cables
- **KVM:** Keyboard/video/mouse signal transmission over copper cables

3.4.1 Top of Rack (ToR)

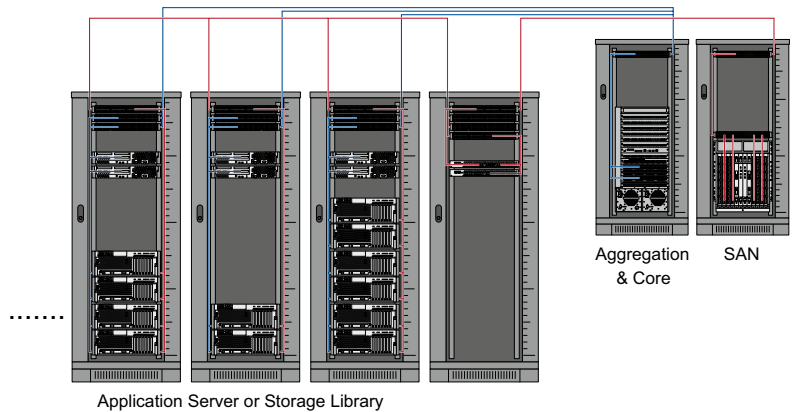
The Top of Rack (ToR) architecture is used for high-speed connections between servers, storage systems and other data center devices. This networking concept is used primarily in virtualized environments, for purposes that include integration of high-performance blade servers. A ToR switch or rack switch is installed on the top of racks as an access switch. This facilitates patch cabling, to be more specific connecting individual servers via patch cords. Migrations to 10 gigabit Ethernet are easily managed through the use of ToR.



ToR switches are usually fitted so they can be adapted for any specific purpose. For example, they include slots for transceiver modules allowing for the use of 10/40/100 gigabit Ethernet and increase in port density. SFP+ modules allow 48 ports to be represented on a single height unit (44 ports in the cases of QSFP+ modules). ToR switches can achieve data throughputs of one terabit per second (Tbit/s) or higher. Section 3.6.4 describes transceiver modules in greater detail.

Other ToR switch developments allow for data center bridging (DCB) and in turn lossless Ethernet and converged enhanced Ethernet (CEE). Data center bridging is described in greater detail in section 3.8.7.

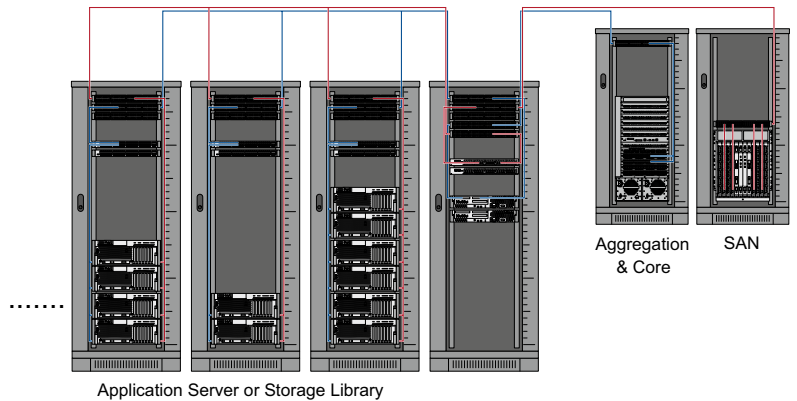
The adjacent figure depicts the ToR concept for conventional LAN communication. The SAN connection here is designed as an EoR architecture and thus requires an additional rack. As a result, LAN racks include additional space for servers.



This model optimizes the port assignment for SAN switches, and fewer SAN switches are required overall.

The second cabinet row scheme depicts a Cisco ToR architecture variant.

LAN fabric extenders are used in the place of ToR switches. These components use expansion modules to make 10 gigabit Ethernet connectivity plus Fiber Channel over Ethernet (FCoE) possible.



Fabric extenders consolidate and unify the LAN/SAN network. This is also known as I/O consolidation.

The different ToR concepts share some common characteristics, i.e. advantages and disadvantages:

Advantages:

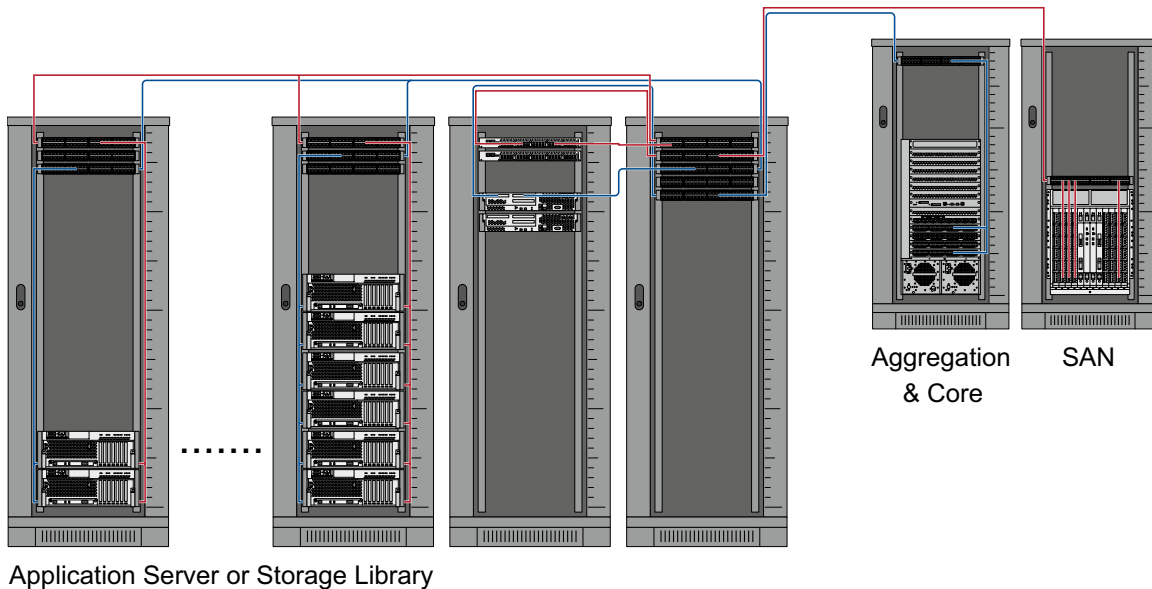
- Smaller cable volumes, lower space requirements for horizontal cabling, lower installation costs
- Suitable for high server densities (blade servers)
- Servers can be easily added

Disadvantages:

- LAN ports not optimally assigned, less efficient use of switch ports
- Sometimes unnecessarily many switches in operation (material and energy costs)
- Fixed relation between access and aggregation layers, makes it difficult to increase server performance and to aggregate into blade servers, makes 100 GbE implementation difficult
- Limitations in scalability and thus adaptability to future requirements

3.4.2 End of Row (EoR)

The end-of-row architecture opens up the cabinet row or cabinet group into a star pattern. Switches sit in one cabinet and route data cables from that point to servers in neighboring cabinets. As mentioned above, each server is normally provided with three cables (LAN, SAN, KVM), as well as two additional cables (LAN und SAN) in case of a redundant connection configuration. This results in at least 96 cables, given 32 servers in one cabinet. As an alternative, servers today may also be connected directly to aggregation switches.



The EoR architecture represents one alternative to ToR. Its advantages and disadvantages include:

Advantages:

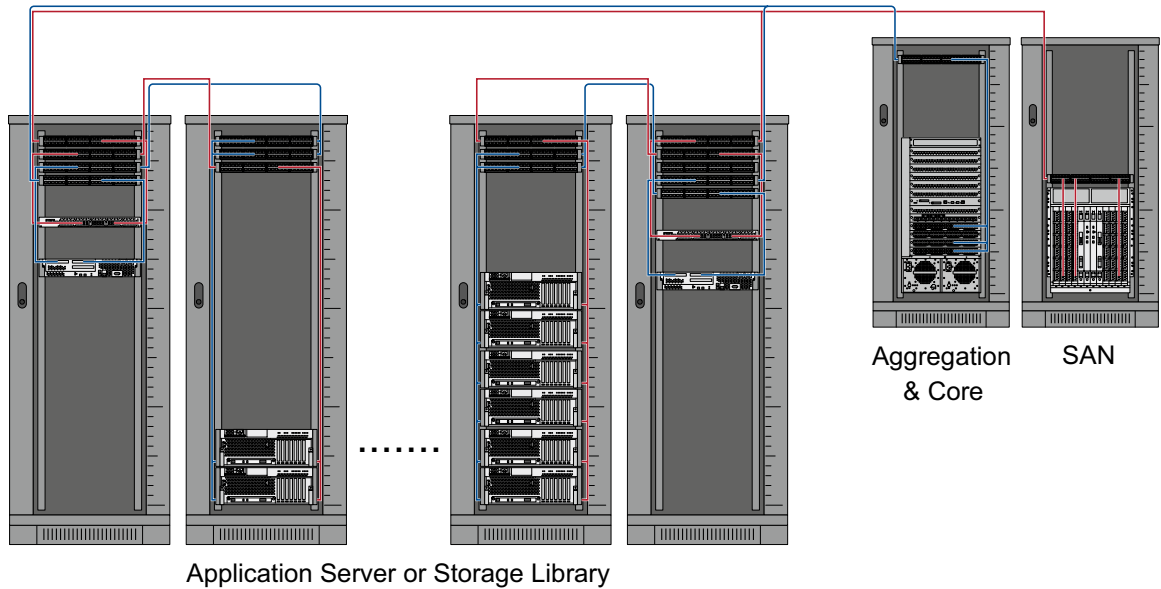
- Flexible, scalable, can grow with future needs
- Efficient assignment of LAN ports
- Concentration of access switches simplifies moves/adds/changes
- Optimal rack utilization, more leeway for server expansion

Disadvantages:

- Greater cable volume in horizontal cabling
- Many cable patches for EoR switches (server and uplink ports)

3.4.3 Dual End of Row

Dual end of row is a variant of EoR variant that provides more potential when redundancy is required. Access switches are distributed over both ends of the cabinet row, and cable runs are divided.



Advantages:

- Can support redundancy
- Flexible, scalable, can grow with future needs
- Efficient assignment of LAN ports
- Concentration of access switches at 2 locations simplifies moves/adds/changes
- Optimal rack utilization, more leeway for server expansion

Disadvantages:

- Greater cable volume in horizontal cabling area
- Many cable patches required for EoR switches (server and uplink ports), though half those required by EoR
- 1 less rack available for servers

3.4.4 Middle of Row (MoR)

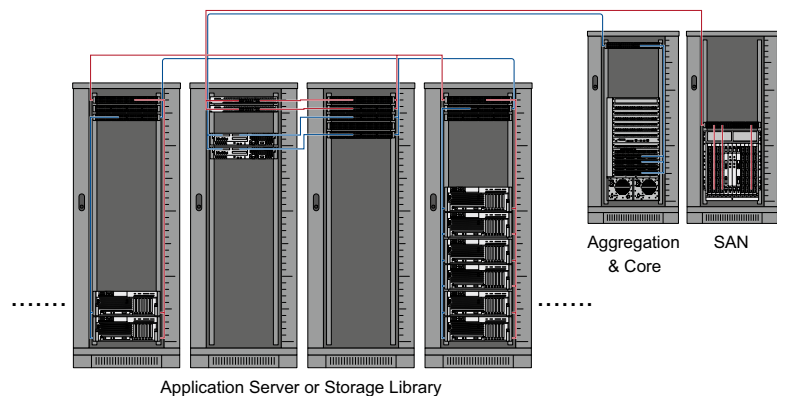
As in EoR, MoR distributors are concentrated at a single point that is arranged centrally within the cabinet row or group.

Advantages:

- Like EoR
- Shorter distances than in EoR

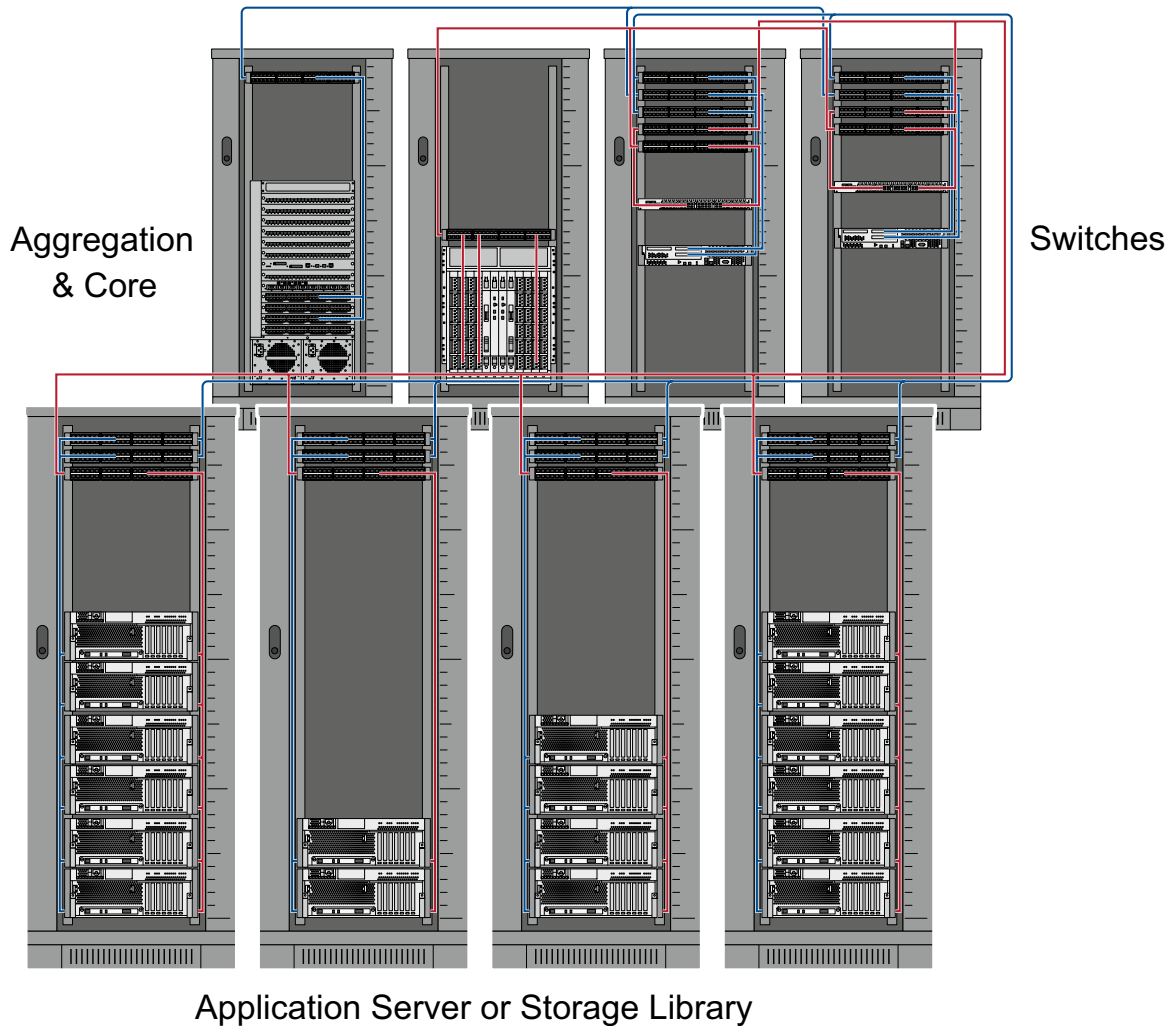
Disadvantages:

- Like EoR
- More cables (horizontal cabling)
- Many cable patches required for MoR switches



3.4.5 Two Row Switching

The two row switching model is often the architecture of choice in smaller data centers. Network components and terminal devices are placed in separate cabinet rows. This architecture is similar to the dual end of row concept.



Advantages:

- Flexible, scalable, can grow with future needs
- Relatively efficient assignment of LAN ports
- Concentration of access switches at 2 locations simplifies moves/adds/changes
- Optimal rack utilization, more leeway for server expansion
- Shorter distances in backbone

Disadvantages:

- Greater cable volume in horizontal cabling area
- Many cable patches required for switches

3.4.6 Other Modules

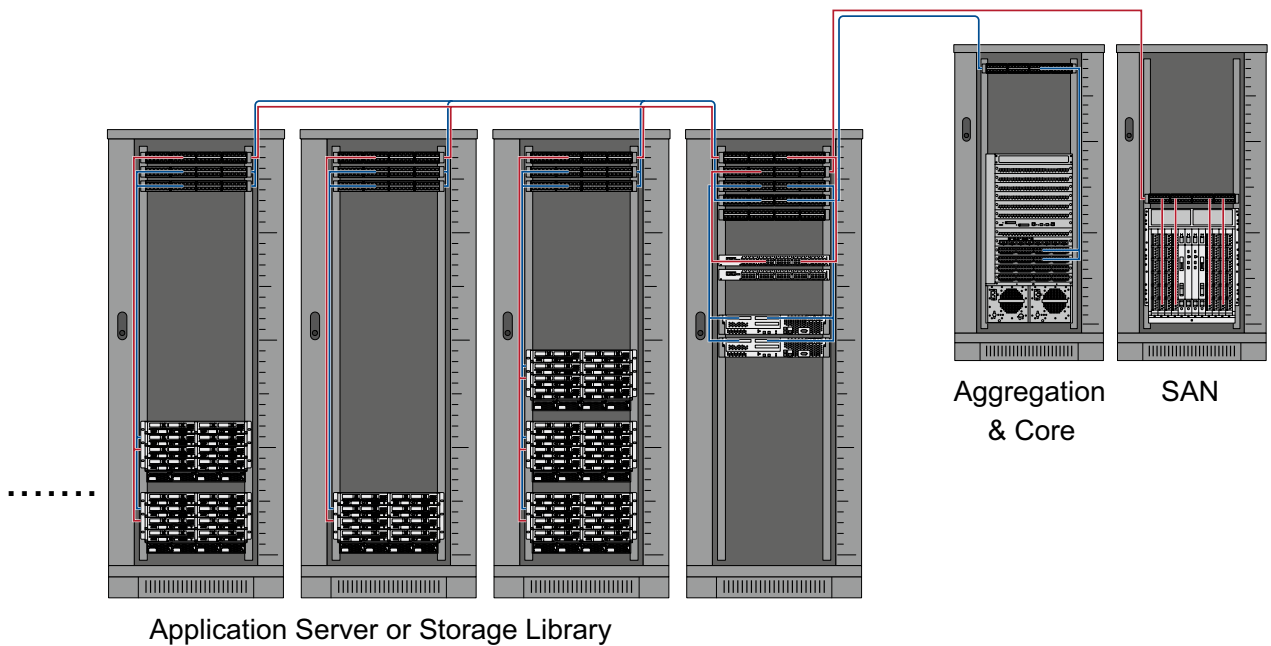
A few other building blocks for cabling architectures that may be relevant in data center planning should be mentioned briefly at this point. These modules can be combined and adapted as needed. Factors that dictate which model or which combination or adapted configuration should be preferred include any special requirements the data center must fulfill, any special conditions involved in the project and the future visions the operator has for the system. It is also important that due attention also be paid to selection of the media to be employed in the solution (copper or glass fiber). Only a comprehensive planning process will lay the foundations for implementing a data center that is scalable, can be easily migrated and thus has the ability to meet future needs. Section 3.8 provides tips for selecting media, which in turn depend on what communication protocols will be selected

ToR/EoR Combination

ToR's outstanding feature is the effective cabling solution it provides for servers. The consequences of this, however, are early aggregation and potential "overbooking" in the uplink direction. EoR/MoR requires high port densities on the chassis that serve as central fabrics for all servers. One conceivable configuration combining these architectures would be: 1 Gbit/s connections in the ToR section are aggregated into 10-Gbit/s and routed to an EoR system with a direct 10-Gbit/s server connection.

Integrated Switching

Integrated switching is based on blade servers that combine switch cards and server cards in a single housing unit. Cabling systems are generally restricted on a glass fiber backbone. The diagram below shows a rather untypical cabling configuration. Integrated switching includes I/O consolidation. Communication with the SAN environment in this configuration can be carried out by means of FCoE (Fiber Channel over Ethernet).



Pod Systems

A pod system consists of a group of 12 to 24 consolidated, self-contained rack systems. These units are designed for maximum modularity, efficiency and profitability and can be replicated quickly and easily. Pod systems can be used in data centers of any size.

Large organizations connect a number of units together until the required IT performance is represented. Pod systems allow companies to respond flexibly to capacity demands as well as business and market developments. Capacities can be extended in a standardized manner.

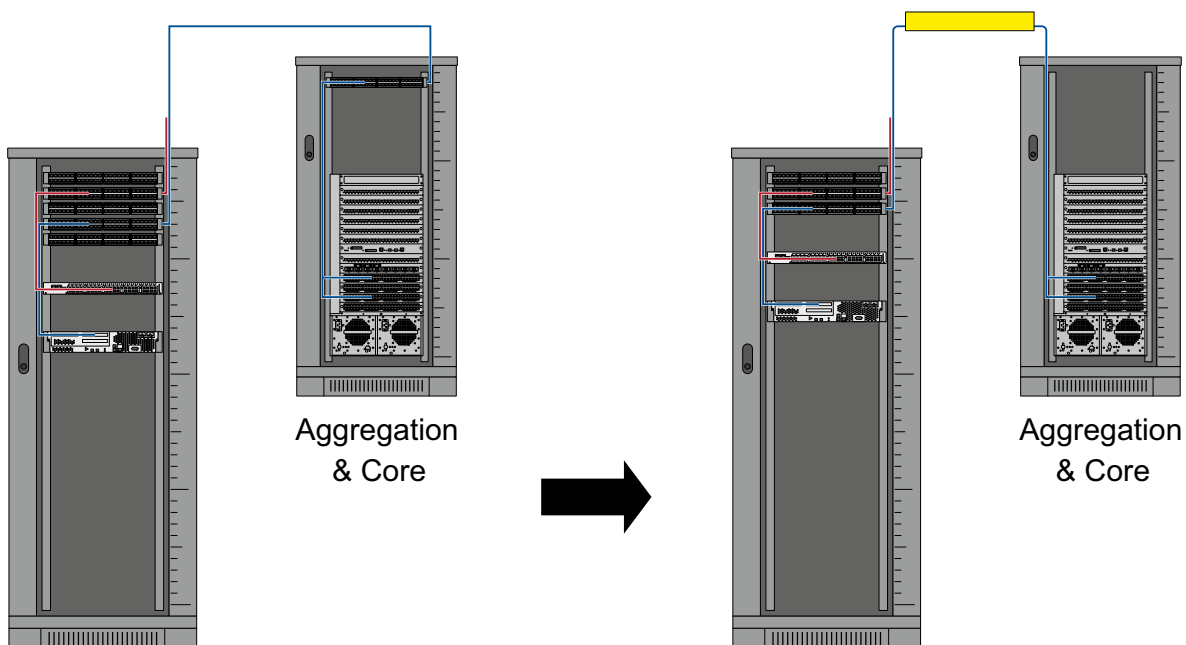
However, systems and channels of communication should be implemented redundantly in order to minimize the "single point of failure" problem.

Uplinks

Planners must also make sure they provide for adequate performance reserves and development potential for uplinks as well. As is generally known, switches are required to transfer a wide variety of data rates for specific terminal devices. For example, if all devices using a 24-port switch want to transfer data at the same time at an unrestricted rate of 1 Gbit/s, the uplink must make at least 24 Gbits/s available. In practice, a 10 Gbit/s connection in full duplex mode can transfer 20 Gbit/s. The example is only intended to show that uplinks are subject to high demands.

Uplink ports should be selected in accordance with the demand. Permanently installed interfaces or available slots are generally available for outfitting systems in a modular fashion. The extensive range of interfaces provides for flexibility and scalability (also see section 3.6.4). Media converters can also be used so that the uplink port can also be used as an interface between copper and glass fiber cabling.

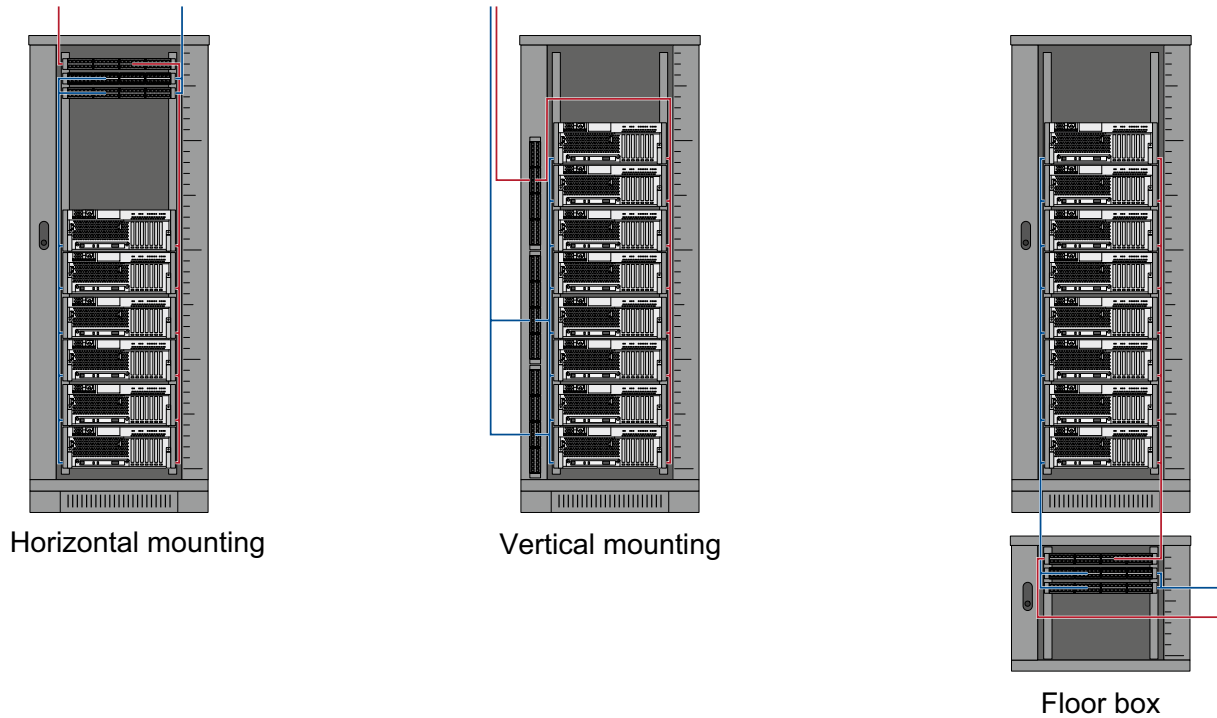
Uplinks are also used to cascade switches. These components are easier to connect in series. The diagram shows a cascading scheme from the access layer to the aggregation layer. At the left are the connections from permanently installed cables, at right those from patch cords that are routed through a cable duct. The variant with patch cords can be useful over short distances since these require fewer patch panels and plug connections.



Arranging Patch Panels

An important item in planning cabling architecture is the arrangement of patch panels. These components should take up as little room as possible, be easily accessible and provide for efficient use. The following options are available as alternatives:

- Horizontal or vertical rank arrangement
- Installation in double floor or in a separate location.

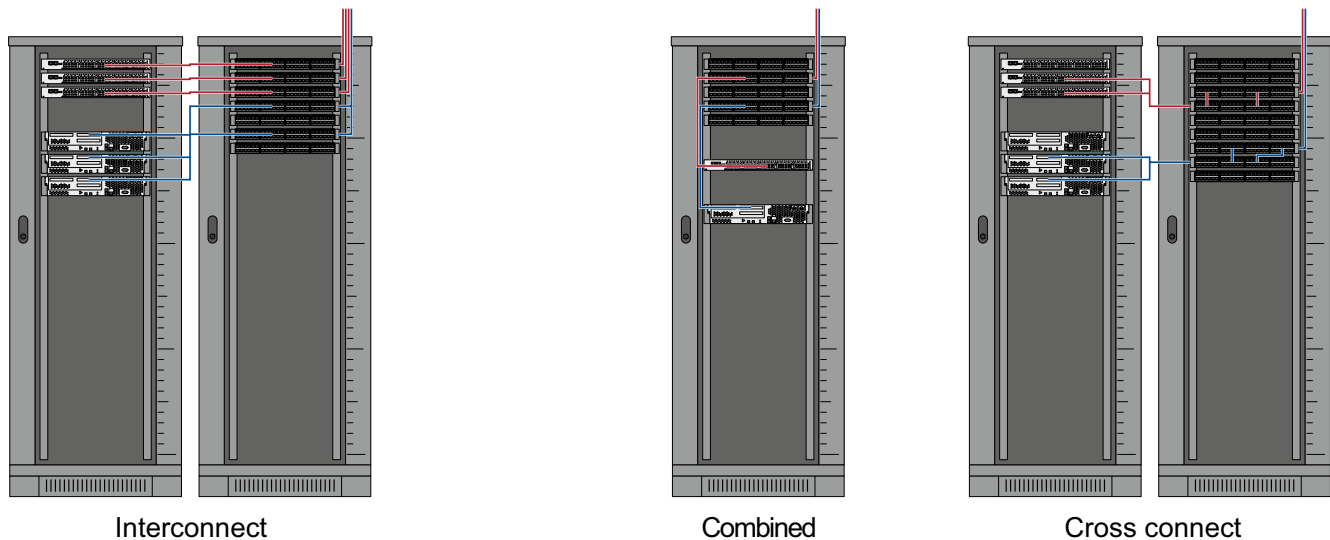


R&M's data center assortment includes a number of space-saving solutions. For example, 3 patch panels can be installed in the Robust (CMS) cabinet type on both the front as well as rear 19" mounting plane, each on the left and right side of the 19" sections (center graphic). Given high-density panels with 48 ports, 288 connections can then be installed into in a rack of that type, in both the front and rear – and the full installation height is still available.

288 connections (copper and/or glass fiber cabling) can also be realized via R&M's Raised Floor Solution. This under floor distributor solution can take in up to six 19" patch panels (graphic to the right). The platform goes together with the double floor grid (600 x 600 mm) and therefore supports the use of narrow racks – which also contributes to efficient use of the space in the data center. However, make sure when planning and installing these solutions that the supply of cooled air is not blocked.

Flexible Cable Patching Solutions

Small data centers can often arrange distribution panels and active network in either the same rack, or in two racks are located directly next to one another. As the following diagrams show, these configurations allow for a wide variety of cable patching configurations.



- Left: Components divided over two racks, separate patch cords from cabinet to cabinet.
- Center: All components in one rack, simple patch cabling between height units.
- Right: Components divided over two racks, pre-assembled cables create the connection between cabinets or distributors and active devices.

SAN

Storage area networks (SAN) are required for various applications like booting, backup, mail servers, file servers, or for operating large databases. SAN communicates primarily over Fiber Channel and not over Ethernet. In contrast to LAN, SAN permits direct hard disk access (block I/O).

Up to this point, servers have been equipped with a network interface card (NIC) for Ethernet and FC host bus adapter (HBA) for Fiber Channel. In the future, however, LAN and SAN will be merged more and more to provide data centers with the ability to manage growing data volumes even more economically. This trend is known as convergence (see section 3.7.2). Convergence has significant long-term consequences for cabling which should already be taken into account in current planning.

3.5 Data Center Infrastructures

Planning data centers is a challenge that is rewarding, but covers numerous facets and entails much responsibility. The purpose of this section is to provide the reader with appropriate guidance in this regard. It covers the key areas of data center infrastructures. This spectrum ranges from systems for power supply and climate control, includes concepts of interior design and cabling routing, and concludes with infrastructure management.

The main principles involved in a professional concept for data centers include: Conserving space and energy, providing support for efficient, economical operation, providing for expansions and changes, and achieving a maximum level of security. Factors such as room planning, the computer room layout and the technical environment must remain secondary to the requirements listed above as well as similar requirements.

Just small changes can translate into an increase in energy efficiency. It is essential that rack rows, hot and cold air routing systems, ventilation and climate control technology, structural elements and cabling routing systems be planned and installed in an optimal manner.

The overall design must take into account typical processes. For example, data center statics must be calculated in such a way that heavy active components and machines can be easily installed and removed. The room must have headroom of at least 2.6 to 2.75 meters as measured to the lowest installations. Floor loading capacity must be at least 750 to 1,200 kg/m². Access doors must be at least 1 meter wide and 2.1 meters high, sealable, and have no thresholds. Cabinet rows must be optimized for cooling active devices. Aisles must also be sufficiently wide so that devices can be easily installed and removed. These installation depths require an aisle width of at least 1.2 m. If a hollow floor is used, it must be possible to keep at least one row of base plates open per passageway.

These are just a few aspects that should be mentioned in advance. A discussion of the essential areas in the infrastructure is presented below.

3.5.1 Power Supply, Shielding and Grounding

All buildings must be properly earthed so that hazardous current is properly discharged and individuals as well as electrical installations in and around buildings are protected. National regulations stipulate how earthing systems are to be installed.

Earthing is especially important in data centers since they house expensive, sensitive equipment that must be protected from surges and electromagnetic interference. Implementing shielded cabling systems in order to run 10 Gigabit Ethernet results in an additional need for earthing. In this case, not only the building, but also the entire data cabling system, must be provided with a reliable earthing system.

Importance of Earthing

An earthing concept guarantees functionality and electromagnetic compatibility (EMC) will be maintained for purposes of safety. The EMC characteristics of a device or system ensure that it will not interfere electromagnetically with any other equipment in operation. A building with IT equipment makes the following demands on an earthing system:

- Safety from electrical hazards
- Reliable signal reference within the entire installation
- Satisfactory EMC behavior, so all electronic devices work together without trouble.

In addition to national regulations, the following international standards are useful tools in developing an earthing concept: IEC 60364-5-548, EN 50310, ITU-T K.31, EN 50174-2, EN 60950 and TIA-607-A.

In order to reduce interference voltage, an equipotential bonding system must be designed to be suitable for high frequencies and also be low resistance. This is achieved through surface connections with all metal masses, housings (racks), machine and system components.

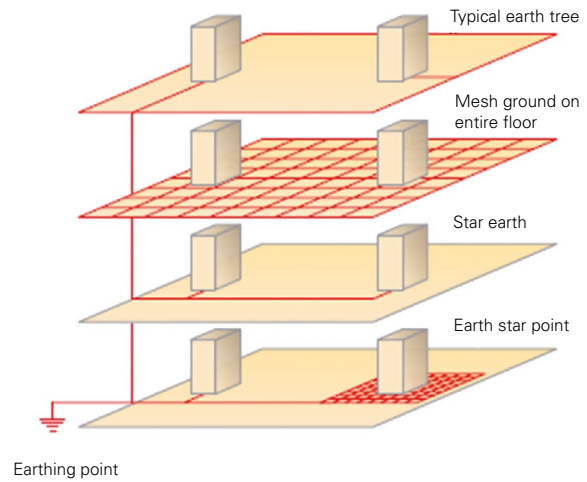
Alternating Current Distribution System

The neutral conductor of the alternating current distribution system should be separated from the earthing system. This function is best carried out through use of a TN-S system. TN-C systems are used in internal installations with PEN conductors (protective earth and neutral conductor combined). Note: These devices may not be used for IT equipment.

Two proven earthing methods for buildings are the tree structure and meshed structure:

Earthing System as a Tree Structure

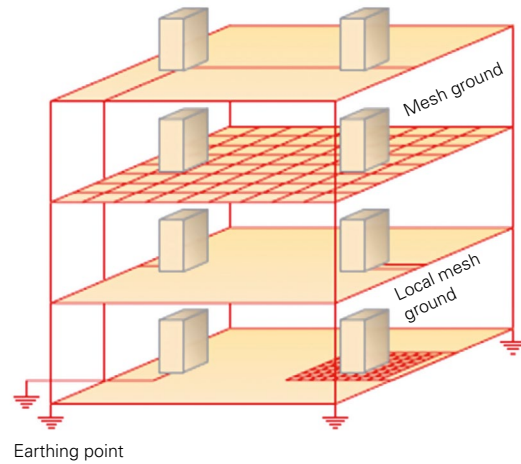
This configuration comes from the field of telecommunications. Earthing conductors are connected together at a central earthing point. The configuration avoids ground loops and reduces the interference from low-frequency interference voltages (humming).



Earthing System as a Mesh Structure

The goal of the mesh structure is to distribute the currents in ground loops as evenly as possible and to minimize these loops. Mesh structures are mostly used for high-frequency data transmissions. This process requires that the building have as many earthing points as possible. All metallic building components must be connected to the earthing system.

If a continuous meshed structure for earthing cannot be installed in buildings, this structure can be approximated by installing cells. Metallic cable ducts, conductive double floor and parallel copper conductors are used for local meshed earthing.



Grounding Options for Patch Panels

So that data center operators can work freely during planning and installation, all patch panels should be earthed using a tree structure as well as meshed structure. This installation feature should be specifically noted at evaluation time. The final selection of the earthing method to be used also depends upon the conductivity of 19" cabinets or mounting rail.

Every patch panel is earthed individually in a tree structure, through the cabinet or to ground bus bars. Looping the earthing connection through from one patch panel to another is not recommended, since this increases impedance.

Cabinet Earthing and Earth Connection

The cabinet in a tree structure itself is earthed after the patch panels are earthed, via telecommunication main ground bus bars (TMGB) or telecommunication ground bus bars (TGB).

In the case of a meshed structure, the cabinet is connected to the next earthing point within the building structure. It is important in this case that the impedance (Z) from the current path to the earth is as low as possible. This value is based on ohmic resistance (R) and line inductance (L), as shown in the following term:

$$Z = \overline{\omega L} + \overline{R}$$

with

$$\overline{\omega} = 2\pi f$$

Impedance must be taken into account when selecting the earth connection for the cabinet. Flat cables, braided straps or copper strips with low impedance are the best choices for this purpose. If stranded conductors are used, these should be 4 to 6 mm² (16 mm² is even better).

It can be a good idea to use HF-shielded housing in applications with high-frequency field-related influences. The parameters for a standards-based housing unit are best determined through on-site measurements.

3.5.2 Cooling, Hot and Cold Aisles

The electrical power that is taken in by IT devices is later released as heat. In this process, every kilowatt of electrical power corresponds to one kilowatt of heat. Condensing data center performance produced even more heat, which must then be drawn off. Heat dissipation is necessary since operational temperatures must be kept constant to ensure equipment availability and safety, and also to avoid overheating. Climate control concepts are a useful way to comprehensively include and appropriately implement necessary cooling functions.

Some figures should suffice to illustrate the magnitudes involved in this process. Heat loads per CPU normally lie over 130 W/cm². This corresponds to the heat per square centimeter emitted by two standard light bulbs. Many data centers implement climate control through cool air blown through the double floor. Experience shows dissipation loss of up to 8 kW in a rack or housing unit can still be cooled through a double floor.

A closed-circuit air conditioning system implemented through the double floor meets its limits as heat loads continue to increase further. Consider a fully equipped 19" cabinet. The devices installed over the 42 height units in the cabinet consume electrical power of over 30 kW. This corresponds to a heat load that is also greater than 30 kW. This heat load may increase even further as server equipment is condensed even further.

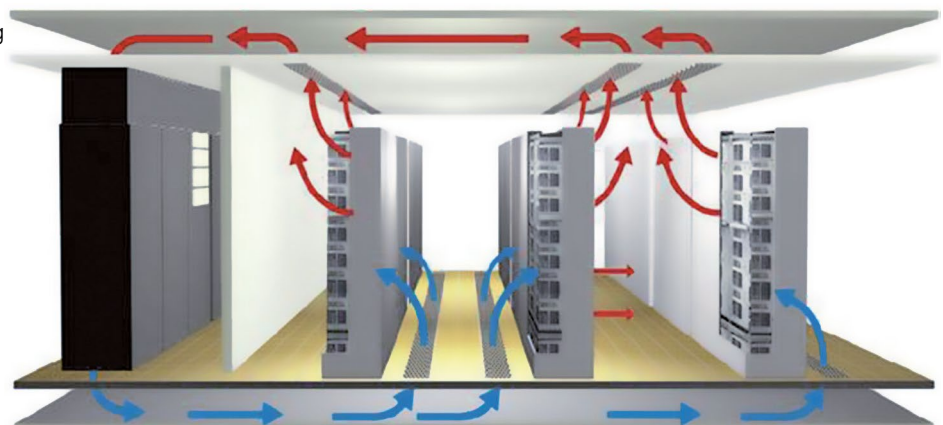
The cold aisle/hot aisle model provides an efficient basis for designing climate control systems. In this model, all devices that give off heat are bundled together in one aisle or on one side of a cabinet. Cold and hot zones are partitioned off from one another. In addition, the aisles can be housed so as to provide the ability to draw off more heat effectively.

Taut cabling in the double floor helps the cool air to flow in unhindered. The climate control system becomes obstructed when too many cables are installed in the floor.

The selection criteria for an air conditioning solution includes the maximum expected dissipation loss, acquisition costs, installation conditions, operating costs, costs for expansion, ability of the given system to grow with future requirements, costs for downtimes and physical safety.

The two established models for climate control:

- Closed-circuit air conditioning
- Direct cooling



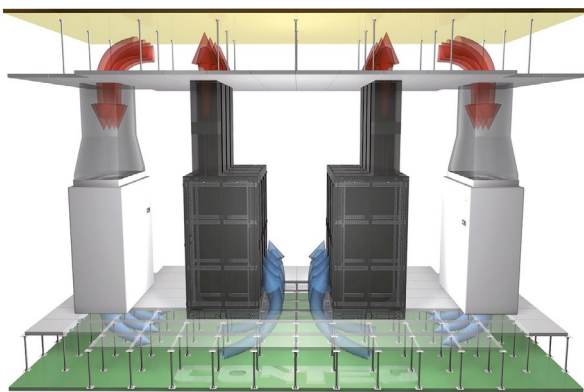
*Cold aisle/hot aisle principle solution
– closed-circuit air conditioning
(source: BITKOM)*

Closed-Circuit Air Conditioning Operation

In a closed-circuit air conditioning system, the cool supply air, cooled by the climate control system, flows in to IT components. At that point the air absorbs the heat from the components, then flows back to the climate control system. The air is cooled down again at that point, and the cycle is thus completed. A small amount of outside air is fed into the air-conditioned room and used only for purposes of air exchange. Optimal conditions with respect to temperature and relative humidity can only be achieved with closed-circuit air-conditioning units, or so-called precision air-conditioning units. Lowering the temperature of the return air allows these systems to work more energy-efficiently.

Rack arrangement and air flow are both crucial factors in the performance of closed-circuit air conditioning systems. In the so-called hot aisle/cold aisle model, air flows through IT components and network components in a horizontal direction. 19" cabinets are arranged here in such a way that the air flow absorbs heat from active components on the way from the double floor back to the air-conditioning unit. Air flow systems are divided into two types: self-contained duct systems (plenum feed, plenum return) room air circulation systems (room feed, room return).

The temperature of the supply air fed into the cold aisle is based on the given application. Its value lies between 18° and 27° C, given a supply air relative humidity between 40% and 60%. The temperature should fluctuate a maximum of 5° C per hour. Preset temperatures of 24° C to 27° C with relative humidity of 60% are currently state of the art.



Equipment for 19" cabinets must be provided on the basis of the circulation principle that is selected. In the case of room feed/room return, cabinet doors must be perforated at least 60%. The floor of the cabinet must be sealed up against the hollow floor at the warm side, in order to separate air flows. Performance of up to approx. 10 kW per cabinet can be achieved using this model.

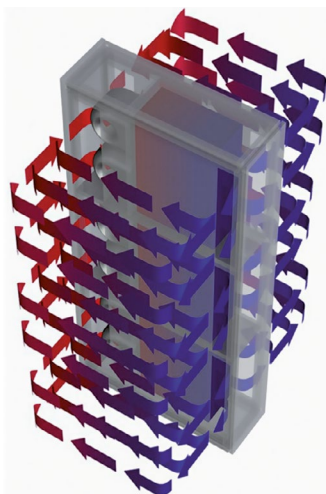
In the plenum feed/plenum return model, it must be possible to seal cabinet doors so they are airtight. The floor must also be sealed on the warm side of the cabinet, though it remains open on the cold side. Possible applications using this principle lie at approximately 15 kW.

Plenum feed, plenum return (source: Conteg)

The cold and warm sides within the cabinet must be kept separate so that air mixtures and microcirculations are avoided. Blind panels and seals should be used to seal unused height units and feedthroughs. Containment of the cold or warm aisle (contained cold/hot aisle) will increase system performance even further.

The height of the double floor is another important factor to consider in climate control. The cold aisle must be provided with slot plates or grids in order for air to escape properly.

Direct Cooling – Water-Cooled Server Rack

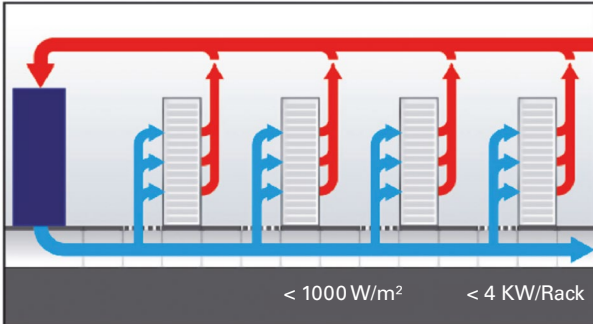


Direct cooling systems must be provided to racks when heat loads exceed 10 to 15 kW per cabinet. This solution is usually provided by installing cold water-cooled heat exchangers under or next to 19" units. A cold-water infrastructure must be installed in the rack area for this purpose. This method provides reliable cooling for heat loads of up to 40 kW per rack.

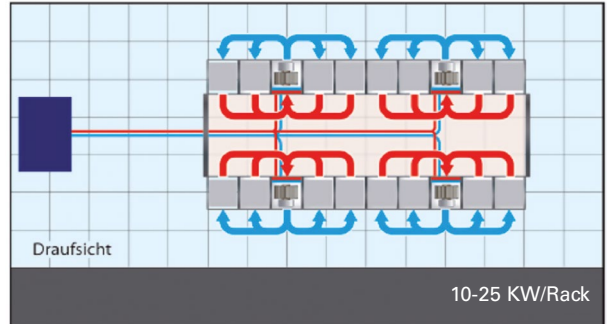
Water-cooled cabinets are not dependent on the room air-conditioning system. Water cooling is a good cooling option in rooms that have low ceilings and no space for double floors. In this case, contained cold aisles or hot aisles must also be implemented in order to achieve high-performance cooling.

The follow figures illustrate the power densities associated with different air conditioning solutions.
(Source: BITKOM)

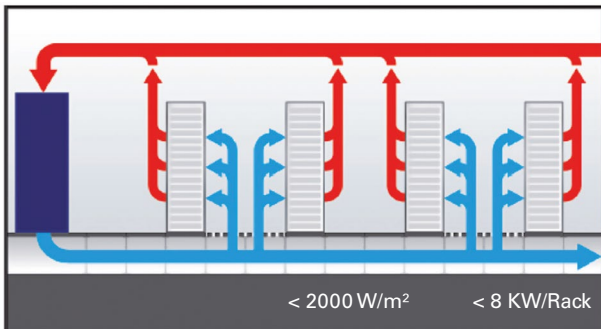
Air conditioning via double floor, racks not arranged for air conditioning



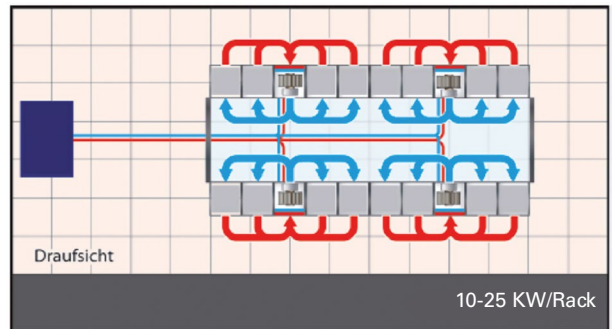
Water-cooled air conditioning with contained hot aisles



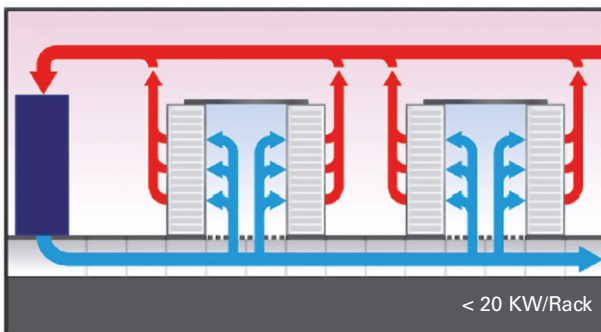
Air conditioning via double floor, racks arranged in cold/hot aisles



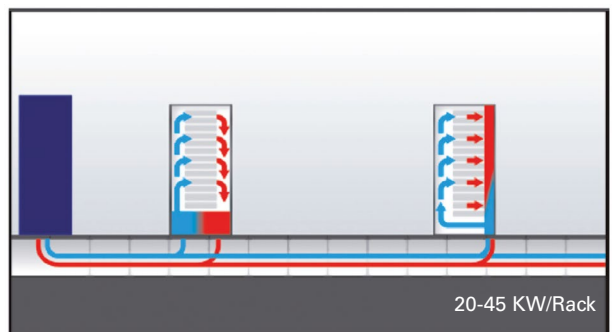
Water-cooled air conditioning with contained cold aisles



Air conditioning via double floor with contained cold aisles



Air conditioning via water-cooled racks (self-contained system)



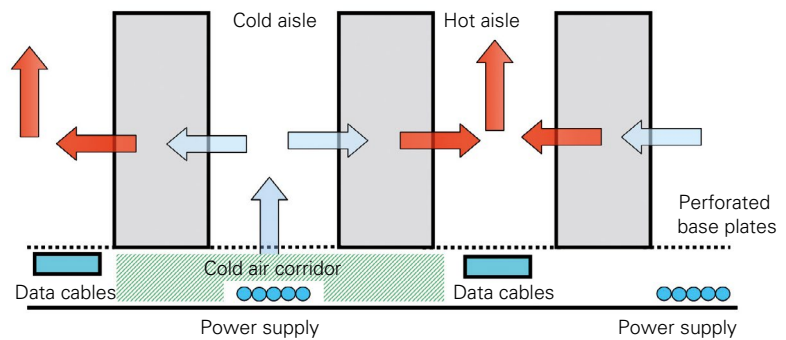
Regardless of whether a closed-circuit cooling system or direct cooling system is implemented, profitability, maximum efficiency and the highest possible energy savings should always be top considerations in selecting an appropriate system. A comprehensive examination of all options must be carried out before the decision-making process even begins.

The cabling system selected can contribute greatly to increasing climate and energy efficiency. The horizontal cabling in the hollow floor or under the ceiling as well as the vertical cabling in the 19" cabinet must be laid out so that air circulation is neither obstructed nor blocked.

3.5.3 Hollow/Double Floors and Hollow Ceilings

The cable routing configuration selected depends upon the design of the building in which the data center is installed. Cables can be routed in the hollow floor, in the ceiling as a suspending cabling, or as a combination of these two models.

Hollow floors and double floors should be 80 cm high. They must provide enough space for air circulation and cable routing purposes. The cables installed should not block the flow of air, nor should they be laid at right angles to the direction of air current. One solution is to combine all cables together under the hot aisle. If this is feasible, cables are laid in the ceiling, and the floor is used only for cooling purposes



Placing cable trays in the hollow floor

Racks in a hollow floor/double floor should be opened out along aisles. Power supply cables require less space and can be laid directly on the floor under the cold aisle. Data cables, requiring more space, can be laid in the cable routing ducts on the hollow floor under the hot aisle.

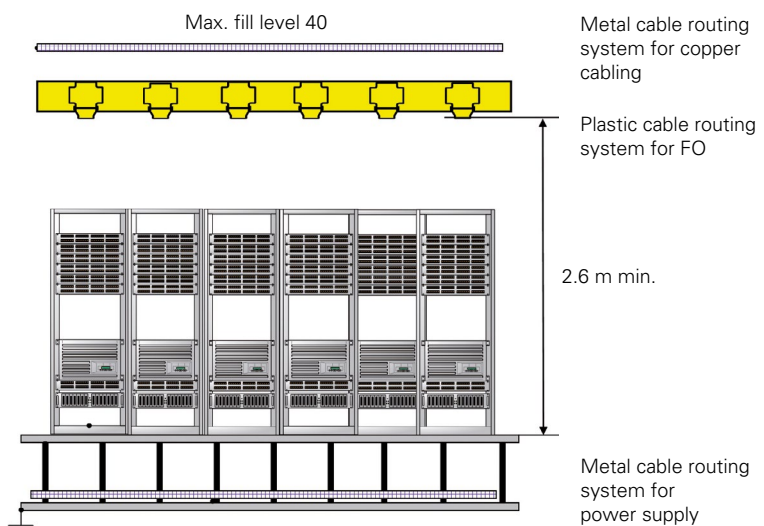
Copper and glass fiber cables should be installed in separate cable trays. The EN 50174-2 standard established requirements for separating data cables and power supply cables.

Obstacle-free cold air corridors are produced in the hollow floor when climate control devices are arranged in this way and housed in an aisle extension.

Cabling must be installed in cable routing systems under the ceiling when no hollow floor exists, or when the hollow floor is reserved for cooling purposes. EN 50174-2 contains specifications on the distances between power cables and data cables for this situation as well. Cable routes should be installed vertically one above the other, or directly above cabinet rows. It is essential that the cable route does not block lighting, security sensors or fire extinguishing systems. Cable routing systems made of metal increase EMC protection.

A cable duct should be filled to 40% at maximum. Data center operators who need to save space may find it a good idea to use low profile copper cables, since these components will significantly reduce the volume and weight of the cabling system. R&M's AWG26 installation cable takes up only 60% of the volume of a standard AWG22 cable and complies with all relevant cabling standards up to 55 m.

Combined cable routing solutions are often planned, depending upon existing conditions. For example, cable routing systems can be used underneath the ceiling for data cables, and the power supply can be installed in the hollow floor.



Mixed cable routing under ceiling and in hollow floor

This, just in itself, ensures the necessary distance between data cabling and the power supply and does not affect cooling capacity.

3.5.4 Cable Runs and Routing

Data center cabling is routed in hollow floors or hollow ceilings (see above) and is subject to the following requirements:

- Must not impair network performance
- Must not affect cooling
- Electromagnetic compatibility must be ensured
- Upgrades, changes and maintenance must be possible

The cable routing system in many data centers and server rooms has grown historically, and is therefore rarely at an optimal level. The reasons for this include:

- Connection cables were put in long after they were needed. As a result, no planned infrastructure existed.
- Documentation on the connection cables that were laid does not exist or is poor. As a result, connection cables that are defective or no longer required cannot be removed.

A double floor becomes overfilled quickly, and can no longer maintain its primary function of ventilation and cooling. The cabling system is constantly changing, making optimal dimensioning of data center cooling capacity difficult. Cabling solutions that take up less volume provide a solution: Glass fiber cables, multi-core cables or low profile cables. The use of cable routing systems such as conventional trays or mesh cable trays is recommended in all cases, since these bundle cables and route them in an orderly manner, and thus create space for air circulation. The advantages and disadvantage of both systems:

Tray

A tray provides better mechanical protection, but not always better electromagnetic protection. A tray is only a good option if edge protection is provided at incoming and outgoing threading points to preserve cables. There is the risk that cables will be damaged if threading points are added at a later time. Cable covers prevent "third-party cables" that may be installed at a later time, such as power lines, from being packed onto data cables and impairing their operation.

Mesh Cable Tray

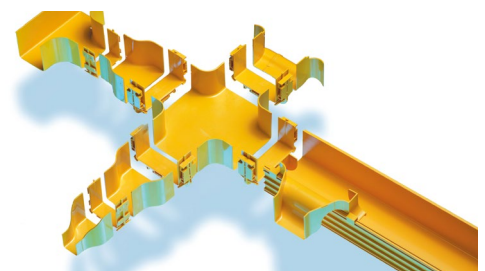
Cables in mesh cable trays have less protection. This is an issue especially for cables at the bottom of the tray. This risk can be reduced by placing a metal plate on the base of the mesh cable tray. An open mesh cable tray makes it easier for cables to be threaded out. Some manufacturers provide an extra cover for mesh cable trays.

Laying Patch Cords

One key question remains: Where should patch cords be installed? Can they be laid in the double floor? A device connection should always supply only one element (e.g. a server) in the same cabinet. Going by this principle, there should be no, or only a few, patch cords that extend beyond the cabinet. As a result, no patch cords should be stowed in the floor. Nevertheless, it can sometimes occur, when longer patch cords are in use, that connections must be made to other cabinets. It should be avoided putting these in the double floor whenever possible. One of the following options should be used instead:

- Conventional or mesh cable trays installed up above (see above).
- Trough systems such as the Raceway System from R&M. Like conventional trays or mesh cable trays, these are installed above cabinets. They also allow for customized configuration options, and preserve the cabling routing system, especially when fiber optic cabling is used.
- Under floor systems such as the Raised Floor Solution from R&M. These keep patch cords in one box that is installed in the hollow floor in front of cabinets. The patch cords run from the box directly into the cabinet and to active components (also see section 3.4.5).

Finally, it should be noted that a patch cabling system that is clearly laid out makes installation work as well as moves, adds, changes (IMAC) in the data center significantly easier. This is why patch cabling, like installation cabling, requires careful planning.



3.5.5 R&MinteliPhy – Intelligent Infrastructure Management



R&MinteliPhy is heralding in a new age for network managers. Managers now also have the ability to manage their physical infrastructure intelligently, completely automatically, and in real time. This system requires neither specialized patch cords nor new patch panels. Handwritten notes and laboriously updated tables are a thing of the past. R&MinteliPhy allows data centers to increase the utilization, profitability and availability of their systems. IT managers now gain one-hundred percent control over all ports, and more. This is because R&MinteliPhy provides support for analysis and documentation, for implementing standardized processes and for all typical management tasks that surround a passive infrastructure.

R&MinteliPhy Monitor and Manage: These components are the two pillars of R&M's IIM (intelligent infrastructure management) solution.

- R&MinteliPhy Monitor consists of just a few upgradable components: RFID tags for plug connectors, sensor bars for patch panels and analyzers for network cabinets.
- R&MinteliPhy Manage is the client-server solution and provides a central database in the LAN or cloud, as well as numerous automatable functions, tools for routing and planning and extensive libraries.

R&MinteliPhy will grow with your needs. Users have wide flexibility in selecting when and what part of their R&M infrastructure they want to administrate automatically.

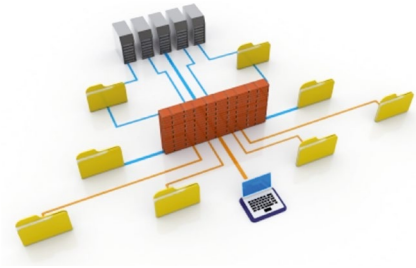
Manual administration is of course an option as well. Maintaining tables and databases involve enormous costs in both personnel and time. In spite of this, this information is never completely up-to-date or complete. This makes a number of processes difficult, from fault isolation and MAC processes to optimal capacity utilization and quality management. Finally, manual data maintenance shows a natural error rate of 10%. As a result: Up to 28% of the downtime experienced by data centers results from patching errors caused by inadequate documentation or missing process controls. Over the course of time, up to 40% of active switch ports fall into oblivion as a result of errors in documentation. This translates into a very inefficient use of investments.

By contrast, an IIM system provides a complete, 100% overview of network status and configuration – all this in real time, and from one central location. IIM replaces manual activities with standardized processes. An investment in an IIM system typically pays off after less than a year.

3.6 Active Components and Network Hardware

Who works the hardest in the data center? IT equipment is in service around the clock. Devices must transport, negotiate and store data packets without a break. Without a doubt, active components represent the engines and energy providers of the data network. This section provides an introduction to the topic of active components and network hardware. It shows the issues that must be taken into consideration in data center planning, evaluation and installation. Given this background of a comprehensive planning approach, a cabling specialist like R&M must then also become involved when the topic turns to active devices. This is because, in the end, the overall cabling solution must be tailored to connecting together a wide variety of different devices.

Considered as a whole, this equipment includes devices for amplifying, converting, identifying, managing and forwarding streams of data. Workplace computers can only communicate with one another and with servers through the use of network devices. Then, only by linking together active components such as switches, routers, transceivers, network interface cards, servers, PCs, storage devices, etc. will the network result. One essential type of distinction is that between the passive infrastructure, such as cabling, and active hardware



3.6.1 Introduction to Active Components and Network Interface Cards

Depending upon the size of work teams and organization, collaboration between users is either based on client/server networks or peer-to-peer networks. These network interface cards make different demands on active components.

- **Client/Server-Network:** Suitable for large groups. Central servers provide specific services and functions from a central location to clients that include workstations, terminal devices, users and customers. The services provided by servers are extremely varied: File servers are responsible for distributing files over the network and making hard disk space available, printer servers manage print jobs, mail servers and communication servers transmit messages, database servers and applications servers make files and software available to clients.
- **Peer-to-Peer-Network:** Suitable for direct collaboration between workstation computers with equal rights. Computers provide certain server functions themselves. A user can open resources on his/her computer for other users in the network. Consequently, this system requires that data be backed up in a decentralized manner.

Users in day-to-day operations generally work with combinations of client/server networks and peer-to-peer networks. This is one sample configuration of how a company might divide up these networks: Central servers ensure direct communication via e-mail, access to the Internet is via a proxy server or a router and data backup. Access to files and to printers within a department is realized as a peer-to-peer network.

A variety of different requirements for active network components results. The main criteria concern:

- Security such as protection against faults, unauthorized access and surveillance
- Performance
- Expansion options
- Connection technology protocols and media supported
- Other functions

3.6.2 IT Infrastructure Basics (Servers and Storage Systems)

Servers and storage systems are central components of the IT infrastructure in an organization and data center. These systems must be integrated to the environment or networks via LAN interfaces. A wide variety of interface types exist. These are specified according to the transmission technology (transmission protocols like Ethernet), speed (100 Mbit/s, 1/10 Gbit/s), media support (copper, glass fiber) and physical connection interface (RJ45, LC).

Another key criterion in the consideration of active components is latency (delay time). The smaller the latency, the better the data flow. Two types of delay exist in data transmission for network-compatible devices:

- Transfer delay (measured in microsecond/nanoseconds, $\mu\text{s}/\text{ns}$, regardless of the medium and distance)
- Switching delay (measured in milliseconds/microseconds $\text{ms}/\mu\text{s}$, regardless of device functions and switching/routing)

Active components can only make full use of their performance capacity when proper cabling is involved. Data transmission quality therefore also depends on the quality of the cabling used in the system. Factors such as insertion loss, modal noise, crosstalk and return loss can affect an otherwise impeccable signal transmission. An additional factor is that cabling is normally used for periods of five years and more. This is because these components are not easily replaced. Cabling must therefore be correspondingly long-lasting, work reliability over the long term and show enormous reserves from the start. Cabling must typically be able to support several generations of active devices as well as future transmission methods, which are constantly increasing in speed and sensitivity. These are also important criteria for planners and decision makers

Servers (Single Server)

A server is a piece of software (program) or a hardware component (computer).

- Server as software: A server in a client/server network makes a program available to a client as a service. Other programs can also access this service. Clients and servers in this process can run as programs on different computers or on the same computer. Servers can be configured according to the given service, e.g. as a mail server, web server, application server, or database server (also see section 1.2).
- Server as hardware: A computer with hardware especially designed for server application. Requirements of this hardware include a high throughput, high RAM, large number of CPUs, and high reliability. This server hardware is also known as a host. A conventional computer can also be used as a server, and provide basic services or server programs.

Server Farm

A server farm refers to the process of networking multiple, equivalent server hosts into one logical system. Distributing loads over individual servers and using the computing power of multiple servers allow process speeds to be increased and processes to be optimized. Specialized software is used to distribute the computing load over the farm.

Virtual Servers

Virtual servers are "machines" that are not established permanently on a single physical host, but are distributed over several computers. This allows the computer cluster (combine of hosts) to provide much more performance. A given client or user is unaware of the specific host processing its request or providing its required service.

Conversely, multiple software servers can be established on one host. The single physical machine then makes multiple virtual servers available for use, and can thus be used for a wide variety of customer applications. The different users and clients on the outside are likewise unaware that they are making use of the same device.

Rack Servers

Rack servers are compact devices that are generally installed in one rack or network cabinet. They provide high performance from just a small amount of space, and provide flexibility for IT infrastructures that are being set up for the first time or are being extended. These components usually take up two or four height units (HU) in a single rack.

A few performance indicators from popular rack server are listed below to provide an example of the performance potential of these devices:

	HP ProLiant DL380 G7	Fujitsu Primergy RX500	HP ProLiant DL380e Gen8
Construction	2 HE / Rack	4U rack	2U rack
Main memory (max.)	384 GB	1,536 GB	384 GB
Processor	Intel Xeon 5500 series; Intel Xeon	Intel Xeon E5-4600	Intel Xeon E5-2400
Storage (max.)	16 TB	7.2 TB	25 SFF or 12 LFF drives
Network ports	4 x Gbit-Ethernet	2 x Gbit Ethernet (opt. 10G)	4 x Gbit Ethernet

Pizza box

A server housing unit in 19" technology with one height unit is also called a pizza box in the slang of the industry, since it brings to mind the typical packaging for a frozen or home delivery pizza.

Blade Servers

Blade servers are the latest in server design. These units are highly condensed, compactly constructed machines in which a number of processing units such as cassettes or disks (blades) can be run together. They are generally offered in sizes of six to ten rack height units (U).

Blade servers can be used for all typical server applications. They should be selected on the basis of their expected use and work load. Their high power densities lead to energy savings and also reduce expenses for cooling. Additional advantages include: easy scalability, flexible administration, easy installation and maintenance, low cabling expenses and problem-free integration into existing infrastructures.

A few performance indicators from popular blade servers on the market:

	HP ProLiant BL460c	IBM Blade Center S	Fujitsu Primergy BX600 S3
Design	6/10 U / rack	7 U / rack	7 U / rack
Server blade module	HP ProLiant BL460c G7	Blade Center HS22	Primergy BX620 S5/S6
Front mounting slots	8/16 x half height or 4/8 x full height	6 x 2 CPU plug-in units and additional slots	10 x full height
Processor	Intel Xeon 5500/5600	Intel Xeon 5500	Intel Xeon 5500/5600
Network ports	2 x 1/10 Gbit Ethernet	2 x Gbit Ethernet and TCP/IP OffloadEngine TOE	4/6 x Gbit Ethernet or 2 x 10 Gbit Ethernet
Power supply	6 x 1,200 / 2,400 watts	4 x 950 / 1,450 watts	4 x 2'100 watts

Mainframes



Source: IBM

Mainframes are large computers that belong in the server category. These units are sometimes installed in racks or integrated into cabinet rows. Only a few manufacturers offer mainframes, mainly IBM.

These systems are primarily used as a server platform or client/server platform for business applications, for managing company and business processes. IBM provides its own operating system and database solution with its commercially available units.

The graphic to the left shows a System-z machine from the manufacturer.

Storage Systems and Storage Networks

Storage systems are used for online data processing and data archiving and backup. Devices on the market include primary mass storage devices such as hard disk storage or disk arrays. Secondary storage systems like jukeboxes and tape drives are also available. The main criteria to consider when selecting these products are access time and the specific requirements of the individual applications used.

Storage systems can be differentiated into (also see section 1.2):

- **DAS** – Direct attached storage (the storage system is located directly on the workstation, computer or server)
- **NAS** – Network attached storage (a central storage system runs in the LAN)
- **SAN** – Storage area networks (central storage network, usually located in data center)

Planning for storage solutions and storage networks is gaining enormous importance in company IT departments. Entire business processes depend upon data archives remaining reliable and available at all times. Compliance regulations place companies under obligation with regard to appropriate investments and guarantees. With all business processes are being digitalized, storage systems are turning into long-term memory. As a result, appropriate care must be taken when creating storage systems and storage networks.

The focus in this area is on NAS and SAN models. New SAN technologies are based on Fiber Channel over Ethernet (FCoE) as a networking concept since this technology goes together with Ethernet LAN (also see 3.7.2.). Companies should weigh the advantages and disadvantages of storage systems to come up with suitable solutions that will grow with future requirements.

DAS – Direct Attached Storage

Direct attached storage (DAS), or server attached storage, is a decentralized solution which uses hard disks that are located in a separate housing and are connected to a single host. These components are connected together via SCSI, SAS, eSATA or even USB interfaces.

NAS – Network Attached Storage

Network attached storage (NAS) makes centralized, independent cost-effective storage capacity available in a network. The technology is generally implemented as individual or coupled RAID hard disk drives on which basic file servers are installed. Device connection and administration is carried out via Ethernet LAN.

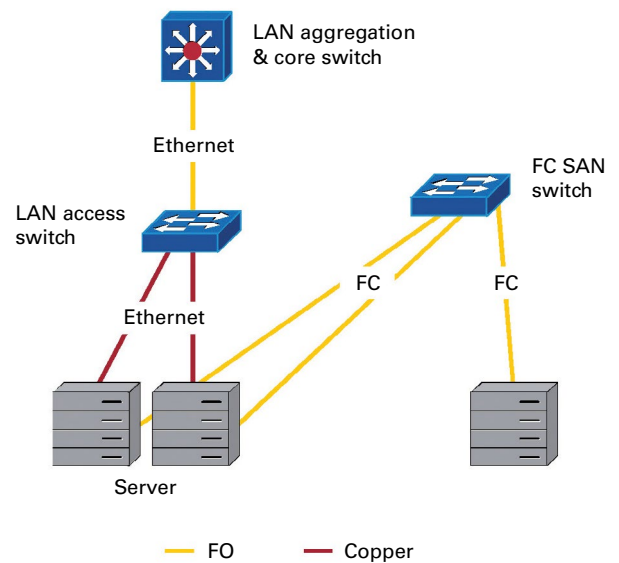
Computers access data media via LAN and work with a TCP/IP protocol such as NFS (Network File System) or CIFS (Common Internet File System). In contrast to direct attached storage, an NAS system represents a standalone computer (host) or virtual computer (virtual storage appliance/VSA). The system runs over its own operating system.

NAS systems have the ability to process extremely large volumes of data and provide rapid access to these data. Professional NAS solutions also provide support for data consolidation. NAS solutions can be designed to be redundant and fail-safe

SAN – Storage Area Networks

A storage area network (SAN) connects server systems with hard disk subsystems and tape libraries. It is generally designed for continuous serial transmission of large volumes of data (up to 16 Gbit/s). Device networking is typically based on the Fiber Channel (FC) standard. Servers are connected in the FC SAN using host bus adapters (HBA).

The illustration to the right shows how SAN over Fiber Channel is realized as a separate network. In the future, the SAM and the Ethernet-based LAN may be combined in FCoE (Fiber Channel over Ethernet). FC and Migration to FCoE are treated in detail in sections 3.7.2, 3.8.3 and 3.8.4.



Storage Solutions

Storage capacities must be constantly expanded. A central theme in this area is cost efficiency. An efficient mix of storage virtualization, cloud storage (storage as a service) and consolidation can help to meet these needs. Unified storage systems are provided as universal solutions. These systems support all storage protocols. Racks that contain only hard disks are finding their way into data centers more and more frequently. These solutions can be purchased pre-assembled.

Following are a few performance features of larger storage solutions that play a significant role on the market:

	HP StorageWorks MSA	Hitachi DS HUS 100	Nexsan SATABoy
Number of disks	48 (after expansion)	120 to 960	14
Max. capacity (SAS/SATA)	22 TBytes / 48 TBytes	3 PBytes; 756 / 360 TBytes	— / 14 TBytes
Interfaces	4 GB FC; 3 GB SAS / SATA / iSCSI	2 x 10 Gbit/s; 6 x 1 Gbit/s	10 / 100 / 1000Tx; SATA; FC; iSCSI
Scalability	Up to three SAS housings	—	Available
RAID level supported	0; 1; 3; 5; 6; 10; 50	0; 1; 5; 6; 10	0; 1; 4; 5; 6; 10

3.6.3 Network Infrastructure Basics (NICs, Switches, Routers & Firewalls)

A network infrastructure is formed from a number of different components. These components can be divided into two groups:

- Passive network components make up the physical structure and include cables (copper and glass fiber), connection modules, plugs, sockets, distribution panels, cabinets, etc
- Active network components are responsible for processing, transporting, filtering and distributing signals and data. These components include network interface cards, routers, switches, firewalls, etc.

Networks can be classified using a variety of criteria. For example, a distinction is usually made between a private local data network (local area network = LAN) and a public network (WAN = wide area network). Ethernet is generally used as a transmission technology in a LAN, while a WAN operates over broadband applications like ATM, xDSL, Ethernet and SDH. Modems and/or routers form the bridge between WANs and LANs.

Details on active network components and their functions and areas of application are presented below.

NICs – Network Interface Cards

A network interface card (NIC) creates a physical connection to a network. This connection can be established at an integrated slot (e.g. an RJ45 connection). The card communicates via the MAC protocol (media access control) and Ethernet (see section 3.8.2 for descriptions of media and speeds).

A MAC address is a unique hardware address for a NIC. This address is necessary for forwarding Ethernet frames to switches. The MAC address consists of six bytes. The first 3 bytes are assigned by the IEEE to the given NIC manufacturer, who uses the remaining 3 bytes as a serial number. Every device in an Ethernet LAN thus has an IP address for routing purposes, and a MAC address for switch forwarding.



Switches

A (layer 2) switch is responsible for dividing a network into physical subnetworks and for providing available bandwidth to each individual device using the switch. The switch automatically creates a source address table (SAT). The switch uses the table to store destination MAC addresses (NIC addresses for terminal devices) and assignment of physical ports (switch connection). The table is constantly updated, e.g. when new terminal devices are inserted into the network. This way the switch can always delivered required data to the correct address.



A switch on the link layer (layer 2, MAC Layer) of the OSI model (see section 3.8.1) functions like a bridge. In this case it is also called a bridging switch. It is, so to speak a multi-port bridge.

The performance capabilities of switches can be distinguished by using the following criteria, among others:

- Number of MAC addresses that can be stored (SAT table size)
- Switching methods used for forwarding data packets
- Latency (delay) of the data packets that are forwarded

The following table provides information on the advantages and disadvantages of different switching methods.

Switching Method	Description	Advantages	Disadvantages
Cut-Through	The switch forwards the frame immediately, as soon as it has the destination address available.	Low latency.	Errors in data packets are forwarded to the recipient.
Store-and-Forward	The switch saves the entire frame in a buffer, where it is checked and processed. The packet is then forwarded to the destination port.	Faulty data packets can be identified and sorted out.	Because data packets are saved and checked, a delay occurs, which is based on the size of the frame.
Combination of cut-through and store-and-forward	Many switches combine switching methods. Cut-through is used when only a few frames are faulty. The switch changes over to store-and-forward as soon as errors occur more frequently.		
Fragment-Free	This method is rarely used. The switch forwards the data as soon as the first 64 bytes of the Ethernet frame are error-free. This method is based on the fact that most errors and collisions occur in the first 64 bytes of a frame.		

Multi-function devices that combine router and switch functions are known as layer 3 switches. It makes routing decisions on the basis of OSI layer 3 information (IP address). A layer 3 switch routes individual ports to different domains (IP subnets) and operates as a switch within these domains. Routing between these domains is also possible.

The different switch types (access, aggregation, core) used in data centers was described in section 3.3. Functions and protocols used for redundancy are covered in section 3.8.6.

Router



The Cisco Nexus 7000 series is a modular, data center class switching system.

A router takes care of communication between network segments that may also operate using different communication protocols (LAN/WAN). It uses the network layer of the OSI reference model (layer 3, see section 3.8.1). In order to increase network security, many routers come equipped with an integrated firewall.

Since a router represents a node between two or more networks or subnets, it possesses an interface as well as an IP address for each network. This makes communication possible in each of the networks. When a data packet arrives at a router, it reads the destination IP address then determines the corresponding interface as well as the shortest path to the destination.

The advantages of routers over switches lie in their better isolation of data traffic. Just in the case of widely branched networks (e.g. WAN), data reaches their destination more effectively when they are forwarded over routers. Disadvantage: Routers slow down data transfers. They are often more expensive than switches. Each specific case must be reviewed to determine how its demands will be best fulfilled. For example, high-end switches also have the ability to manage routing functionalities.

Load Balancing

Large switching/routing engines are responsible for load distribution in data centers. This process is called load balancing and generally implies server load balancing (SLB). The goal of this method is to distribute the computing power in a network over multiple hosts. Server load balancing intervenes in the event a large number of clients overload a single server with a high volume of requests. Criteria for determining a need for SLB include data rate, number of clients and request rate

Firewalls

A firewall monitors data traffic and is located either directly in a computer (as software, known as a personal or desktop firewall) or in a central network location (as an appliance, known as a hardware firewall). Its purpose is to prevent unauthorized access to networks or unauthorized actions on a host. It decides, on the basis of defined rules, what network packets to let pass through and which packets to reject. Firewalls can be connected between networks or network segments to restrict mutual access to these systems.

Other firewall tasks include checking data transfers for anomalies (intrusion detection & prevention/IDP), content/URL filtering, and virus/spam protection. High-end devices can reach monitoring speeds on the order of 30 Gbit/s.



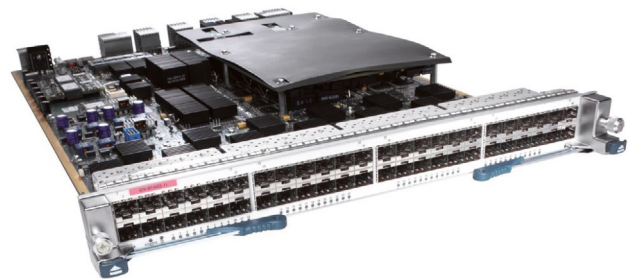
With its SuperMassive E10000, Sonicwall has announced a high-end firewall series. This allows companies to protect entire data centers from intruders

3.6.4 Connection Technology and Interfaces (SFP, SFP+, QSFP+, CFP)

Two options exist for connecting active components to a network:

- Permanently installed interfaces (the network technology is already defined by the time the purchase decision is made)
- Exchangeable interfaces, or so-called SFP (small form factor pluggables), also known as QSFP or CFP

Companies first decide, during the data center/network planning stage, whether data center and network connections will be based on copper or glass fiber cabling (also see section 3.9), and if so, in what areas this will be implemented and what interfaces to use. This decision will provide planners with the possible communication protocols they can use for the system (also see section 3.8).



Cisco Nexus 7000 Series 48-Port Gigabit Ethernet SFP Module

In the past, data center operators relied on copper cabling and Gigabit Ethernet, given the normal requirements of distance and performance in LANs. With the introduction of 10 Gigabit Ethernet, however, copper ran up against its performance limits, even when network interface cards with copper interfaces for 10 GbE were available. The IEEE standard 802.3 allows 10 Gbit/s transmissions over twisted pair copper cabling over a distance of 100 m. However, 10GBASE-T NICs in "data center mode" are frequently used for link distances of 30 m. This configuration does however require optimal conditions from interfaces, connection modules, plugs and cables. One example of a fully developed copper system solution for this application case is R&M's Cat 6_A ISO module.

Companies that wish to use 10 Gigabit Ethernet in their backbones should install glass fiber cables. Single mode fibers and LC plugs are the correct choice for greater distances.

40/100 Gigabit Ethernet has by now made its way into many data centers. This technology requires the use of top-quality OM3 and OM4 glass fiber cables as well as MPO-based parallel optic transceivers combined with MPO/MTP® connection technology of equal quality (MPO = multipath push-on).

MPO/MTP® plug connectors with twelve fibers are required for 40 Gigabit Ethernet transmissions. The four outer fibers on each connector are used to send and receive signals. 100 Gbit/s transmissions require ten fibers on each plug for sending and receiving. This is achieved by using the ten middle channels of 12-fiber MPO/MTP®, or by using a 24-fiber MPO/MTP® plug (see sections 3.10.1 and 3.10.2).

SFP / SFP+

Small form factor pluggables (SFP) are interfaces for high-performance network connections. These components are commercially available versions of transceivers which can be replaced during continuous system operations. These units are also called Mini-GBIC, SFF GBIC, GLC, and New GBIC or Next Generation GBIC. They are specified up to 5 Gbit/s. They meet their physical performance limits with Gigabit Ethernet.



SFP / RJ45 / 1000BASE-T



XFP: 8.5 x 18.5 x 71mm
[Image: Cisco]



SFP / SFP+: 8.5 x 13.4 x 56.5mm
[Image: Cisco]

SFP+ modules, even with their significantly smaller dimensions, provide for higher port densities. They make use of a single, serial data stream. Areas of application for SFP+ modules include 10 GbE, 8 and 16 gigabit Fiber Channel as well as SDH and SONET. XFP makes use of lasers with different wavelengths in order to run DWDM. This process greatly extends the possible areas of application for the technology.

SFP adapts signals to the type of a given transmission. So, for example, an SFP module can convert an electrical interface into an optical connection. Given its separate sending and receiving units, SFP and SFP+ have both electrical as well as optical interfaces available. SFP and SFP+ support wavelengths of 850 nm, 1,310 nm and 1,550 nm as optical interfaces.



Third-party suppliers also offer transceivers equipped with an intelligent configurator for flexible use in any system. Switch/router manufacturers may block these "open" systems. In any case, these systems should always be checked before they are implemented in any application.



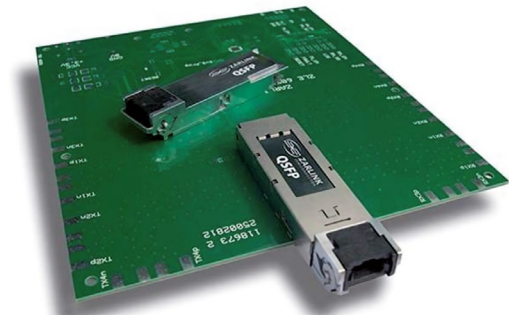
Example of an SFP switching solution from Hewlett Packard

QSFP+

The QSFP+ module is replacing SFP+ interfaces. This transceiver solution is suitable for 40 Gigabit Ethernet. QSFP stands for quad small form factor pluggable. It increases port density over SFP+ and also reduces total costs. This interface can also be used for Fiber Channel and InfiniBand.

The back side of the QFX3500 Data Center Switch from Juniper is shown as an example of this technology. This device combines a total of 48 dual mode SFP+ transceiver connections and four QSFP+ ports onto a single height unit, allowing the following network performance to be achieved:

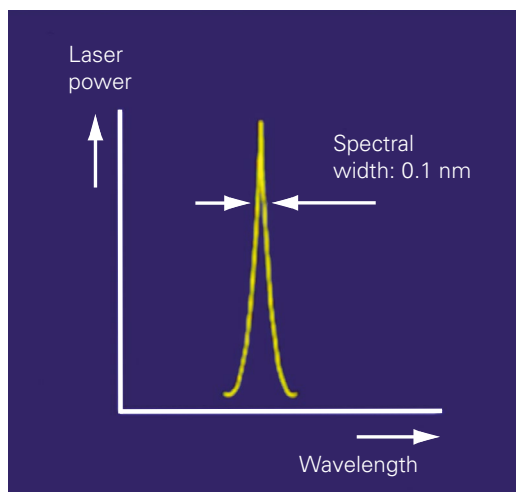
- 48 x 10 Gigabit Ethernet with:
- 36 dual-mode 10 GbE / 1 GbE FO port or 18 RJ45 ports
- 12 dual-mode 10 GbE or 2/4/8 Gbit/s Fiber Channel ports
- 16 x 10 Gigabit Ethernet via QSFP+ to SFP+ DAC cables or 4 x 40 Gigabit Ethernet QSFP+ ports



Source: Juniper

CFP

CFP modules are optical interfaces for 100 Gigabit Ethernet, and are comparable to SFP+ or XFP modules for 10 Gigabit Ethernet. These units are pluggable optical transceivers with optical transmitters and receivers, multiplexers and demultiplexers. They can combine ten parallel data streams each with 10 Gbit/s and multiplex these over four wavelengths over 25 Gbit/s.



Four DFB lasers (distributed feedback lasers) are used in this process. As this process generates heat, CFP modules require a system for heat dissipation.

A DFB laser is characterized by its high spectral purity and extremely low spectral width (see graphic to the left). Spectral purity results in lower chromatic dispersion in monomode fibers. This allows transmissions to bridge even greater distances, e.g. up to 100 km at data rates of 2.5 Gbit/s. This distance is reduced to several kilometers when transmission rates increase to 10 Gbit/s.

External modulation between lasers and optical fibers improve chromatic dispersion, so rates of speed value increase by an approximate factor of 10. Power output lies between 1 mW (0 dBm) and 10 mW.

DFB lasers support Gigabit Ethernet, 10 and 100 Gigabit Ethernet. Distance ranges can reach 40 km with OS2 fibers. This technology is suitable for DWDM (dense wavelength division multiplexing).

CFP modules are hot swappable. Typical wavelengths here are 850 nm, 1,310 nm and 1,550 nm.

Suitable areas of applications include 40/100 Gigabit Ethernet, Fiber Channel (FC), Sonet (synchronous optical networking) and SDH networks (synchronous digital hierarchy).

A list of parameters of some representative CFP modules for 100 Gigabit Ethernet over monomode fibers appears below:



Product example from Finisar

	Alcatel-Lucent	Brocade		Cisco		Juniper	
Product Line	7450 ESS, 7750 SR	MLXe	Nexus 7000	ASR 9000	CRS-3	MX240, 480, MX960	T1600, T4000
Feature Set	L2, IP, MPLS	L2, IP, MPLS	L2, IP, MPLS	L2, IP, MPLS	IP, MPLS	L2, IP, MPLS	IP, MPLS
Card type	1 port full slot	2 port full slot	2 port full slot	2 port full slot	1 port full slot	1 Port Half Slot	1 port full slot
Total Capacity in Gbit/s	100	480	440	160	140	130	100/240
Total 100 GbE Ports	10	32	32	20	16	22	8
CFP Media Types	10x10 10km, 100GBaseLR4	10x10 2km, 10x10 10km, 100GBase-LR4	100GBase-LR4	100GBase-LR4	100GBase-LR4	100GBase-SR10, 100GBase-LR4	100GBase-LR4

As of: 2012

The following table uses products from Brocade to illustrate some media-based applications of CFP modules in 100 Gigabit Ethernet networks. Note the low power consumption in the case of 100GBase-SR10.

Physical Layer Reach	100 m OM3/ 150 m OM4 MMF	2 km SMF	10 km SMF	10 km SMF	40 km SMF	40 km SMF
CFP Module	 100GBASE-SR10	 10x10-2km	 10x10-10km	 100GBASE-LR4	 10x10-40km	 100GBASE-ER4
Media Type	 MPO MMF	 Duplex SMF	 Duplex SMF	 Duplex SMF	 Duplex SMF	 Duplex SMF
Standard	June 2010 IEEE 802.3ba	March 2011 10x10 MSA	August 2011 10x10 MSA	June 2010 IEEE 802.3ba	August 2011 10x10 MSA	June 2010 IEEE 802.3ba
Electrical Signaling (Gbps)	10 x 10	10 x 10	10 x 10	10 x 10	10 x 10	10 x 10
Optical Signaling (Gbps)	10 x 10	10 x 10	10 x 10	4 x 25	10 x 10	4 x 25
Power (W)	~8	~19	~19	~24	TBD	TBD
Target Availability	2012	Now	Now	Now	2012	2012
Relative List Price	\$	\$\$\$	\$\$\$\$	\$\$\$\$\$	TBA	TBA

© 2011 Brocade Communications Systems, Inc.

16



Source: Brocade Communications Systems

Summary

Demands of providing more connections in the same space have led to new design for Ethernet interfaces. The following module types and formats have results for various Ethernet applications

- 1 Gigabit Ethernet: SFP (Mini-GBIC)
- 10 Gigabit Ethernet: SFP+, XFP (XENPAC, XPAK, X2)
- 40 Gigabit Ethernet: QSFP+
- 100 Gigabit Ethernet: CFP

3.6.5 Energy Requirements of Copper and Glass Fiber Interfaces

At this point we present a comparison of power consumption requirements of copper and glass fiber interfaces. Objectives of savings costs and energy must be considered in all details from the very start of the data center planning process. The question therefore arises with regard to energy consumption of what media and interfaces are optimal.

Acquisition costs for glass fiber systems are definitely higher than those for copper systems. However, the situation appears somewhat different when issues of power consumption and in turn operating costs are examined. This difference is 40%.

Power consumed by a 10 Gbit/s Switch Chassis:

336 glass fiber connections	Power	336 copper connections	Power
7 modules with 48 glass fiber ports at 1.5 W *)	504 W	7 modules with 48 copper ports at 4 W*	1,344 W
Total ventilation	188 W	Total ventilation	188 W
NMS module	89 W	NMS module	89 W
10 GB fiber uplinks	587 W	10 GB fiber uplinks	587 W
Total (with glass fiber ports)	1,37 kW	Total (with copper ports)	2,21 kW

*) Average according to information from various manufacturers, 2012

A switch with glass fiber ports consumes only 60% of the power of a copper port. This results in the following values for total energy consumption (also see section 1.9):

Power consumption of glass fiber switch	1.37 kW	Power consumption of copper switch	2.21 kW
DC/DC conversion	0.25 kW	DC/DC conversion	0.40 kW
AC/DC conversion	0.42 kW	AC/DC conversion	0.69 kW
Power distribution	0.05 kW	Power distribution	0.09 kW
Uninterruptible power supply	0.19 kW	Uninterruptible power supply	0.31 kW
Cooling	1.47 kW	Cooling	2.36 kW
Switchgear in power distribution	0.14 kW	Switchgear in power distribution	0.22 kW
Total power requirement	3.9 kW	Total power requirement	6.3 kW

Operating costs become very different when other different PUE factors (see section 1.10 and 2.4.3) are taken into consideration. The higher one-time acquisition costs for glass fiber technology pay for themselves after a short time due to the significantly lower regular operating costs. Company-specific, proportional data center costs such as maintenance, monitoring and costs for space were not included in this model. The following figures are based on R&M research and comparison data typical in the industry.

Power costs for Switching Hardware	Glass Fiber Switch	Copper Switch
Power consumption (during operation)	3.9 kW	6.3 kW
Hours per year	24 h x 30.5 days x 12 months = 8,784 h	
Power consumption per year	34,258 kWh	55,339 kWh
Power costs per kWh in Germany	0.15 € (industrial customers)	
Power costs per year	5,138.70 €	8,300.85 €

Energy costs by energy efficiency		
PUE factor = 3.0	15,416.10 € / year	24,902.55 € / year
PUE factor = 2.2	11,305.15 € / year	18,261.85 € / year
PUE factor = 1.6	8,221.90 € / year	13,281.35 € / year

3.6.6 Trends in Network Technology

Foresighted data center planners and operators always take long-term technological developments into consideration. These developments generally involve life cycles of 15 to 20 years. At the same time, data centers must have the ability to cope with short-term IT trends as well as the frequent turnover experienced in terms of active components. This section describes a few current trends that may have consequences on planning and operating data centers. It must be generally assumed that demands on networks and data centers are constantly growing.

- The market and consumers, companies and organizations constantly make more intensive use of information and communication technology (ICT). Fixed and wireless networks continue to merge closer and closer (convergence). The wide-scale use of mobile devices is increasing the volume of the data that must be transported and stored. The hunger for bandwidth is continuing to grow.
- Power densities in data centers are growing, and servers are becoming more and more efficient. These trends require infrastructures that are more compact.
- High ICT availability is becoming increasingly important. 24/7 services is a basic expectation of companies.
- Professionalization in data centers is making great strides. This trend sometimes requires the construction of new facilities, modernization or outsourcing.
- Increasing capacity utilization of data networks through cloud computing, virtualization and the "Internet of things".
- Solutions for digital archiving are being driven forward. Legislation and risk management demand storage systems that are secure over the long-term and available at all times. The importance of storage is increasing.
- Energy efficiency is gaining critical significance. Data center power consumption must be contained in all cases, for reasons of sustainability, climate protection and profitability.
- Rising need for plug-and-play solutions that can be installed more efficiently, quickly and without resulting in error – in spite of a shortage of personnel.
- Further extension of systems for direct company communication. Development of communities and extension of links from data centers.

Another megatrend is the introduction of data center infrastructure management (DCIM). The objective of this development is to provide real-time monitoring for all data center components, processes, performance indicators and status conditions. This monitoring is based on data like temperature, power consumption, storage capacity, rack equipment and a number of other information. The goal of DCIM is to develop data centers that are run optimally in terms of profitability, organization and technology. This should allow transparency to be more easily achieved, and trends and growth better observed.

3.7 Virtualization

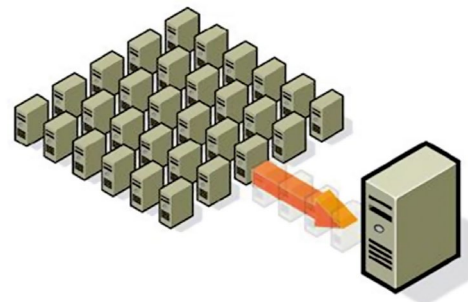
The trend toward virtualization in areas of IT already has a number of consequences for data centers. They can offer professional virtualization services in a wide number of areas and thus open up additional markets for potential. Virtualization measures can contribute to operating server resources more efficiently and economically and saving energy. Virtualization is one method of serving a large number of customers with the minimum number of machines possible. Conversely, users of virtualization can outsource certain services or programs without having to also operate a complete physical server. However, virtualization does require an infrastructure that is especially high-performance; a requirement that must be taken into consideration when planning and/or upgrading a data center.

Virtualization is especially considered the consolidation of multiple virtual servers, especially a large number of virtual servers, onto one device in the data center (also see sections 1.8, 1.10 and 3.6.2). Virtualization can be implemented in two ways:

- Virtualization through software (e.g. VMware)
- Virtualization at the hardware level (e.g. AMD64 with Pacifica)

The advantages of virtualization include:

- Less hardware
- More efficient energy consumption
- Easier resource management
- Clear patching and cable management
- Better security management
- Simple recovery processes
- Increased flexibility with regard to applications
- Lower costs of acquisition and operation



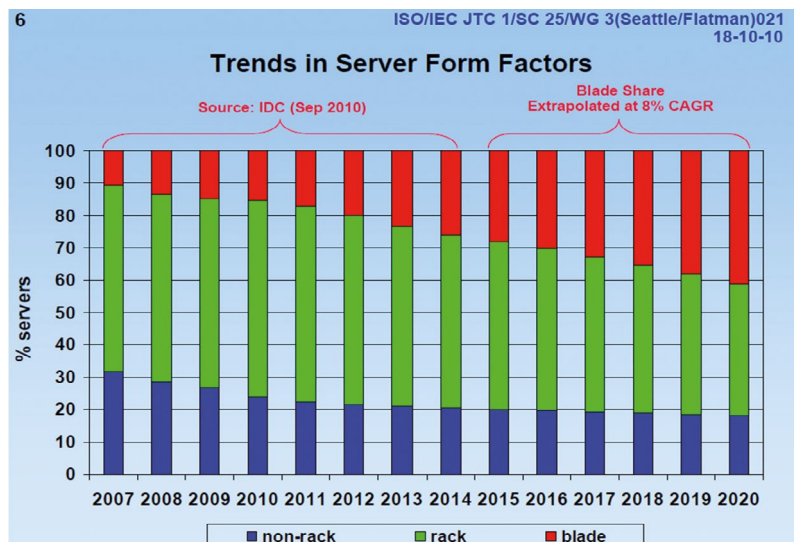
Consequences on cabling systems:

- Virtualization requires higher-performance connections, so-called fat pipes.
- Virtualization requires more connections between servers and switches (due to aggregation).
- Virtualization requires additional redundant connection (due to availability requirements).

3.7.1 Server/Storage/Client Virtualization Basics

An fundamental objective of virtualization is to get maximum utilization out of a computer or server, and to use as few devices as possible to support as many users as possible. In order to achieve this, several virtual servers, or even a large number of virtual servers are packed into one device (see above). An abstraction layer that exists above the level of the operating system simulates to users that they are each using their own server while in reality, a number of customers are using the same device at the same time. The connection between servers and users is uncoupled, so to speak.

Virtualization lets data center operators combine a number of servers into one homogeneous environment and manage them in a uniform manner. This allows operators to increase capacity utilization of both individual machines as well as the entire data center. This effect can be multiplied even further by implementing blade servers (see section 3.6.2) and condensing the server infrastructure.



The adjacent graphic shows the evolution of server condensation.

Server Virtualization

Server virtualization involves provisioning complete virtual machines (VM) that behave like physical servers. In the process, multiple instances of one or more operating systems are run together simultaneously on a single machine. A software object runs in a flexible manner, independent of the underlying hardware, since, from the standpoint of the base operating system (host), the object is decoupled from the hardware. The VM installation packages available on the markets can normally install four to eight machines on one CPU.

Storage Virtualization

Storage virtualization takes this process one step further. In this process, even computing and storage capacities are decoupled from the actual hardware. A single physical environment is simulated and presented to the user. Resources in the background can be used more efficiently and extended in a flexible manner. Storage virtualization is realized in a storage pool that encompasses the various hardware components and treats them as equals. Management of stored data is carried out automatically for the most part. Rules are defined in a storage management tool. This allows for flexibility in categorizing and copying data or moving data into different virtual hardware storage systems.

However, each application does require an infrastructure which must always be available, in a cost-effective manner and at the right time. In addition, the system must also take into account legal requirements with regard to retaining data and documentation (see section 2.3.4).

As a consequence of storage virtualization, data centers have the options of moving toward storage consolidation solutions. In so doing, storage area network switches (SAN switches) and Fiber Channel can be implemented to give operators the ability to use the entire existing storage space virtually and more efficiently. Data can be brought together into fewer systems which better utilization and improved performance. By contrast, the classic dedicated assignment of storage and servers to separately reserved resources is significantly less efficient.

Client Virtualization

A technology that continues to be developed further is client virtualization, or desktop virtualization. This method simulates an entire PC desktop at one central location, the data center. This allows multiple users to execute application programs on a remote computer, simultaneously and independent of one another.

By virtualizing desktops, each user gets his/her own virtual system environment, that in principle behaves like a complete local computer. In the process, a host provides operating system instances that are individually configured. This process should not be confused with the provision of a terminal server. In this case, multiple users share the resources of a specially configured operating system.

- **Advantages:** Systems can be individually configured and hosted at a central location. Common user hardware is utilized better than decentralized clients.
- **Disadvantages:** Operating systems must be maintained redundantly. This increases resource requirements and also requires reliable network connections.

Storage Virtualization and Storage Consolidation Classic

Structure

The adjacent graphic shows an example of a classic server and storage structure in a data center with separate networks.

Each server is connected physically to two networks, the LAN for communication and the SAN for storage media.

This leads to an inefficient use of all available storage capacities, since each storage of an application is handled separately and its reserved resources must be made available.

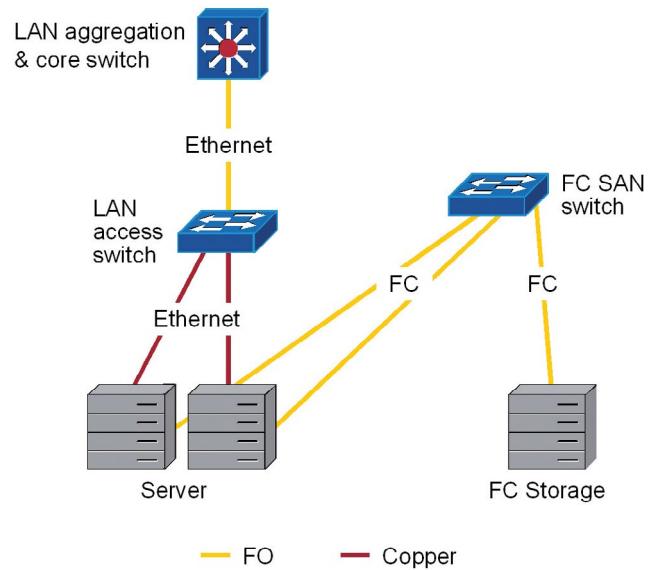
Data center servers in the access/LAN area are typically networked together via copper cabling. Glass fibers are the medium of choice in the area of aggregation and core areas due to their ability to grow with future requirements.

Fiber Channel is the typical application for data center storage.

3.7.2 Converged Networks, Effect on Cabling

Expectations are that the communication protocols of Ethernet for LAN and Fiber Channel for SAN will merge in the future (convergence). This unification makes possible a structure known as Fiber Channel over Ethernet (FCoE).

The Fiber Channel Industry Association (FCIA) recommends a 3-stage path for migrating from FC to FCoE. The migration must take into consideration the reusability of hardware and the service lives of individual components.

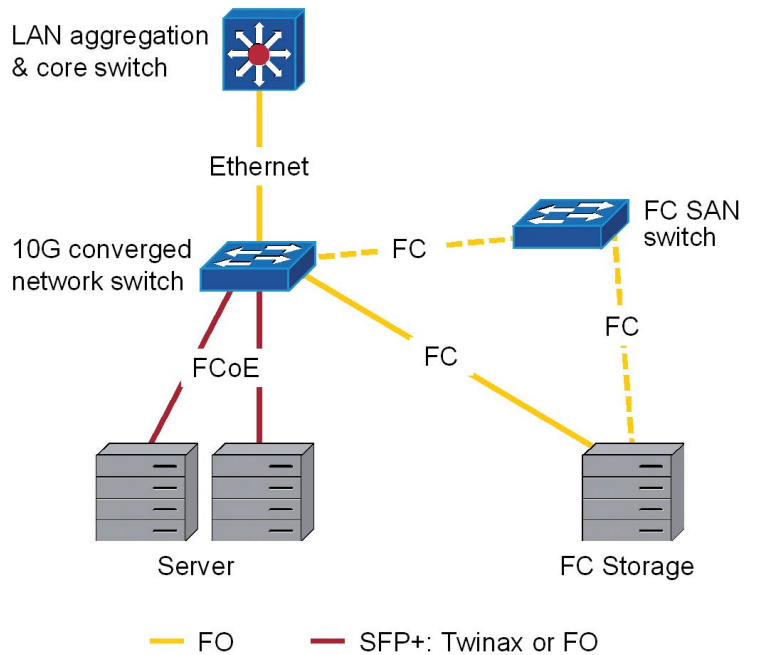


Stage 1

Installation of a new converged network switch will allow existing hardware to continue to be used for the time being.

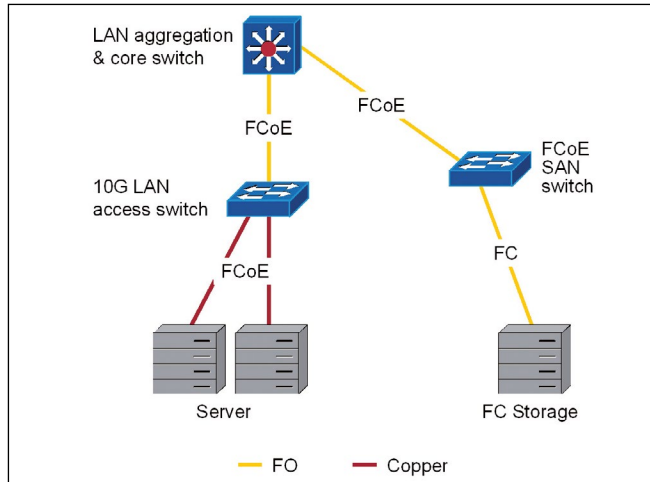
The converged switch can also directly connect together storage systems in smaller data centers. SAN switches installed in larger data centers will prevent possible bottlenecks. The servers here are connected via converged adapters.

The FCIA recommends SFP+ (glass fiber and copper) as its transceiver interface of choice. If copper cables are used, installation is then only possible over 7 m using Twinax cables. Future system enhancements must be based exclusively on glass fiber cabling in order to respond to convergence demands.



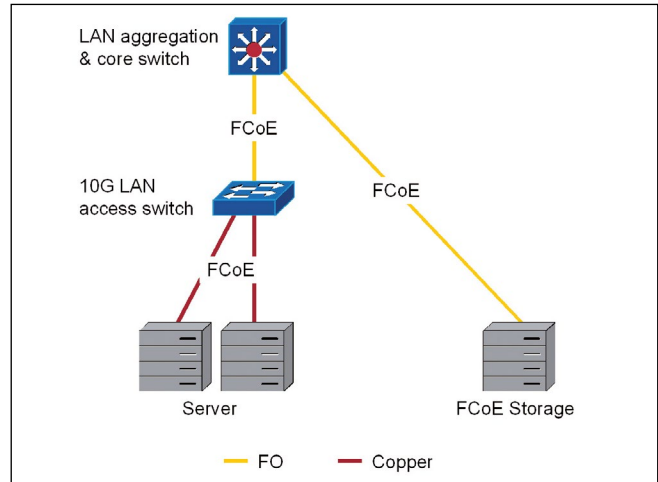
Stage 2

The second stage of the migration provides converged switches with an FCoE uplink and integrates it with FCoE in the backbone.



Stage 3

The third stage of the migration connects the FCoE solutions directly to the core network. FC has now been completely replaced.



3.7.3 Trend toward Virtualization and Cloud Computing

Data centers today can assume that their needs for virtualization will continue to grow. One force driving virtualization is the demand for cloud computing. Virtualization is accepted by the market as a technical prerequisite that will allow IT services to be provided faster, more flexibly and more cost-effectively than in the past. The higher the level of virtualization, the more sustainable a given cloud computer application will be. However, applications and users still expect unconditional availability of computing power and storage space.

3.8 Communication Protocols

Protocols are used in the data transmission process to prepare information for transport from point A to point B, on the basis of agreed rules. The use of protocols is a basic feature of the IT world, comparable to the use of envelopes for sending personal letters or cardboard packages for sending goods. These protocols are a basic component in transmission technology and transmission software.



The relationship between protocols and a network infrastructure and cabling is especially important factor in data center planning. Generally speaking: The more complex and demanding the data transmission, the higher performance the cabling must be.

The purpose of this section is to provide a general overview of common communication protocols. Numerous sources are available in IT technical literature and on the Internet for those who wish to find out more about the origin, definition and technical details of protocols.

Protocols can be divided into connection-oriented and connectionless protocols. A connection-oriented protocol establishes a connection before any data is transmitted, waits for confirmation and finally terminates the connection. A connectionless protocol is faster but unreliable, since it logs no information regarding establishment and termination of the connection or confirmation. Typical protocol types include:

- Transport-oriented protocols (OSI layer 1–4) & application-oriented protocols (OSI layer 5–7)
- Routable and non-routable protocols (concerning the ability to forward data through routers)
- Router protocols (decisions on data path selection, e.g. RIP, OSPF, BGP, IGRP)

Network protocols, also known as communication protocols or transmission protocols, regulate how data are transmitted between the computers or processes in a distributed system. These rules are based on interaction between syntax and semantics. Syntax = set of rules and formats which specifies the communication behavior (semantics) of the instances in the computers involved in the communication.

Various protocols, which are responsible for different tasks, are required for the data transmission process. In order to provide clear delimitation for these tasks, these protocols are organized into layers. Protocols structured in this way form a so-called protocol stack, the best-known of which is perhaps the TCP/IP protocol stack.

3.8.1 Implementation (OSI & TCP/IP, Protocols)

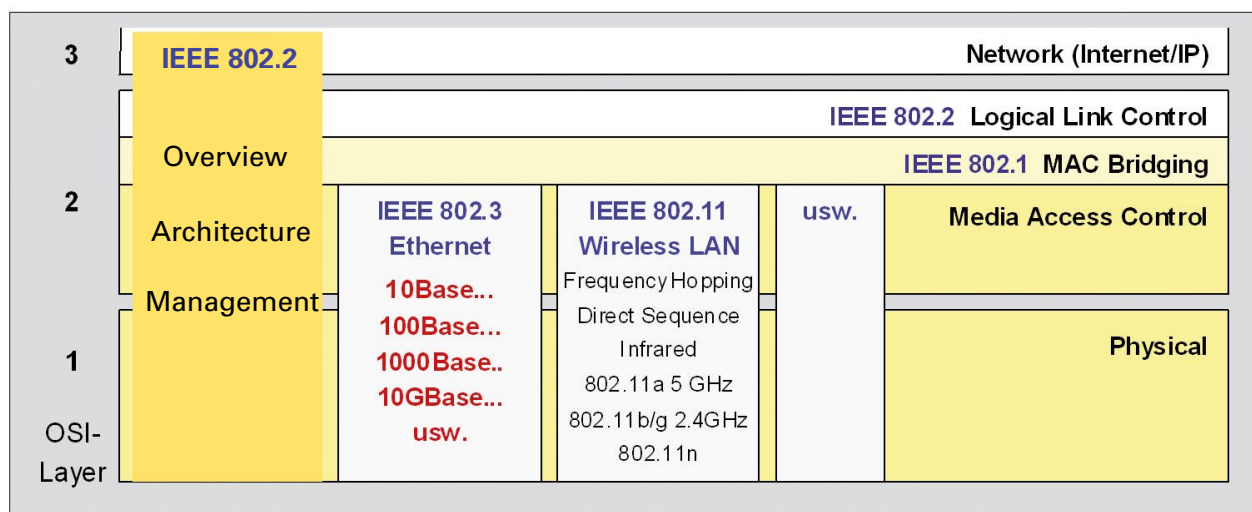
The ISO standardization organization created the OSI model as a basis for communication standards (ISO 7498 of 1984). OSI stands for Open Systems Interconnection. The purpose of this model is to facilitate communication between different networks and computer worlds. OSI protocols define not only application data, but also information on structures and processes. The model makes use of seven protocol levels, or layers, with clearly delineated functions. Data packets run through all seven layers on both the sender and receiver machines.

Layer 1 – Physical Layer

Layer 1 controls the establishment and termination of connections. It is responsible for the protocol information pattern, the information on the voltage level through which the logical information "1" and "0" is described. Cables and plug connectors as well as electrical and optical signals are assigned to this layer.

Layer 2 – Data Link Layer

Layer 2, the data link layer, checks whether data was transmitted without error. Bitstream correction functions exist in this layer. In addition, flow control takes place here, as well as cell numbering, in the event cells are transmitted. In LAN applications, layer 2 is subdivided into the sublayers called logical link control (LLC) and media access control (MAC). Sender rights are assigned by MAC. The well-known communication protocol Ethernet (IEEE 802.3) also resides on this layer. Network adapters and layer 2 switches are assigned to this layer.



Extract from OSI model.

Layer 3 – Network Layer

Layer 3 is responsible for routing information. This communication may be carried out a number of networks of different types. For the routing process to work, IP network addresses are read and evaluated, then this information is passed to the next stages (networks) using routing tables. In order to do this, router require communication parameters such as bit transmission rates, network load, threshold values and service quality. Routers and layer 3 switches are assigned to this layer.

Layer 4 – Transport Layer

Layer 4 controls end-to-end communication. When a connection becomes unstable or fails, this layer takes care of re-establishing the connection (handshake) as well as address conversions, if necessary. Devices with protocol functions specific to this layer are known as layer 4 switches.

Layer 5 – Session Layer

Layer 5 carries out and completes the session from the application layer. This layer also specifies whether the connection is full-duplex or half-duplex. Finally, it is responsible for monitoring and synchronizing the data stream.

Layer 6 – Presentation Layer

Layer 6 interprets the different data structures that arrive from different computer systems. This layer ensures that syntax is uniform or correct (with regard to character set, coding language, etc.). The sender's data format is converted into a device-independent format. In addition, cryptography is incorporated in this layer when data security is a requirement.

Layer 7 – Application Layer

Layer 7 passes the data that was transmitted up to user programs. This layer must naturally have the ability to communicate with a wide variety of applications, which of course makes standardization difficult. Common application protocols include HTTP, FTP SMTP and DNS.

Order of Events in a Transmission

The sender begins the information transmission in layer 7. It passes data packets from layer to layer until they reach layer 1. The information gets a header in every layer. This header is added to the front of the data to be transmitted. Layer 3 adds information including the IP source and destination addresses that allow routers to make appropriate selections for data paths. Layer 2 adds a checksum field as a basic security check for the information being transmitted. All additional information together form the frame.

As a result, significantly more information than just data actually runs over cables. The length of an Ethernet frame must be at least 64 bytes and may be a maximum of 1,518 bytes, or 1,522 bytes with frame extension. This extension contains additional identifying characteristics (tags) that are required for transmitting data in virtual local networks (VLAN).

Half- / Full-Duplex

Full-duplex and half-duplex describe the data transmission on the basis of direction and time. Half-duplex uses only a single channel for transmission, which can either send or receive data. Data streams in full-duplex mode flow in both directions, at the same time and at the same speed. Example: Gigabit Ethernet (1 Gbit/s) in full-duplex mode has a transmission speed of 2 Gbit/s.

TCP/IP

The transmission control protocol/Internet protocol (TCP/IP) was developed to make reliable data transmissions possible over large networks and networks of different types, and to allow networks to connect with one another. TCP/IP provides the technical open standard that made development of the Internet possible in the first place. Typical tasks for protocols with regard to data transmission in the Internet include:

- Retrieving and loading websites and hypertext files (HTTP and HTTPS)
- Sending and receiving e-mails (SMTP, POP3, IMAP)
- Uploading files to or downloading files from servers (FTP, HTTP and HTTPS)

Even though the OSI model is recognized around the world, it still has a somewhat academic nature. The TCP/IP reference model and the TCP/IP protocol stack lie closer to actual practice in the IT world and are based on the structure of tried and tested protocols. Both models functions according to the principle of transmitting data down through the stack as it is sent, then up through the stack as it is received.

Comparison of both models:

OSI layers		TCP/IP layers		Protocol examples		Coupling elements
7	Application	4	Application	HTTP, HTTPS, FTP, SMTP, IRC, POP3, Telnet, etc.	DHCP, BootP, NTP, TFTP, LDAP, CLDAP, SNMP, etc.	Gateway, Content Switch, Layer 4 to 7 switch
6	Presentation					
5	Session					
4	Transport	3	Computer	TCP	UDP	Router, layer 3 switch
3	Network	2	Internet	IPv4, IPv6, ICMP, IGMP, etc.		
2	Data Link	1	Network access	Ethernet, wireless LAN, FDDI, etc.		Bridge, switch
1	Physical					Cabling, repeater, hub, media converter

3.8.2 Ethernet IEEE 802.3

Ethernet technology has been revolutionizing the world since 1973. In the beginning there only existed a single fascinating idea: computers should have the ability to talk to each other. Today it is natural for computers to exchange their information over networks and defined protocols – whether this is in local data networks or over long distances. At that time, the computer scientist Robert Metcalfe shaped the essential basics of this packet-switched network technology for cable-connected data networks that he called Ethernet (a combination of the words ether, or air, and network).

The reference to air is founded in the historical assumption that it is the medium for spreading waves, radio waves to be specific. The packet principle was selected since data packets are self-contained and can circulate networks independently and flexibly. Every packet knows its source and its destination. This way the process is not dependent on specific transmission speeds or failures on individual path segments.

Since February 1980, the IEEE 802 project maintained by the standardization organization IEEE has been stamping out further advanced principles for Ethernet. The 802.3 work group of the IEEE 802.3 handles specifications for local data networks. Ethernet activities in a data network run on layers 1 and 2 (see section 3.8.1). Ethernet protocols define cable types, plug connectors and forms of transmission for the physical connections between active components or stations in a network. One essential element of Ethernet is the regulation of asynchronous station access to common media: This is known as Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

The name Ethernet has become synonymous with a large portion of network and protocol technology. Ethernet has virtually dominated the market since the 1990s. The success of Ethernet is based on the favorable acquisition costs provided by standardized systems as well as reliability, ease of use and scalability. This has led to its wide popularity.

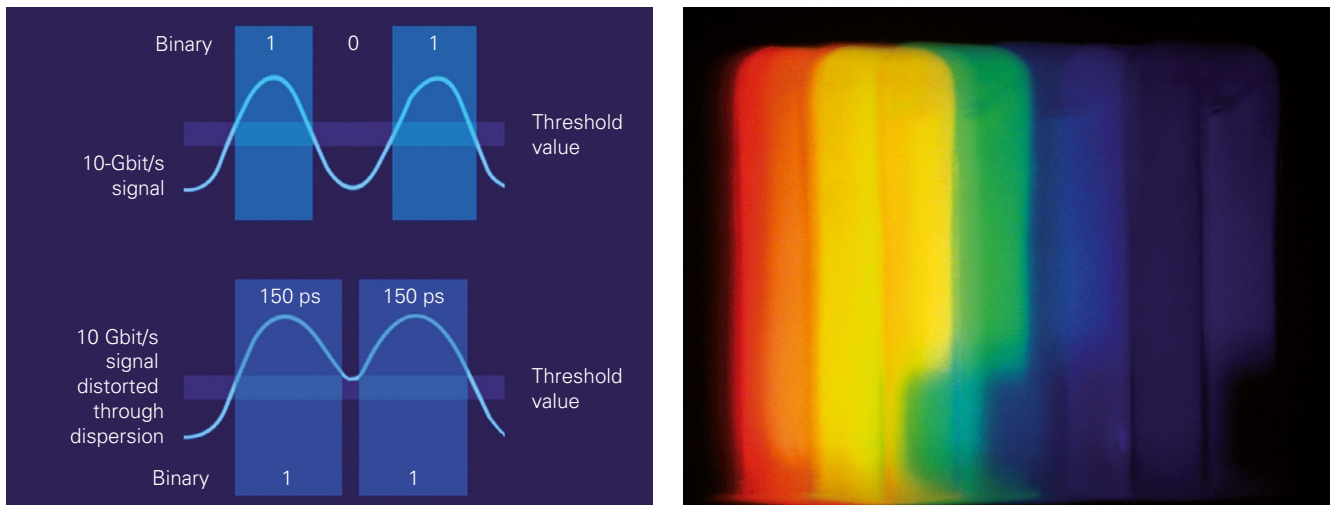
A key consideration in data center planning are the future plans being developed by IEEE 802.3 committees, now that they have established 10 Gigabit Ethernet. The most important topics in this area include:

- 40 and 100 Gigabit Ethernet
- Enhancements of Power over Ethernet (PoE)

A central theme of 40 and 100 Gigabit Ethernet is the search for cost-effective cabling solutions, in particular cost-effective glass fiber cabling. This is because these technologies require a great deal more glass fiber technology in order to have the ability to manage growth at all, in terms of bandwidth and data streams. Approaches for this are shown below.



40GBASE-SR4 and 100GBASE-SR10 technologies are designed to support maximum distances of 100 meters using OM3 glass fibers in accordance with the IEEE 802.3 Section Six Standard. Connections up to a length of 150 meters are feasible if OM4 glass fibers are used. Cabling routes of just this length already allow for data center installation of most (> 85%) typical optical channels. Appropriate frames of reference can therefore be provided for data center planning. Restricting distances to these lengths, relatively short for glass fiber connection, is based on a very good reason: cost. Cost-effective transceivers can be implemented over these short distances (also see section 3.6.4) and still ensure a quality signal transmission.



Parallel optical technology is the medium of choice for bundling 10 Gbit/s channels and thus paving the way for 40 and 100 Gigabit Ethernet (see sections 3.10.1 and 3.10.2). The 40 Gbit/s solution uses four glass fibers in each of the two directions, and the 100 Gbit/s solution ten fibers. A MPO plug connection is used as a connection (12-pin with 8 fibers for 40 GbE or 24-pin with 20 fibers for 100 GbE).

Lasers used in data centers provide additional potential for saving costs when equipping networks. Most data centers use surface emitting semiconductor lasers (vertical cavity surface emitting lasers/VCSEL, pronounced "vixel"). These components are easy to manufacture and cost-effective but still have a relatively large spectral width. The demands for this spectral width were softened in the IEEE 802.3 Section Six standard, from 0.45 nm to 0.65 nm. The result is higher chromatic dispersion, the phenomenon that spreads an optical pulse as it is transmitted through the optical fiber.

The reduction in technical demands still lies in a justifiable framework. In any case, system costs are lowered as a result. The shortened link lengths and higher insertion losses must be accepted as a consequence. For 10GBASE-SR, maximum losses amount to 2.6 dB over OM3. With 40GBASE-SR4 and 100GBASE-SR10, these are lowered to only 1.9 dB and 1.5 dB respectively for OM4.

Nevertheless, planners, installers and users can ensure the performance of new glass fiber networks. They make use of products that exhibit minimal optical losses. R&M's fiber optic assortment of products for data centers offers appropriate systems and complete pre-assembled solutions.

Glass fiber technology can therefore be tied to the historical success of Ethernet. The continued development of this technology into 40 and 100 Gigabit Ethernet is coming at the right time. It meets current needs and also provided sufficient investment security for the future.

At the same time, the advantages of high-performance copper cabling should not be forgotten. It should continue to provide valuable services in the future in many data center areas for managing data volume. In particular, the ISO 11801 Cat. 6_A/class E_A generation meets all conditions for fulfilling requirements of highly condensed Ethernet networks. In this connection we should also make reference to the unsurpassed performance values of R&M's innovative Cat. 6A connection module. With its module data center assortment of products R&M provides flexible, comprehensive solutions for copper cabling.

The following tables provide an overview of current Ethernet applications for copper and glass fiber cabling.

Ethernet Applications for Copper Cabling with Cat. 6 & Cat. 6A

Category & Class acc. ISO/IEC 11801			Cat. 6 - Class E		Cat. 6A - Class EA		
			shielded & unshielded		shielded & unshielded		
Topology			PL ²⁾	Channel ¹⁾	PL ²⁾	Channel ¹⁾	
Installation cable							
		AWG	Wire type				
IEEE 802.3 Section Three - 1000BASE-T		26	Solid	55 m	65 m	55 m	65 m
		26	Flexible	55 m	65 m	55 m	65 m
		24	Solid				
		23	Solid	90 m	100 m	90 m	100 m
		22	Solid	90 m	100 m	90 m	100 m

¹⁾ Channel calculation based on 2x5m patch cord (flexible)

²⁾ Permanent link and Channel length reduction if patch cord (flexible cable) >10m

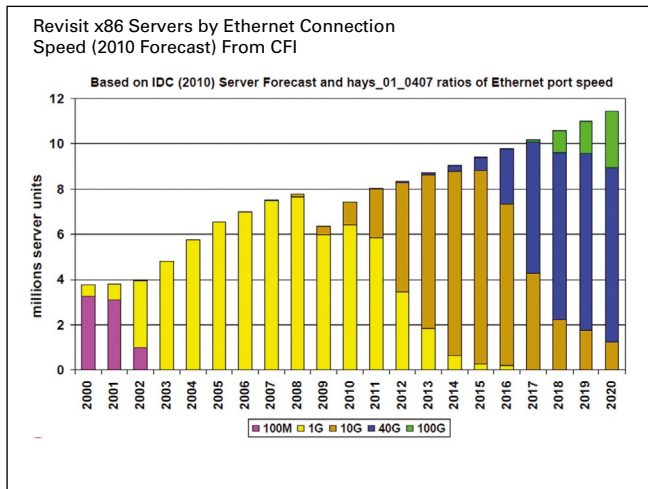
10GBASE-T, 10 Gigabit data transmission over copper cables, still uses a 4-pair cable for transmitting on all 4 pairs and allows a segment length of 100 m.

Ethernet Applications for Glass Fiber Cables with OM3, OM4 & OS2

Fiber type accord ISO/IEC 11801				OM3		OM4		OS2	
Wavelength				850nm	1300nm	850nm	1300nm	1310nm	1550nm
Overfilled modal bandwidth (MHz*km)				1500	500	3500	500		
Eff. Laser launch modal bandwidth (MHz*km)				2000		4700		NA	NA
				y)	z)				
ISO/IEC	8802-3	100BASE-	F	X	2km		2km		
	LED				11.0dB		11.0dB		
IEEE	802.3	1000BASE-	S	X	550m		550m		
	LED				3.56dB		3.56dB		
IEEE	802.3	1000BASE-	L	X	550m		550m	5km	
	LED				2.35dB		2.35dB	4.57dB	
IEEE	802.3	10GBASE-	S	R	300m		400m		
	VCSEL				2.6dB		2.9dB		
IEEE	802.3	10GBASE-	L	R				10km	
	Laser							6.0dB	
IEEE	802.3	10GBASE-	E	R					30km (11) 40km (11)
	Laser								
IEEE	802.3	10GBASE-	L	X	300m		300m	10km	
	WDM			4 ^{k)}	2.0dB		2.0dB	6.0dB	
IEEE	802.3	10GBASE-	L	R	220m		220m		
	OFL			M	1.9dB		1.9dB		
IEEE	802.3	10GBASE-	S	W	300m				
	VCSEL				2.6dB				
IEEE	802.3	10GBASE-	L	W				10km	
	Laser							6.0dB	
IEEE	802.3	10GBASE-	E	W					30km (11) 40km (11)
	Laser								
IEEE	802.3	40GBASE-	L	R				10km	
	WDM			4 ^{k)}				6.7dB ^{a)}	
IEEE	802.3	40GBASE-	S	R	100m		150m		
	VCSEL			4 ^{o)}	1.9dB ^{b)}		1.5dB ^{b)}		
IEEE	802.3	100GBASE-	L	R				10km	
	WDM			4 ^{k)}				6.3dB ^{a)}	
IEEE	802.3	100GBASE-	E	R				30km (15) 40km (18) ^{a)}	
	WDM			4 ^{k)}					
IEEE	802.3	100GBASE-	S	R	100m		150m		
	VCSEL			10 ^{o)}	1.9dB ^{b)}		1.5dB ^{b)}		

- a) These channel insertion loss values include cable, connectors and splices.
- b) The channel insertion loss is calculated using the maximum distances specified in Table 86-2 and cabled optical fiber attenuation of 3.5 dB/km at 850 nm plus an allocation for connection and splice loss given in 86.10.2.2.1.
- k) Wavelengthdivision-multplexed lane assignment
- o) Number of fiber pairs
- y) Wavelength: S=short 850nm / L=long 1300/1310 / E=extralong 1550
- z) Encoding: X=8B/10B data coding method / R=64B/66B data coding method / W=64B/66B with WIS WAN Interface Sublayer

Trend



In R&M's estimation, the trend in data centers is clearly leading over 10 Gigabit Ethernet to 40/100 Gigabit Ethernet. This confirms the forecast shown in the graphic to the left, based on the spread of servers with fast Ethernet ports.

The state of technology is server interfaces being designed for use of 10 Gigabit Ethernet. Expectations are that blade servers will be equipped with adapters for 40 Gbit/s. Even switches with uplinks for 40 and 100 Gbit/s are no longer just a Utopian dream.

The migration to more sophisticated technologies will extend over a longer period. This will result in multiple stages being operated in a single network: 10, 40 and 100 Gigabit Ethernet. This trend demands full compatibility and prudent planning of cabling systems.

3.8.3 Fiber Channel (FC)

Fiber Channel is a protocol provided for serial, continuous high-speed transmission of large volumes of data. Storage area networks (SAN) run on the Fiber Channel standard. Transfer rates with this technology reach 16 Gbit/s. Copper cable is used for transmission within storage devices and glass fiber cable for connecting storage systems with one another.

Fiber Channel assigns a WWNN (world wide node name) for each device, as well as a WWPN (world wide port name) for each port of a device. This 64-bit value therefore provides every Fiber Channel device with a unique identification feature.

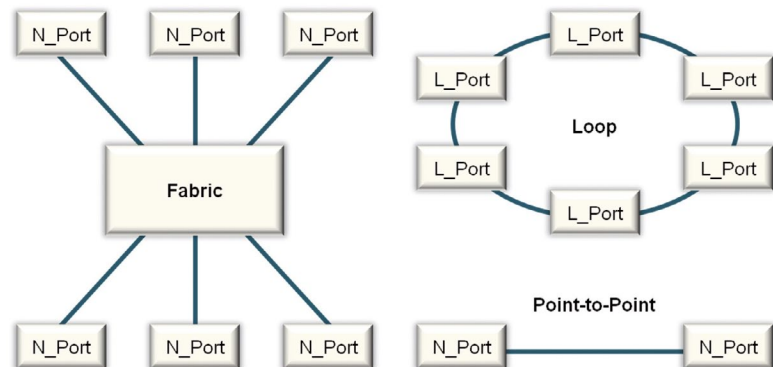
Fiber Channel relies on other protocols such as SCSI or IP in the higher layers of the OSI layer model. This facilitates the use of existing drivers and software. Fiber Channel achieves a useful data capacity of over 90%, as opposed to Ethernet which only achieves 20% to 60%.



WiebeTech FC Host Bus Adapter:
• 2 x LC • PCI Express x8 • 4 Gbit/s

Topologies

In general, Fiber Channel is used in the design of two topologies: Fiber Channel Switched Fabric (FC-SW) and Fiber Channel Arbitrated Loop (FC-AL). Terminal devices in FC-SW are connected through point-to-point connections. FC-AL is a logical bus in which devices share the data transmission rate.



FC-AL is frequently used as an entry point for constructing storage area networks. FC-AL is especially suitable for small clusters in which multiple physical nodes access a mass storage system. Up to 127 devices can be operated in an FC-AL bus. They share transmission rates from 133 MBit/s up to 8 Gbit/s. FC-AL cabling usually runs in a star configuration over a Fiber Channel hub, or devices are connected in series.

FC-SW is a higher-quality solution. It allows the highest performance and most reliable Fiber Channel applications to be realized. The Fiber Channel switch, or director, in the center of the system connects all devices with one another. This way point-to-point connections can be set up between any devices.

Reliability in Fiber Channel installations can be increased through redundancy, implemented by means of two independent switched fabrics. In the process each storage subsystem and each server is connected to each of the two fabrics using at least one HBA (host bus adapter). This configuration eliminates one single point of failure. In view of demands of high availability, all arguments generally speak in favor of using FC-SW.

Fiber Channel Applications for Glass Fiber Cables with OM3, OM4 & OS2

Fiber type accord ISO/IEC 11801	OM3		OM4		OS2	
Wavelength	850nm	1300nm	850nm	1300nm	1310nm	1550nm
overfilled modal bandwidth (MHz*km)	1500	500	3500	500		
eff. Laser launch modal bandwidth (MHz*km)	2000		4700		NA	NA
1G Fiber Channel 100-MX-SN-I (1062 Mbaud)	860m 4.6dB		860m 4.6dB			
1G Fiber Channel 100-SM-LC-L					10km 7.8dB	
2G Fiber Channel 200-MX-SN-I (2125 Mbaud)	500m 3.3dB		500m 3.3dB			
2G Fiber Channel 200-SM-LC-L					10km 7.8dB	
4G Fiber Channel 400-MX-SN-I (4250 Mbaud)	380m 2.9dB		400m 3.0dB			
4G Fiber Channel 400-SM-LC-M					4km 4.8dB	
4G Fiber Channel 400-SM-LC-L					10km 7.8dB	
8G Fiber Channel 800-M5-SN-I	150m 2.0dB		190m 2.2dB			
8G Fiber Channel 800-SM-LC-I					1.4km 2.6dB	
8G Fiber Channel 800-SM-LC-L (4250 Mbaud)					10km 6.4dB	
10G Fiber Channel 1200-MX-SN-I (10512 Mbaud)	300m 2.6dB		300m 2.6dB			
10G Fiber Channel 1200-SM-LL-L					1km 6.0dB	
16G Fiber Channel 1600-MX-SN (10512 Mbaud)	100m 1.9dB		125m 1.9dB			
16G Fiber Channel 1600-SM-LC-L					10km 6.4dB	
16G Fiber Channel 1600-SM-LC-I					2km 2.6dB	

Source: thefoa.org

Fiber Channel provides the following advantages for storage networks:

- Broad support by hardware and software manufacturers
- Higher level of technological maturity
- High performance
- High-availability installation (redundancy)

3.8.4 Fiber Channel over Ethernet (FCoE)

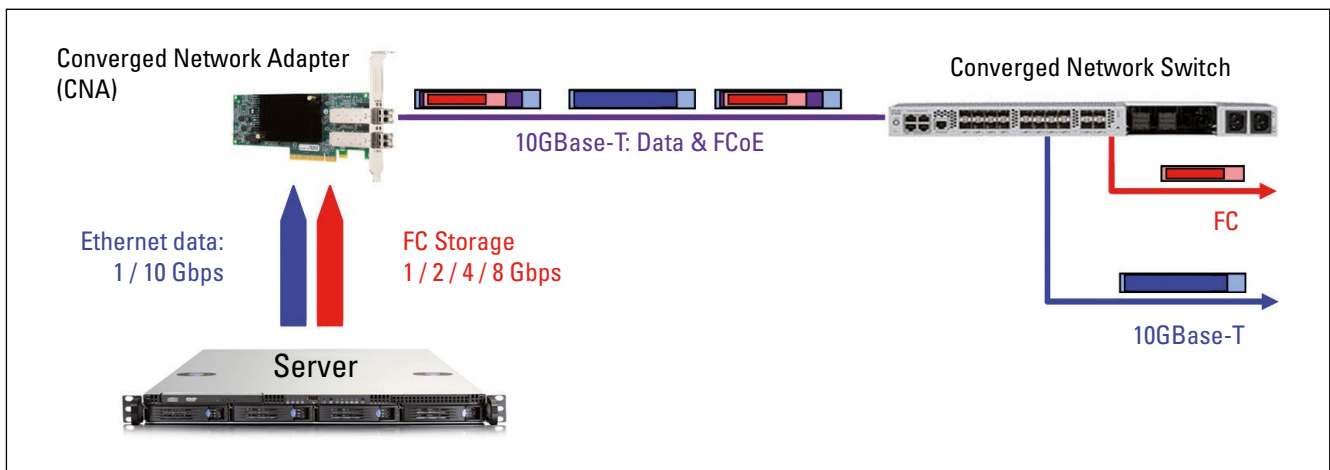
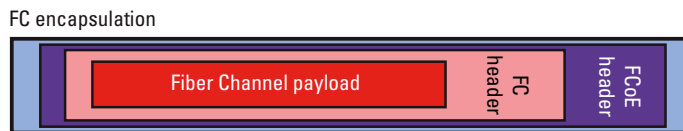
The communication protocol FCoE makes it possible to use a single infrastructure for both Fiber Channel as well as Ethernet applications. This means that one can especially play off the advantages of Ethernet – flexibility, scalability and bandwidth. FCoE is used in networks with full-duplex Ethernet. However, it does use the Fiber Channel framework.

Disadvantages of the classic Ethernet protocol lie in its low reliability, e.g. when frames are lost because of overloading. In order to improve this situation, the system runs on data center bridging (see section 3.8.7).

FCoE can contribute to reducing the complexity of network structures since it can be considered a form of virtualization on the basis of physical media that extend up to host systems for virtualized servers. A specific need for such consolidation possibilities exists in the course of implementing 10 Gigabit Ethernet. The cost benefits are obvious, since the expenses for passive infrastructure, network interface cards, power supply and heat dissipation are reduced.

Converged 10 GbE

The combination of 10 Gbit/s Ethernet and Fiber Channel has led to Converged 10 GbE, which includes FCoE. In this process, FC packets are encapsulated in the header of the Ethernet frame. This solutions allows for the use of a converged Ethernet topology. If switches are also equipped with FCoE, they can then manage a variety of packet sizes and provide equal support for FC and iSCSI storage as well as LAN

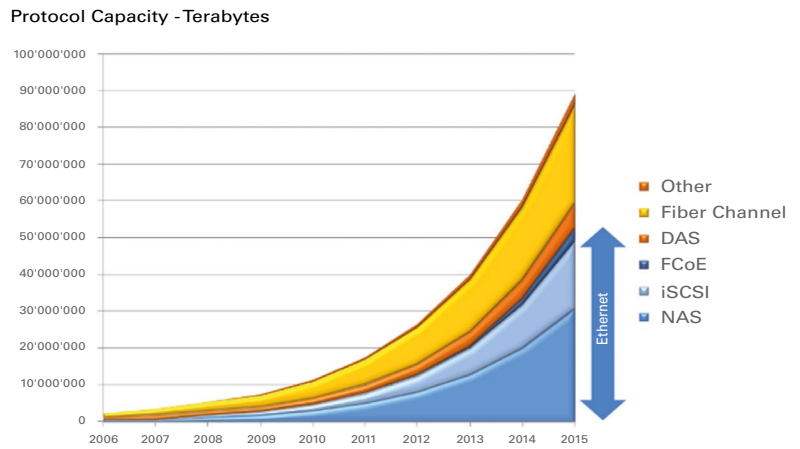


A frame for Fiber Channel data comprises 2,112 bytes, consisting of the payload (the actual data for transport) as well as header and checksum field. Better performance can be achieved through the use of jumbo or baby jumbo frames. This avoids the necessity of having to break up an FCoE frame into two Ethernet frames and then putting the frames back together. Ethernet infrastructures that must support FCoE should be designed so they transmit data completely loss-free. This requirement is fulfilled by using the highest quality network technology possible and also by automatically breaking off the data transmission on the active component side when a buffer overflow is imminent.

The 3-stage migration from Fiber Channel to Fiber Channel over Ethernet is described in section 3.7.2.

3.8.5 iSCSI, InfiniBand and Remote Direct Memory Access

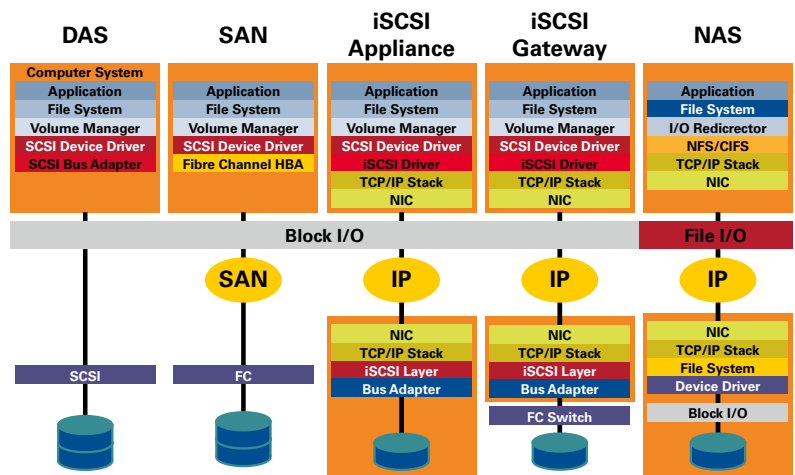
Other relevant protocols include iSCSI, InfiniBand and remote direct memory access (RDMA) that are especially necessary for block level access to network storage. As the graphic to the right shows, iSCSI is clearly playing a crucial role on the market. Data centers, however, rely primarily on the use of Fiber Channel since top-quality storage systems often support only this protocol and come equipped with the corresponding connectivity.



Graphic: IDC, 2012

Database operation in networks require that networks support block level access. As the graphic to the right shows, a number of different technologies are available for this purpose:

- DAS = Direct Attached Storage (parallel over SCSI und SAS)
- SAN = Storage Area Network (over FC)
- iSCSI (over TCP/IP, Ethernet)
- NAS = Network Attached Storage, File accesses only (over TCP/IP, Ethernet)

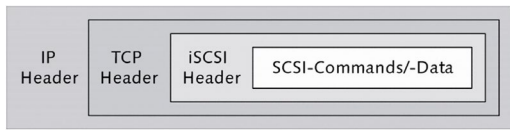


iSCSI

Storage resources are connected to servers via iSCSI (Internet small computer system interface). This protocol permits block level access to network storage systems via LAN. Under certain conditions, iSCSI can be used as an alternative to FCoE, so that data centers are spared from having to use a comparatively expensive Fiber Channel network.

iSCSI uses the SCSI protocol over TCP/IP. As in SCSI, a controller (initiator) is responsible for managing communication. One advantage of iSCSI is that storage arrays can be easily re-found, even if they are moved to another network subsegment. This is because iSCSI nodes are not based on its IP address. Instead, a 255-byte name and alias are used to identify an iSCSI node. iSCSI is suitable for both company network structures as well as wide area networks. This is because the protocol is capable of supporting routing due to its universal ability to communicate via TCP/IP.

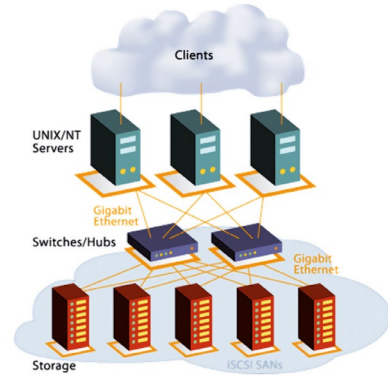
iSCSI in servers uses commercially available network interface cards. The iSCSI protocol runs over a software component. iSCSI host bus adapters with a Gigabit Ethernet connection can also be used. These adapters behave like SCSI controllers to the operating system.



The iSCSI protocol encapsulates SCSI commands and data into TCP/IP packets for the purposes of the Ethernet transmission. Common network standards and the same infrastructure solutions that are used in LAN can be used in SAN.

One disadvantage of iSCSI is its lower efficiency due to the increased requirements of the protocol (overhead) and the smaller packet sizes for Ethernet and TCP/IP. This results in higher loads for switches and servers as well as longer latencies. Transmission speeds depend upon the quality and performance of the given network technology. Due to latencies in the network, performance cannot match that of a locally installed SCSI system. However, iSCSI should perform satisfactorily at high bandwidths of 1 Gbit/s and greater.

iSCSI provides for high security. This is provided through CHAP authentication as well as encrypted packet transmission. However, iSCSI does not encrypt packets itself and encryption, e.g. through IPsec, must be integrated.



Performance comparison between iSCSI and FC:

Name	Transmission speed	Data throughput	Efficiency
Fiber Channel 1GFC	1.0625 Gbit/s	200 MByte/s FDX	97.24 %
iSCSI over GbE	1 Gbit/s	250 MByte/s FDX	91.81 %
Fiber Channel 2GFC	2.125 Gbit/s	400 MByte/s FDX	97.24 %
Fiber Channel 4GFC	4.25 Gbit/s	800 MByte/s FDX	97.24 %
Fiber Channel 8GFC	8.5 Gbit/s	1.6 GByte/s FDX	97.24 %
Fiber Channel 10GFC	10.52 Gbit/s	2.4 GByte/s FDX	97.24 %
Fiber Channel over 10 GbE (10GFCoE)	10.52 Gbit/s	2.4 GByte/s FDX	96.17 %
iSCSI over 10 GbE	10 Gbit/s	2.5 GByte/s FDX	98.61 %
Fiber Channel 20GFC	21.04 Gbit/s	5.1 GByte/s FDX	97.24 %

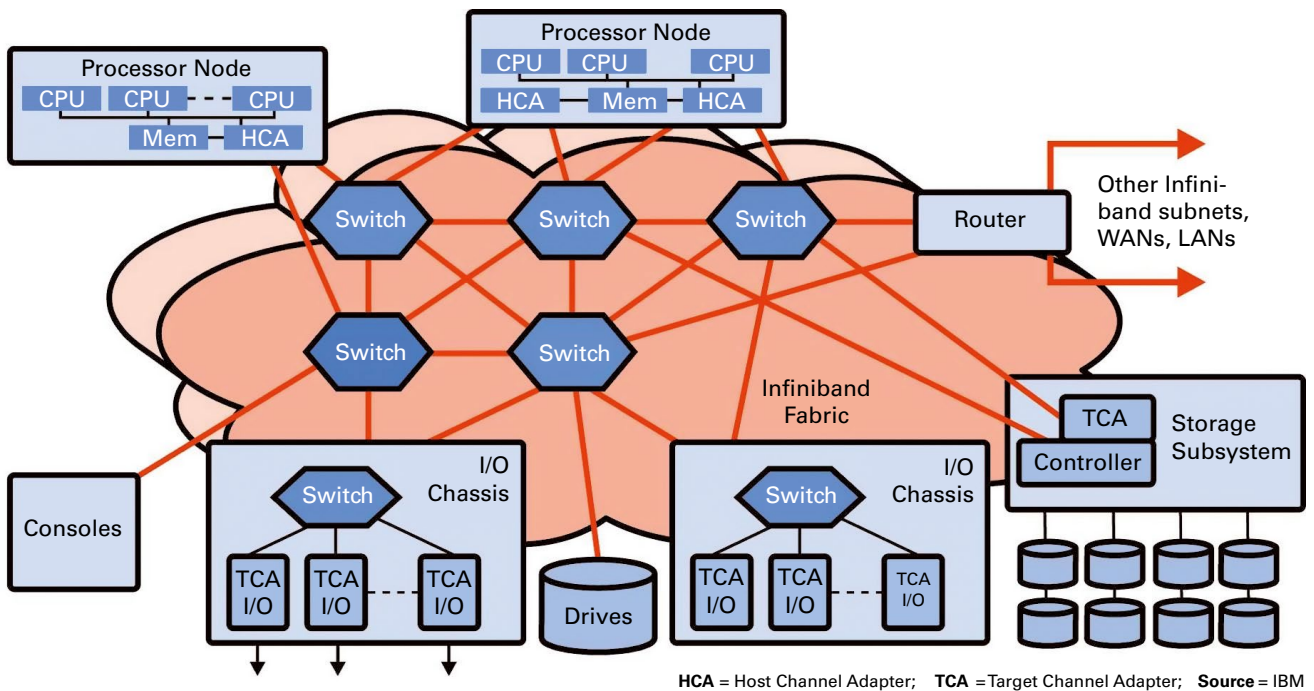
Source: LSI Corporation, 2011

InfiniBand

InfiniBand is a switched I/O system providing for fast data exchange between output units, processor nodes and mass storage devices. It is notable for its scalability as well as its options for quality of service and failover (redundancy function). It supports point-to-point connections and full-duplex operation.

InfiniBand transfers data in packets with a length of 4,096 bytes. In addition to its payload, every data packet has a header with addresses and error correction. InfiniBand allows for addressing of up to 64,000 devices in a network.

The InfiniBand concept is based on four components with one or more ports, which communicate with other components via a speed class (1X, 4X, 8X, 12X). These components are the host channel adapter (HCA), target channel adapter (TCA), switch and router.



As the graphic above shows, InfiniBand provides a logical yet flexible topology. HCAs communicate with one or more switches. I/O devices reach their switches via TCAs. HCA and TCA can also communicate with one another specifically over the switch. Multi-point connections are also possible. An InfiniBand router functions like a switch, but it can also transfer data between local subnets.



IB1X connector for 1xInfiniBand
Sierra Technologies



IB12X connector for 12xInfiniBand

Transmission links of up to 15 m can be realized using copper cabling. Media converters and glass fiber cabling must be used for longer distances. Media converters convert InfiniBand channels to fiber pairs. Optical ribbon cables and parallel optic technology (MPO plugs) come into use for this purpose. Transmission links of up to 10 km can be realized over single mode glass fibers.

InfiniBand can achieve higher transfer rates through bundling. Bundling is done in sets of 4, 8 or 12 links. This process allows transfer speeds of 10 and 30 Gbit/s to be achieved. This rate can even increase to 120 Gbit/s of raw data or 12 GByte/s of useful data if a 12X quad data rate link (QDR) is implemented. These connection types are used in larger systems like clusters, supercomputers and inter-switches. A listing of additional performance levels appears below:

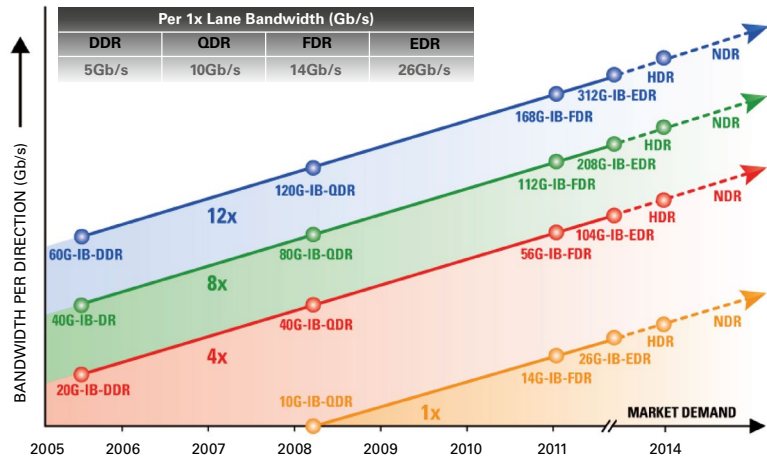
	SDR [8B/10B] Single Data Rate	DDR [8B/10B] Double Data Rate	QDR [8B/10B] Quad Data Rate	FDR-10 [64B/66B] Ten Data Rate	FDR [64B/66B] Fourteen Data Rate	EDR [64B/66B] Enhanced Data Rate
1X	2.5 (2) Gbit/s	5 (4) Gbit/s	10 (8) Gbit/s	10.3125 (10) Gbit/s	14.06 (13.64) Gbit/s	25.78 (25) Gbit/s
4X	10 (8) Gbit/s	20 (16) Gbit/s	40 (32) Gbit/s	41.25 (40) Gbit/s	56.25 (54.54) Gbit/s	103.13 (100) Gbit/s
8X	20 (16) Gbit/s	40 (32) Gbit/s	80 (64) Gbit/s	82.5 (80) Gbit/s	112.5 (109.1) Gbit/s	206.25 (200) Gbit/s
12X	30 (24) Gbit/s	60 (48) Gbit/s	120 (96) Gbit/s	123.75 (120) Gbit/s	168.75 (163.64) Gbit/s	309.38 (300) Gbit/s

[coding] / (usable data)

A glance into InfiniBand's road map shows plans to introduce HDR (high data rate) technology in 2014, and the NDR (next data rate) category in 2017. Expectations are that speeds of 50 Gbit/s can be achieved with HDR 1X, and 100 Gbit/s with NDR 1X um 100 Gbit/s.

InfiniBand advantages include:

- High bandwidth, currently up to 300 Gbit/s
- Low latencies from 1.0 to 1.2 μs
- Low CPU loading through use of remote direct memory access
- Extreme data integrity provided through cyclic redundancy checks (CRC)
- High availability provided through redundant, loss-free I/O fabrics with automatic failover paths and link layer multipathing
- High performance at an attractive price/performance ratio



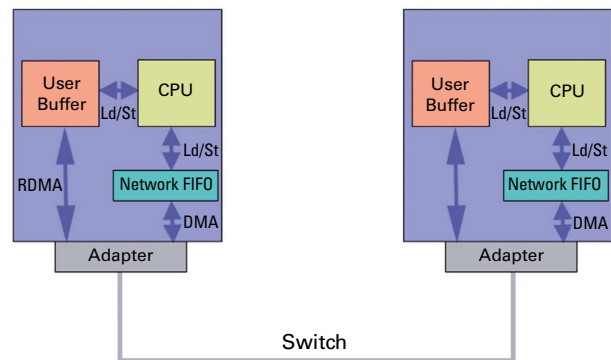
The total overhead required for power consumption, space and management in data centers decreases significantly through the use of InfiniBand. This decrease is achieved by consolidating the network, clustering and storage transfer into a single fabric. Its excellent QoS capabilities allow a variety of different workload and traffic classes to be defined.

Remote Direct Memory Access (RDMA)

Remote direct memory access is a method that allows for direct access of storage devices over networks. It runs over rapid, transparent data transfers provided by Fiber Channel and InfiniBand networks. InfiniBand with RDMA bypasses the protocol stack ("stack bypass"). Data are transferred directly from the RAM of one system into the RAM of another system. In spite of this, the process ensures application security, and also reduces the load on CPUs in host systems of high-speed networks.

RDMA provide an interface protocol that speeds up communication between servers and storage devices and servers and other servers. The process stands out because of its low overhead. It executes a direct, transparent, continuous transfer of data into the target memory. Finally, RDMA requires no process cycles from the remote system.

The iSCSI protocol must rely on a transfer protocol that supports RDMA. This requirement is met by making use of the iSER specification (iSCSI Extensions for RDMA). This protocol contains RDMA read/write services and transfers data directly into the SCSI I/O buffer.



Networking is carried out through use of the Internet Wide Area RDMA Protocol (iWarp). This solution results in extremely low latencies and is thus well-suited for high performance clusters. A big advantage of networking with iWARP is its compatibility with existing network infrastructures, management solutions and applications. Ethernet enhancements such as DCB (data center bridging, see section 3.8.7) also work well with iWARP. No special functions are required of network devices, since these do not have to process iWARP at all, as the protocol exists above the TCP layer. Finally, iWARP can be integrated into existing environments. The integration process can be facilitated through use of an open source RDMA software stack for iWARP provided by the Open Fabrics Alliance. The stack makes the hardware and applications required for iWARP transparent.

The IPoIB protocol (IP over InfiniBand) is also based on RDMA and provides a rapid method for IP address allocation. Its areas of application include iSER management and integrating sockets applications with SDP (Sockets Direct Protocol) on InfiniBand. SRP (SCSI RDMA protocol) also provides a storage protocol that is based completed on RDMA.

RDMA over Converged Ethernet (RoCE)

RDMA over Converged Ethernet (RoCE, pronounced "rocky") is an extension of InfiniBand (IB). Like FCoE (Fiber Channel over Ethernet), it replaces the two lowest layers of the IB architecture with convergent Ethernet (DCB, lossless). IB data are encapsulated in a RoCE packet. An existing infrastructure does not need to be adapted to support this enhancement. RoCE technology is based on broadband server I/Os.

A typical InfiniBand product is presented to show the enormous performance potential that can be achieved using technology and its associated protocols. The ConnectX-3 VPI adapter from Mellanox, manufactured in 2012 features the following characteristics:

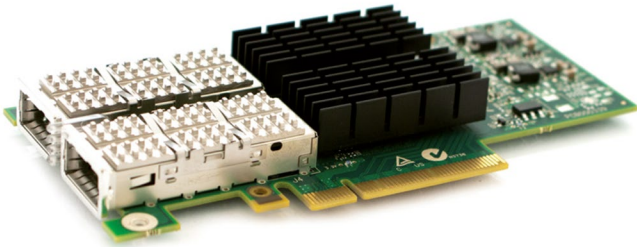


Image: Mellanox ConnectX-3 Virtual Protocol Interconnect Adapter, supports Open Fabric RDMA protocols and uses IBTA RoCE

- Compatible with InfiniBand IBTA specification 1.2.1
- 16 million I/O channels
- 1 μs MPI ping latency
- Up to 56 Gbit/s IB or 40 GbE per port
- Precision time synchronization
- Hardware-based QoS and flow control
- Fiber Channel encapsulation (FCoIB or FCoE)
- Ethernet encapsulation (EoIB) and DCB
- Hardware-based I/O virtualization & SR-IOV

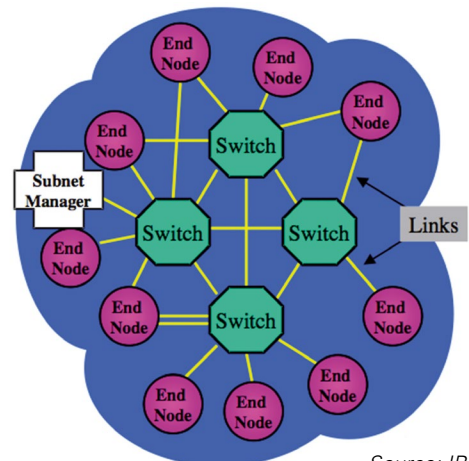


Image: Mellanox SX6036 56 Gbit/s InfiniBand switch with redundant power supply and ventilation, 36 QSFP ports (see section 3.6.4)

InfiniBand protocols stand out because of their stringency and determinism, and are designed for high throughput and minimal latencies. These protocols make it easier to implement RoCE than FCoE. This process requires only a few small procedures for monitoring communication on a continuous basis and intervening in case of faults. According to manufacturer measurements, RoCE minimizes the latency in convergent 10 GbE systems to 1.3 μs, and to just 0.8 μs in a 40 GbE network (determined by Voltaire and Mellanox). As a result, RoCE is suitable for time-critical applications in the fields of research and finance, and for database applications or applications involving extensive transactions.

InfiniBand Management

The InfiniBand fabric manages itself through a subnet manager component. The most important characteristics of this system are: Networks of any structure can be implemented (point-to-point, star, mesh). All nodes receive diagnostic commands. QoS is available from a central location. The host channel adapter gets addresses (LID, local identifier) through the subnet manager. All components are hot swappable. Management overhead and expenses are reduced dramatically. [www.rdmaconsortium.org]



Source: IBTA

3.8.6 Protocols for Redundant Paths

Data centers are increasingly required to support high availability and real-time applications. At the same time, they need to make sure they produce in a cost-effective manner. Conventional network models assume that overcapacities and multiple redundancies must be maintained to fulfill these requirements. This implies a certain wastefulness in broadband resources and infrastructures, since these systems are only rarely at full utilization. Also, as is generally known, redundancies are required only in cases of fault. In addition, real-time applications require short transmission paths along with low latencies. Shortest path bridging is on the scene as another new requirement and is changing how redundant systems are created. The result is that networks must now be completely re-planned.

This section describes the most important protocols for network redundancy along with their specific characteristics.

Spanning Tree

The spanning tree protocol (STP) defined by IEEE 802.1D prevents "looping" in Ethernet networks with star topologies and thus allows these networks to support redundant paths. STP is used in layer 2 switching. The STP process works as follows:

- When redundant network paths exist, one path is active and the others passive in order to prevent looping.
- Switches themselves are responsible for automatically negotiating and selecting these active and passive paths.
- If an active network path fails, all network paths are then re-calculated and the required connection established.

However, layer 2 switching that uses spanning tree bring two disadvantages:

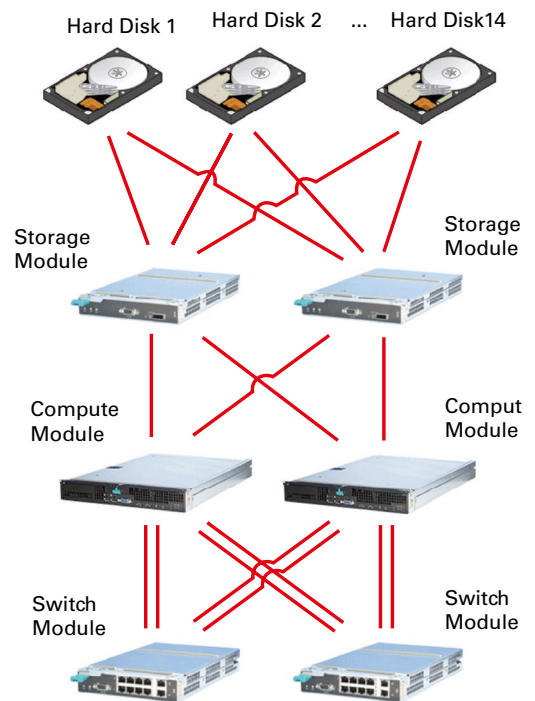
- Half of all available network paths remain unused (no load distribution).
- It can take a while to re-calculate network paths, and the network has only limited availability as this is being done.

The rapid spanning tree protocol (RSTP) provides a way of shortening the re-calculation process. Re-calculation now stops just a few connections instead of all communication. The previous configuration continues to operate until the re-calculation process is completed. As a result, failure of a path and re-calculation does not result in total network failure and downtimes are decreased drastically.

According to the IETF (Internet Engineering Task Force), the spanning tree protocol has by now reached its performance limits and is to be replaced by the TRILL protocol (TRansparent Interconnection of Lots of Links).

One alternative is layer 3 switching. This process uses routing protocols like RIP and OSPF. Failure of an active path no longer involves torn down network paths and extensive recalculations.

In practice, layer 3 switching is frequently implemented in the core layer, with layer 2 switching implemented in the aggregation/access layer. In layer 3 switching, a separate segment is implemented for each switch. This requires careful planning of IP address ranges.



Link Aggregation

In link aggregation, multiple LAN interfaces are bundled into a single logical channel (IEEE 802.3ad, 802.1ax as of 2008). This allows a higher data throughput to be achieved between two Ethernet switches, as well as higher reliability. Link aggregation can also connect servers and other systems over Ethernet, and is therefore of vital significance in data centers for many configurations.

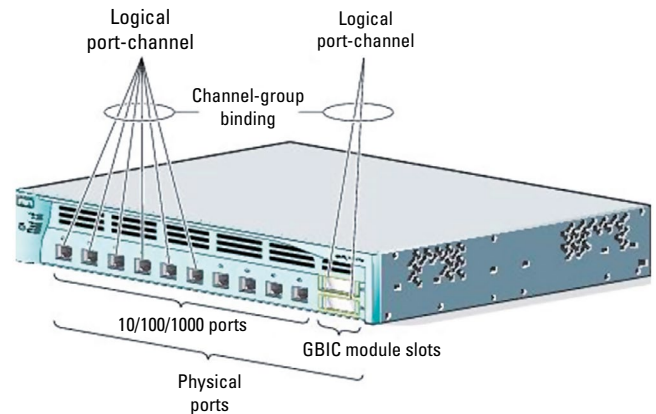
Since manufacturers use a number of different concepts and differing terminology, aggregation of Ethernet interfaces is not a process that provides 100% compatibility. Some of these different terms and specific concepts for aggregation include:

- Bonding in Linux environments
- Etherchannel in Cisco environments
- Load balancing in Hewlett-Packard environments
- Trunking in 3Com and Sun Microsystems environments
- Teaming in Novell Netware environments
- With bundling the term used in Germany

The following conditions must be provided before link aggregation can be implemented:

- Identical speed at all ports
- Full-duplex operation

Only those interfaces with high speed should be bundled. Four times Fast Ethernet 100 MBit/s (full-duplex) corresponds to "only" 800 MBit/s, while four times Gigabit Ethernet achieves 8 Gbit/s.



Shortest Path Bridging (SPB)

In the shortest path bridging method (IEEE 802.1aq), the link state protocol (LSP) is responsible for calculating the so-called shortest path tree (SPT) for each node in the network, where the SPT represents the shortest connecting structures of all bridges and switches in the area in which SPB is implemented. The SPBM process (SPB-MAC) distributes the MAC addresses for participating stations and information on interface service affiliations to those stations that are not participating in the process. This topology data is used to determine the cheapest connections from each individual node to all other participating nodes. This way each switch and router always has an overview of all paths available between nodes.

When a switch or link is added to the topology, the entire topology must be re-learned by all switches. Advantages provided by shortest path bridging include:

- Truly meshed networks can now be created in Ethernet.
- Network loads are distributed equally over the topology.
- Redundant connections are no longer automatically deactivated and can be used.
- The method allows a flatter network design with better performance between network nodes.

By contrast, the main disadvantage of shortest path bridging is its dynamic path negotiation. Transmission paths change frequently, which makes traffic management and troubleshooting more difficult.

Shortest path bridging provides a new way to design networks. However, it also brings significant consequences which must be taken into consideration and planned on at an early stage.

3.8.7 Data Center Bridging

The trend toward convergence, mentioned in numerous places in this handbook, is a key consideration for data center planners and operators. As the example with FCoE shows, Ethernet is being used increasingly to transfer data streams. Since Ethernet is not suitable for loss-free data transmission, the IEEE is continuing to develop the data center bridging standard (DCB, or "Data Center Ethernet" as it is known at Cisco, or "Converged Enhanced Ethernet" at IBM).

The use of DCB requires that servers be equipped with special converged network adapters (CNAs) that "understand" Ethernet and Fiber Channel. Special switches must also be implemented for DCB implementations. Advantages: A single DCB Ethernet network can replace both SAN and LAN infrastructures. CNAs also support iSCSI and RoCE (see section 3.8.5).

DCB actually includes four separate, independent standards that together provide ways to improvement network management, reliability and responsiveness:

- Priority-based flow control (PFC, 802.1Qbb)
- Enhanced transmission selection (ETS, 802.1Qaz)D
- CB exchange protocol (DCBX, 802.1Qaz)
- Congestion notification (CN, 802.1Qau)

PCF optimizes the current Ethernet stop mechanism. It only deactivates one channel, and not the entire transfer, in case a fault occurs. ETS defines priority classes within a PCF channel. Switches exchange configurations via DCBX. CN represents a form of traffic management, and restricts the flow of data traffic (rate limiting). It can arrange for the source to lower its transmission speed.

Data center bridging is already possible in 10 Gigabit Ethernet applications. It works over layer 2 and can handle a number of protocols with varying requirements. It is therefore also suitable for FCoE environments.

Finally, it is expected that DCB will contribute to standardized Ethernet devices and adapters for LAN and SAN applications. Ethernet technology should be optimized for this purpose so that it has the ability to ensure loss-free communication in convergent networks.

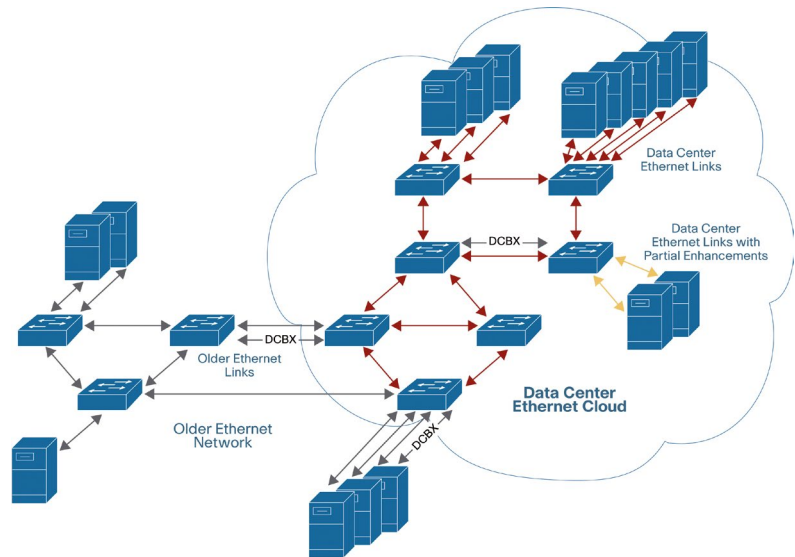


Image: Cisco, DCBX in use

3.9 Transmission Media

The selection of transmission media and connection solutions plays a central role in network planning. This process requires foresight, since the passive infrastructure is often not easily replaced and must provide useful service for many years.

Indeed, the passive infrastructure in the data center is essentially based on common principles of structure communication cabling (EN 50173, ISO/IEC 11801, EIA/TIA 568). However, this was not explicitly defined for a long time. Only with the introduction of the TIA 942 standard in 2005 was the foundation established for a comprehensive standardization of data center structures. The TIA 942 is a standard developed by the American National Standards Institute (ANSI). International and European standards followed.

The best approach in selecting transmission media and connection solutions, whether you are planning a new data center or redesigning an existing one, is to look into the future as far as possible, then to strive for acquiring the equipment that has the best specifications possible. In the process, proven standards for structured cabling can still serve as guides. This is because these standards support the usual criteria for success such as scalability, profitability, quality, operational reliability, etc.

The various kinds of different data center media are considered in more detail below

3.9.1 Glass Fiber Cables (Fiber Optic)

Growing demands on data centers are forcing operators to use fiber optic cabling. This is because the fiber optic medium offers the most resources over the long term and can also support virtually any required bandwidth. Glass fiber makes extremely short access times possible. Cabling systems are easily scaled and require little space. Optical transmission technologies are clearly a technology of the future. Ethernet requires glass fiber infrastructures, especially for migrations to 40/100 Gigabit Ethernet.



However, all this does not imply that companies should depend solely on glass fiber. Depending on the size, structure and operational concept of a data center, a practical mix of glass fiber and copper cabling should be selected. The norm makes it possible for companies to plan different areas or hierarchical layers that are based on different media and different length restrictions. In turn, planners and operators can then orient themselves to concepts of structured cabling.

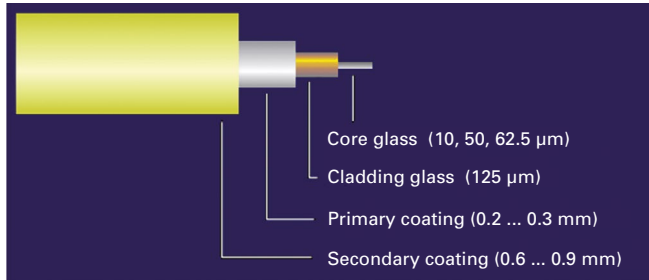
An overview is presented below of the fundamental topics, terminologies and issues that play a role in planning a glass fiber cabling system in a data center. We then present an orientation for decision makers, and information on some progressive glass fiber solutions that are currently available on the market.



3.9.2 Multi-mode, OM3 / OM4

Optical media can be grouped into glass (glass optical fiber/GOF) and plastics (plastic optical fiber/POF). POF is not suitable for data center applications. In turn, glass fibers can be grouped into two different types:

- Multi-mode glass fibers with gradient index profile
- Single-mode glass fibers



Structure of a glass fiber (core: 10 μm single mode, 50 & 62,5 μm multi mode)

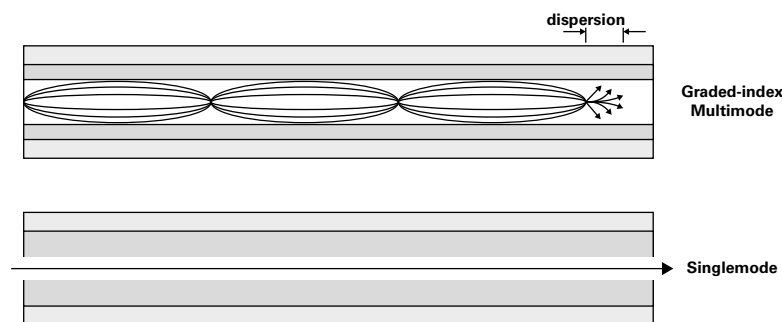
The modes in multi-mode glass fibers with a gradient index profile run in a wave shape around the fiber axis, which provides for an extensive compensation of signal delay differences. This glass fiber type has an attractive cost-benefit ratio, and has established itself as the standard fiber for high-speed connections over short to medium distances, e.g. in data centers.

Attenuation, measured in dB/km, and bandwidth length product (BLP), specified in MHz*km, represent the key performance indicators for glass fibers. A BLP of 1000 MHz*km means that the usable bandwidth is 1000 MHz over 1000 m, or 2000 MHz over 500 m.

In addition, multi-mode fibers can be divided into four categories. While OM1 and OM2 fibers work with LEDs as signal sources, OM3 and OM4 category fibers use lasers. OM3 and OM4 are laser-optimized 50/125 μm multi-mode glass fibers. The cost-effective VCSEL is usually used in data centers. Lasers have the advantage that, unlike LEDs, they are not limited to a maximum frequency of 622 MBit/s and can therefore transmit higher data rates.

OM4 fibers play a crucial role in data centers and thus deserve special attention. They offer additional leeway for insertion loss over the entire channel, which allows for more plug connections. Use of OM4 results in higher reliability of the overall network, a factor which is important for 40/100 Gigabit Ethernet applications. Finally, with its 150-meter range (as opposed to 100 meters with OM3) OM4 provides a reserve length, which is also covered by a higher attenuation reserve.

3.9.3 Single-mode, OS1 / OS2



Only one light path exists in single-mode glass fibers. The reason for this is their extremely thin core diameter of 9 μm. As a result, no multi-path propagation with signal delay differences between modes exists in these fibers. The advantage of this is that single-mode glass fibers can maintain extremely high transfer rates over long distances.

Single-mode glass fibers demand extremely precise light injection and consequently top-quality connection technology. This medium is used in high-performance areas like MAN and WAN backbones.

Dispersion-optimized monomode fiber technology, including non-dispersion shifted fibers (NDSF), dispersion-shifted fibers (DSF) and non-zero-dispersion shifted fibers (NZDSF) are available for applications based on WDM and DWDM technology (dense wavelength division multiplexing) technology. These fibers were standardized by the ITU in its G.650 ff. recommendations.

OS1 (as of 1995) and OS2 (as of 2006) classes, which differ by the maximum attenuation they establish, were defined for single-mode glass fibers. The following table shows the specifications of all standardized multi-mode and single-mode glass fiber types:

Fiber Types and Categories				
Modes	Multi-mode		Single-mode	
ISO/IEC 11801 class	OM3	OM4	OS1	OS2
IEC 60793-2 category	10-A1a	10-A1a	50-B1.1	50-B.1.3
ITU-T Type	G.651	G.651	G.652	G.652
Core/cladding (typical)	50/125 μm	50/125 μm	9(10)/125 μm	9/125 μm
Numerical aperture	0,2	0,2	—	—
Attenuation dB/km (typical)				
at 850 nm	3.5 dB/km	3.5 dB/km	—	—
at 1300 nm	1.5 dB/km	1.5 dB/km	1.0 dB/km	0.4 dB/km
Bandwidth length product (BLP) MHz*km				
at 850 nm	1,5 GHz*km	3,5 GHz*km	—	—
at 1300 nm	500 MHz*km	500 MHz*km	—	—
Effective modal bandwidth	2 GHz*km	4,7 GHz*km	—	—

3.9.4 Plug Connectors for Glass Fiber Cables

What is true for glass fibers also applies for fiber optic plug connectors – i.e. quality, performance and profitability are the decisive factors for what solutions are possible for a given data center. In contrast to copper connection technology, glass fiber plug connectors offer a wider assortment of formats and mating faces. This makes proper component selection a little more difficult. Basic knowledge in this area of quality grades for fiber optic connectors is indispensable for planners and installers. The following section provides information on current standards and discusses their relevance for product selection.



Connector Quality and Attenuation

The primary goal in the development, manufacture and application of fiber optic connectors is to eliminate causes of loss at fiber junctions. The small diameter of glass fiber cores requires a maximum degree of mechanical and optical precision in the manufacturing process. Tolerances of 0.5 to 0.10 μm (much smaller than a grain of dust) mean that manufacturers are approaching the limits of fine mechanics.

A plug connection is actually made up of a connector / adapter / connector combination. The fiber ends must meet each other precisely in the inside of the plug connection so that as little light energy as possible is lost or scattered back (return loss).



One can of course determine on site whether a plug connector has been snapped into place correctly. However, the quality of the connection can only be determined through the use of measuring equipment alone. Users must be able to rely on manufacturer specifications for specifications like attenuation, return loss, or mechanical strength.

A division into classes also exists for fiber optic channel links – though this classification must not be confused with the categories that describe fiber type and material. A channel link consists of permanently installed links (permanent links) as well as patching cables and device connection cables. As the following table illustrates, classes like OF-300, OF-500 and OF-2000 specify permissible attenuation in decibels (dB) and maximum fiber length in meters.

Channel Link Classes and Attenuation						
Class	Realized in category	Maximum attenuation of channel link in dB				Max. length
		Multi-mode		Single-mode		
		850 nm	1300 nm	1310 nm	1550 nm	
OF-300	OM1 to OM4, OS1, OS2	2.55	1.95	1.80	1.80	300 m
OF-500	OM1 to OM4, OS1, OS2	3.25	2.25	2.00	2.00	500 m
OF-2000	OM1 to OM4, OS1, OS2	8.50	4.50	3.50	3.50	2,000 m
OF-5000	OS1, OS2	—	—	4.00	4.00	5,000 m
OF-10000	OS1, OS2	—	—	4.00	4.00	10,000 m

The limit values for OF-300, OF-500 and OF-2000 are based on the assumption that 1.5 dB must be calculated in for connection technology (2 dB in the case of OF-5000 and OF-10000). For example: Using OF-500 with multi-mode glass fibers of 850 nm we get: 1.5 dB connection technology + 500 m x 3.5 dB/1,000 m = 3.25 dB.

This attenuation budget is calculated in order to ensure a reliable transmission. This is especially important for real-world data center applications like 10 Gigabit Ethernet and IEEE802.3 Section Six 40/100 Gigabit Ethernet protocol variants. In these cases, an extremely low attenuation budget must be included. The maximum link ranges then result.

The quality of a fiber optic connector is usually characterized by two values:

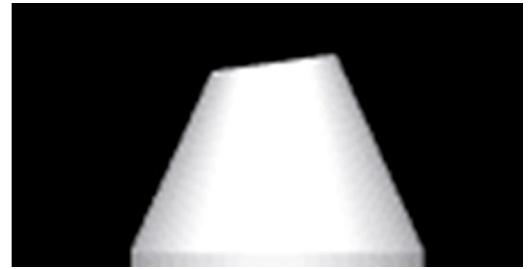
- Insertion loss (**IL**)
Ratio of light output in fiber cores before and after the connection
- Return loss (**RL**)
Amount of light at the connection point that is reflected back to the light source

The smaller the IL value and the larger the RL value, the better the signal transmission in a plug connection will be. ISO/IEC 11801 & EN 50173-1 standards specify the following values for both single-mode as well as multi-mode:

Insertion loss (IL)	Return loss (RL)
≤ 0.75 dB for 100% of plug connections	≥ 20 dB for multi-mode glass fibers
≤ 0.50 dB for 95% of plug connections	≥ 35 dB for single-mode glass fibers
< 0.35 dB for 50% of plug connections	

Standards require that fiber ends come with a PC (physical contact) or APC (angled physical contact) cut surface. The expression HRL (high return loss) is sometimes used for APC. In a PC cut surface, the front of the fiber end gets a convex ground end surface so fiber cores can make contact at their highest elevation points. As a result, the creation of reflections on the connection point is reduced. An additional improvement in return loss is achieved by means of APC bevel grinding technology. Here, the convex end surfaces of the ferrule are ground with a bevel of 8° to the axis of the fiber.

Different amounts of light or modes – depending on the physical properties of the fibers – are diffused and scattered back at the transition point of the two fibers. A PC connector that is well-ground and cleaned has about 14.7 dB RL against air and 45 to 50 dB in when plugged in. With APC connectors, modes are also scattered back as a result of the 8° or 9° grind, though at an angle that is greater than the angle of acceptance for total reflection. Modes which have an angle of greater than 7.5° are decoupled after a few centimeters and therefore do not reach the source and interfere with it. A quality APC connector has at least 55 dB RL against air and 60 to 90 dB when plugged.

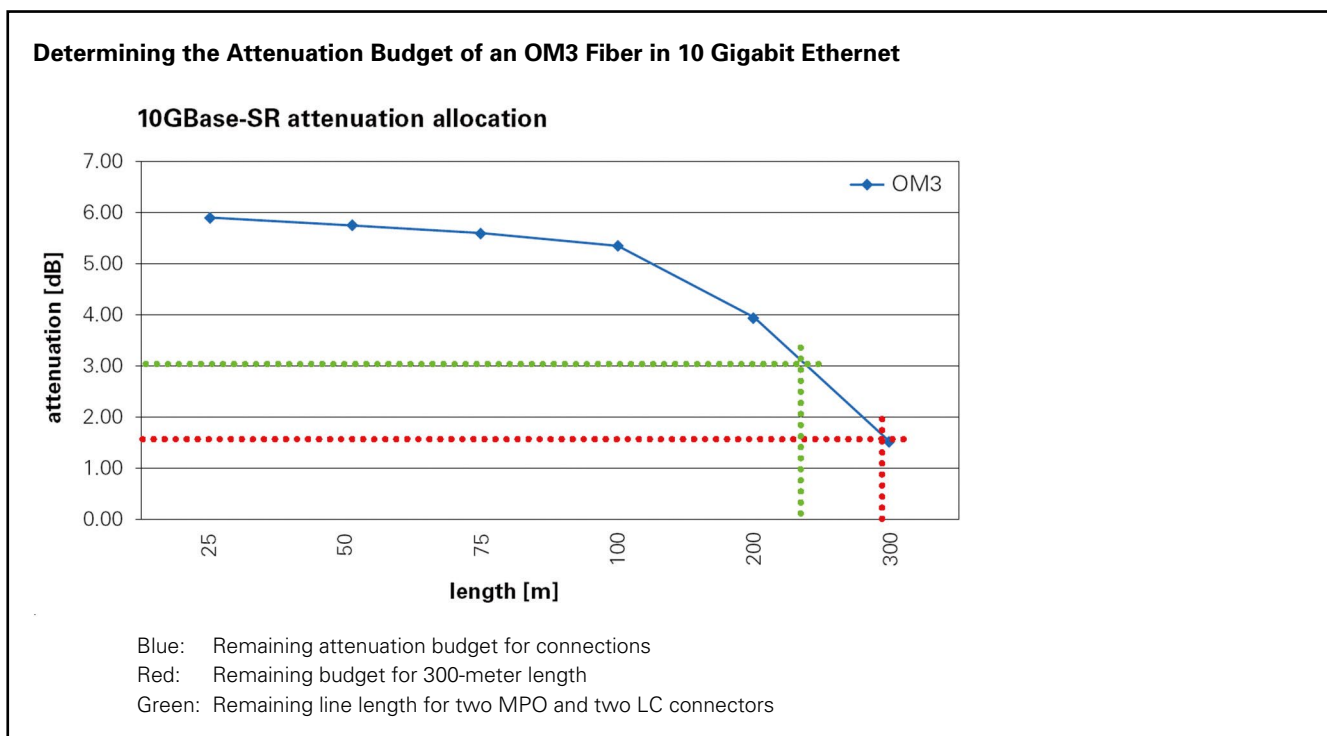
*PC Physical Contact**APC Angled Physical Contact*

Quality Grades

In order to achieve user-friendly compatibility of fiber optic connectors, manufacturer-neutral attenuation values and geometric parameters for single-mode connectors were defined in 2007 by the standards IEC 61753 and IEC 61755- 3-1/-2. The attenuation values established for random connector pairings, also known as each-to-each or random-mated pairings, come significantly closer to actual operating conditions than the attenuation values specified by manufacturers. Quality grades are geared to typical values, so-called mean values, instead of maximum values. This provides an optimal basis for the calculation of path attenuation.

A grade M was also considered for multi-mode connectors in the drafts of the standards, but it was rejected again in the standard that was adopted. Manufacturers and planners have been getting by with using information from older or accompanying standards to find guideline values for multi-mode connectors.

With the introduction of 10/40/100 Gigabit Ethernet, however, these standards for multi-mode connector quality were no longer sufficient. An example should underscore this point:



10 Gigabit Ethernet as defined by IEEE 802.3 Section Four should be able to transmit over the maximum distance of 300 meters using OM3 fibers. In accordance with the standard, 1.5 dB for connection losses still remains after deducting fiber attenuation and power penalties (graphic, red line). A maximum of two plug connections is therefore possible using current grade M multi-mode connectors and an insertion loss of 0.75 dB per plug. However, this is not very realistic.

To reverse the argument, two MPO and two LC plug connections, for example, should now be used. Total attenuation comes to 3 dB given an insertion loss of 0.75 dB for each connection. As a result, the link should still be about 225 meters (graphic, green line).

The same example, using a data rate of 40 Gbit/s, decreases the link to 25 meters. This shows that the attenuation budget available for plug connectors becomes smaller and smaller as the data rate increases.

Plug Connector Types

LC and MPO plug connectors were defined for data center applications in accordance with ISO/IEC 24764, EN 50173-5 and TIA-942 standards for fiber optic cabling systems.

MPO Plug Connector (IEC 61754-7)

MPO (multipath push-on) is based on a plastic ferrule that provides the ability to house up to 24 fibers in a single connector. Connectors with up to 72 fibers are already in development by this time. This connector stands out because of its compact design and easy operation, but brings disadvantages in optical performance and reliability.

This connector type is of crucial importance because of its increased packing density and ability to migrate to 40/100 Gigabit Ethernet.



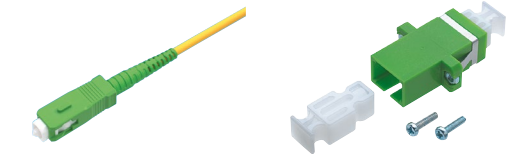
LC Plug Connector (IEC 61754-20)

This connector is part of a new generation of compact connectors. It was developed by Lucent (LC stands for Lucent Connector). Its design is based on a 1.25 mm-diameter ferrule. Its duplex adapter matches the size of an SC adapter. As a result, it can achieve extremely high packing densities, which makes the connector attractive for use in data centers.



SC Plug Connector (IEC 61751-4)

SC stands for square connector or subscriber connector. It makes high packing densities possible because of its compact design, and can be combined into duplex and multiple connections. Despite its age, the SC continues to gain in importance because of its outstanding properties. It has been the most important WAN connector worldwide up to today, usually as a duplex version, because of its good optical properties.



E-2000™ Plug Connector (LSH, IEC 61753-15)

This connector is a development by the company Diamond SA which specializes in LAN and CATV applications. It is produced by three licensed manufacturers in Switzerland, which has also led to its unequalled quality standard. The integrated protective flap provides protection from dust and scratches as well as laser beams. The connector can be locked using grids and levers which can be coded by color and also mechanically.



Footnote: E-2000™ – manufactured under license from Diamond SA, CH-6612, Losone.

3.9.5 Coax and Twinax Cables

Asymmetrical cable media such as coaxial cables are rarely used in typical data center network infrastructures. They may still be found in cabling for video surveillance and analog KVM switches.

Nevertheless, Twinax cables are being found more and more in server uplinks, for both Ethernet as well as Fiber Channel. These media are suitable for distances up to 15 m.

IEEE 802.3 Section Four defines connections in accordance with 10GBASE-CX4. The standard allows transmissions at a maximum rate of 10 Gbit/s by means of Twinax cabling, over a maximum length of 15 meters. 10GBase-CX4 uses a XAUI 4-lane interface, a copper cabling system which is also used for CX4-compatible InfiniBand (see section 3.8.5). A maximum connection of 10 meters is supported in 40 and 100 Gigabit Ethernet (40GBASE-CR4 and 100GBASE-CR10) using Twinax cables in 4- or 10-pair configuration respectively (double twinaxial IB4X or IB10X cables respectively).

3.9.6 Twisted Copper Cables (Twisted Pair)

The classic widespread variant of copper cabling is twisted pair. This is usually the most cost-effective and universally usable transmission medium from an economic standpoint. Data centers, even in the future, can cover even large network areas with twisted pair copper cabling when they select high-quality solutions for this purpose. High-quality in this case means that data centers, wherever possible, rely on shielded cables and plug-in systems that offer all-around protection against electromagnetic influences. Sensitive high-frequency transmissions over 10 Gigabit Ethernet especially demand such protection.



The most essential copper cabling components include:

- Category 6 (specified up to a bandwidth of 250 MHz)
- Category 6A / 6_A (specified up to a bandwidth of 500 MHz)
- Category 7 (specified up to a bandwidth of 600 MHz)
- Category 7_A (specified up to a bandwidth of 1,000 MHz)

Listed are a few important pointers regarding the latest standards relevant to network planning:

- The IEEE, in its IEEE 802.3 Section Four standard published in 2006, not only established a transmission protocol for 10 Gigabit Ethernet (10GBase-T), but also defined the minimum standards for channels to be able to transmit 10 Gigabit up to 100 meters over twisted copper lines.
- EIA/TIA followed that standard with 568B.2-10 in 2008, which imposed higher minimum standards for channels, and also specified requirements for components, and thus category 6_A was born.
- In the same year, ISO/IEC 11801 appeared, whose Amendment 1 formulated even tighter requirements for channels, and so channel class E_A was defined. The definition of components remained open.
- This gap was closed in 2010 with publication of ISO/IEC 11801, Amendment 2. The new standard defines components, i.e. category 6_A cables and plug connections (note the subscript _A), and thus sets standards which surpass those of EIA/TIA.

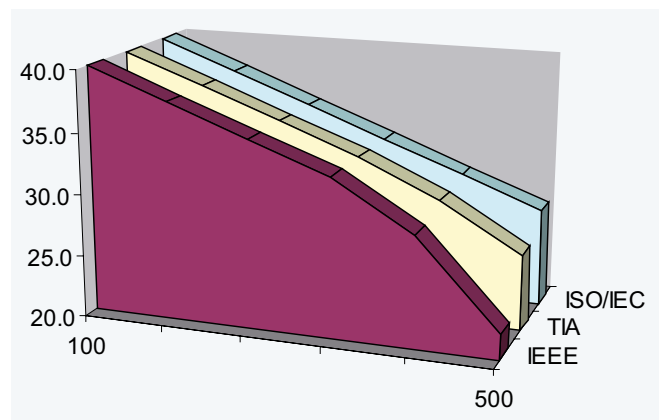
Frequency	IEEE	EIA/TIA		ISO/IEC	
	Channel etc.	Channel	Components	Channel	Components
1-250 MHz	1GBASE-T	Cat. 6	Cat. 6	Class E	Cat. 6
1-500 MHz	10GBASE-T IEEE 802.3 Section Four	Cat. 6A EIA/TIA 568B.2-10 (2008)	Cat. 6A EIA/TIA 568B.2-10 (2008)	Class E _A ISO/IEC 11801 Amendment 1 (2008)	Cat. 6 _A ISO/IEC 11801 Amendment 2 (2010)
1-600 MHz				Class F	Cat. 7
1-1'000 MHz				Class F _A	Cat. 7 _A

Current cabling standards for typical data center requirements

EIA/TIA Cat. 6_A channel standards show a moderate 27 dB drop in the attenuation curve starting at 330 MHz, while ISO/IEC Class E_A defines a straight line for the channel.

A design based on ISO/IEC therefore provides for the highest availability and best possible transmission in twisted pair copper cabling based on RJ45 technology. In the case of 500 MHz, this means the NEXT performance required for class EA must be 1.8 dB better than for a channel with Cat. 6_A. In practice, this higher requirement leads to better network reliability, and in turn to fewer transmission errors.

This also lays the foundation for a longer useful, overall life of the cabling infrastructure.



IEEE 802.3 Section Four vs. TIA vs. ISO/IEC / NEXT limit values for the channel

Cable Selection

The general principle that maximum bandwidth normally allows a maximum data rate applies in the selection of cable. It therefore follows that companies that eventually expect to implement 10, or even 40 Gigabit, Ethernet should go with the highest quality cabling type, i.e. category 7_A. One disadvantage of this cabling type, however, is its large outer diameter. This affects its characteristics with regard to installation, and requires larger cable routing systems which can lead to higher costs.

Shielding is also a factor in cable selection, since it is also a significant cost factor. As mentioned above, new protocols like 10 Gigabit Ethernet are susceptible to electromagnetic influences. The better the shielding, the more reliable the signal transmission.

Nevertheless, unshielded cabling can be used for 10GBase-T if appropriate ambient conditions and other basic conditions are fulfilled. These additional requirements are necessary since UTP cabling systems require additional protective measures to support 10GBase-T, such as:

- Careful separation of data cables and power supply cables or other potential sources of interference (minimum distance of 30 cm between data and power cables)
- Use of a metallic cable routing system for data cables
- Prevention of the use of wireless communication devices in the vicinity of the cabling system
- Prevention of electrostatic discharges

The EMC (electromagnetic compatibility) behavior of shielded and unshielded cabling systems for 10GBase-T is described in detail in section 3.10.6.

Since old cabling designations related to shielding were not standard, were inconsistent, and often provided for confusion, a new naming system of the form XX/YZZ was introduced in ISO/IEC 11801 (2002).

- **XX stands for the overall shielding provided**
 - o U = no shield (unshielded)
 - o F = foil shield
 - o S = braided shield
 - o SF = braid and foil shield

- **Y stands for the shielding provided for the core pair**
 - o U = no shield (unshielded)
 - o F = foil shield
 - o S = braided shield

- **ZZ always stands for TP = twisted pair**

Twisted pair cables in the following shield variants are available on the market:

Shielding		U/UTP	F/UTP	U/FTP	S/FTP	F/FTP	SF/FTP
Overall shield	Foil		(✓)			✓	✓
	Wire mesh		(✓)		✓		✓
Core pair shielding	Foil			✓	✓	✓	✓

Lightweight low-profile cables (AWG26 cables) with a diameter of 0.405 mm (as compared to 0.644 mm in AWG22) and other advances in shielding and cabling technology are leading to savings in cabling solutions. At the same time, these solutions can increase performance and efficiency in passive infrastructures. A maximum savings of 30% in cabling volume and weight is possible using these cables. However, some details may come into play with regard to planning, product selection and installation. These involve achieving sufficient attenuation reserves in the channel and permanent link, and in turn full operational reliability of the cabling system.

AWG stands for American Wire Gauge and is coding systems for wire diameter. The following core diameters are used for communication cabling:

- AWG22 / Ø 0,644 mm
- AWG23 / Ø 0,573 mm
- AWG24 / Ø 0,511 mm
- AWG26 / Ø 0,405 mm

The network planning process must also consider any requirements where devices need to be supplied with power through data cabling. The IEEE 802.3 Section Two standard (Power over Ethernet/ PoE, Power over Ethernet Plus/PoEplus) standards define ways in which data cables can be used to supply devices with the electrical power they need. Common applications of this technique include wireless access points, VoIP phones and IP cameras.

Pre-Assembled Systems / Plug-and-Play Solutions

Installing systems and components in data centers requires precision work and complex measurements that must be carried by an enormous number of highly qualified personnel. In addition, producing the countless connections required in networks by hand is a lengthy operation. Quick, spontaneous changes to the positions of connections – a typical requirement in data centers – are only possible under certain conditions, and are relatively expensive.

Manufacturers like R&M therefore offer the following pre-assembled solutions:

- Multi-core cables consisting of multiple twisted-pair cables or multi-fibrous cables, both ends sealed with normal plug connectors or outlets or even a special unique manufacturer-specific plug. The manufacturer provides a measurement report with all connections.
- Modular terminal blocks which can be mounted in the cabinet using 19" technology or in double floor systems. Multi-core cables can be connected to this block at the input side using the special plug, and then RJ45 outlets or glass fiber adapters are available on the output side.

Cabling systems pre-assembled at the factory allow data center availability to be increased. This is because, given a best-case scenario, installation is reduced down to a simple plug and play, saving time and money. In addition, plug-and-play solutions allows systems enhancements to be implemented in no time at all. Plug-and-play solutions mean that no waste accumulates in the security area during installation, and third-party personnel or a company's own technicians only have to enter the security area for a short time, maybe even not at all.

The supplier provides units that have been inspected and are one-hundred percent flawless and immediately ready for operation. These units have uniform quality and transmission properties throughout. Furthermore, these solutions provide high investment protection, since in general they can be kept up-to-date, upgraded and reused.

The trend towards compression of glass fiber cabling has led to parallel optic connection technology and in turn to innovative multi-fiber connectors that are as compact as an RJ45 plug connection. This is because four or even ten times the number of plug connections must now be provided to ports in order to implement 40/100 Gigabit Ethernet (see section 3.10.1). Multipath push-on (MPO) technology has shown itself to be a practical solution and features specifications as defined under IEEE 802.3 Section Six. On the downside however, MPO plugs with 12, 24 or even 72 fibers cannot be assembled on site. The use of MPO plug connectors therefore always involves the use of trunk cables. These components can come pre-assembled and delivered in the desired length.

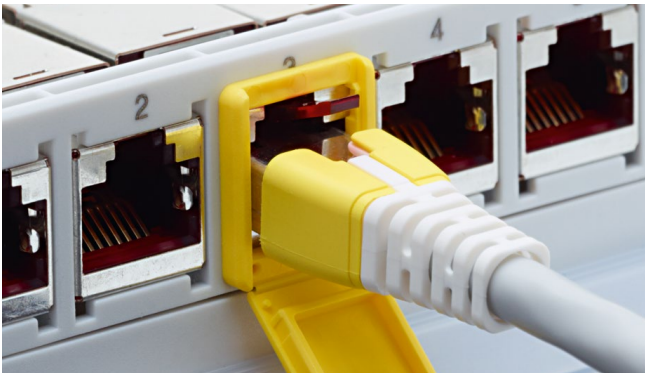


Pre-assembled shielded cable with category 6A modules



Trunk cable with R&M MPO/MTP® plug connector

3.9.7 Plug Connectors for Twisted Copper Cables



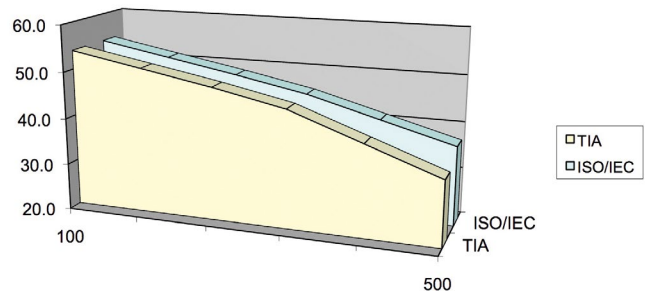
The RJ45 plug connection system is the universal connection solution in twisted-pair copper cabling. The eight-pin miniature plug-in system for shielded and unshielded cabling is used in virtually every IT environment. Its transmission properties are determined through its small dimensions. Parameters like frequency range, attenuation and crosstalk also play an important role in determining the plug's transmission behavior, and must be taken into consideration in planning and evaluation processes. Crosstalk is especially critical, since core pairs that are guided into the cable separately must still run together in the body of the connector. The low contact distances of the RJ45 plug as well as certain other factors have proven to be problematic for high-frequency behavior

Only plug-in modules that were optimized with respect to contact

geometry satisfy standards up to categories 6A and 6A. As in Channel technology (see above), higher performance can also be achieved using a 6A connector designed in accordance with ISO specifications than with a Cat. 6A plug connection designed in accordance with EIA/TIA specifications.

A 40 dB attenuation drop should be allowed for in Cat. 6A starting from 250 MHz, and a 30 dB drop for Cat. 6A. In the case of 500 MHz, this means that a Cat. 6A module must achieve NEXT performance that is 3 dB better than a Cat. 6A module (see graphic to the right).

ISO/IEC Cat 6A vs. TIA Cat 6A Connecting Hardware NEXT Values

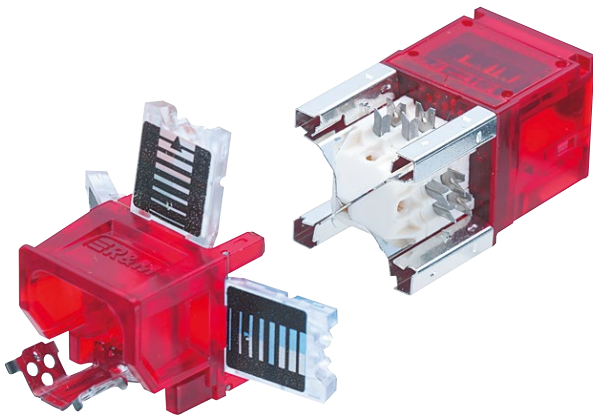


Because the required attenuation reserve cannot be achieved through a change in the existing design alone, this performance increase will require a radical change in how new modules are developed. Above all, more compensating elements are required to balance out the additional coupling effects like cross-modal couplings. Greater effort is required to separate core pairs at the end point from one another. The connecting or contacting process must be performed in a very precise manner and guaranteed to be without error, to ensure consistent signal transmission.

R&M has succeeded in doing just that with its Cat. 6_A ISO module. It features enormous safety reserves that even go beyond those defined by the strict international standards (an example of the product appears below).

RJ45 connectors can only achieve Cat. 7/7_A transmission property requirements by specifically assigning the outer pin pairs. This restricts flexibility considerably. It is for this reason that the RJ45 connector was not used for connecting Cat. 7 and 7_A cables. Instead, the GG45 connector, ARJ45 connector and TERA connector were developed and standardized to support these categories. These connection systems have a different contact geometry from RJ45 which separates the critical center core pairs from one another.

Category 6_A from R&M



Cat. 6_A module with X Separator from R&M

R&M's category 6_A solution, with its distinctive, innovative red connection module, has proven itself to be one of the most outstanding copper connection technologies ever offered in RJ45 format, and features the highest performance ever shown. Its wiring technology that features an automatic cutting process guarantees its cores are always wired precisely, no matter how they are handled by electricians. This was proven by means of a pilot project carried out in 2011 that used over 2,000 class EA permanent links of different lengths. All electricians testing our module achieved exceptionally good NEXT values (4 to 11 dB reserve).

The inside of the module is provided with metal pyramids that divide wire cores to all four sides, and also with an X separator component that provides insulation. This design provides maximum protection against crosstalk. The Cat. 6_A ISO module from R&M has a radical design that makes it easy to use but at the same time offers unbeatable performance.

The module is also subject to a strict quality control process – R&M production-tests every single module over relevant parameters.

Conclusion

So what should a data center planner or operator finally decide on when it comes to cabling components for copper? For financial and technical reasons, current thinking definitely sees a shielded category 7_A cable combined with a shielded category 6_A plug connection system as the best choice.

Security Solutions for Cabling Systems

A quality cabling system can have a positive effect on data center security, and appropriate planning will allow it to be designed in such a way that it can be adapted to increasing requirements at any time. Clearness, clarity, simplicity and usability play a major role in this process. And in the end, the cost-benefit ratio should also be taken into consideration in product selection. Often a simple, yet consistent, mechanical solution is more effective than an expensive active component or complex software solution.



Security solutions from R&M, ranging from insertable color coded units (left) to locks for patch cords (right)

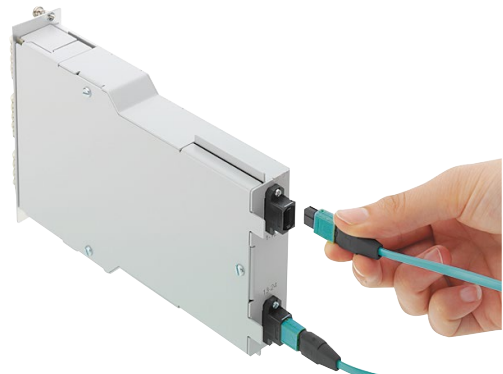
R&M's three-stage security system for network connections is one good example of a solution that not only answers all of these security requirements, but also extends R&M's basic principle of modularity into the area of security. One element central to this system is its color coding scheme. The unit is fitted with sleeves so it can be easily plugged onto the ends of patch cords. These sleeves can be replaced by hand. The cable itself does not need to be unplugged or removed, so IT operation remains unaffected. Color coding units can also be added onto patch panels and connection sockets, allowing for a clear assignment of connections. Finally, this system reduces costs, since the need to stock up on color patch cords is eliminated.

Mechanical coding solutions and locking solutions are also available as the second and third stages of the R&M security system. These solutions ensure that cables are not connected to the wrong ports, and that a cable – whether copper or fiber optic – always stays in its place. The connection can only be opened with a special key. R&M's visual and mechanical coding systems and locking solution together provide an enormous increase in the passive security of your data center.

3.10 Implementations and Analyses

Generation 40/100 Gigabit Ethernet will keep data centers extremely busy in the coming years. The question arises, how can the infrastructures and components that have already been presented in this handbook be implemented in data centers elegantly and with justifiable expense? This section will show a few promising methods, by presenting the reader with some basic information as an introduction to parallel optic connection technology.

In addition, the reader will become familiar with related criteria of performance and quality. Decision makers will receive an initial orientation for planning their optical fiber strategy and selecting connection technology. The logical migration path to 40/100 GbE is described, as well as the essential polarity methods in this area.



In contrast to many earlier upgrades that were managed by means of complex technological breakthrough, the path to 40/100 Gigabit Ethernet appears to be relatively simple. In general, you just multiply existing photonic technology, e.g. in extremely precise, parallel optic plug connectors known as multipath push-on (MPO). Sections 3.10.1 and 3.10.2 will reveal whether the process is really as easy as it seems. The need exists in many large data centers which already support tens of thousands of fiber optic links, for these faster solutions with an extremely high density, which can be easily managed and scalable to a high bandwidth requirement.

The migration can succeed only if you have the ability to correctly assign the great number of fibers and polarities of cables and plug connectors during installation and continuous operation. This is because the sending port and receiving port must be directly connected with one another. Given the growing number of fibers, this process can be somewhat confused, but the challenge can be overcome.

Whoever examines predictions regarding IT and the Internet will unavoidably begin to seek the best possible path to 40/100 Gigabit Ethernet. The market trend is moving in this direction. Data centers will not be able to close their eyes to this fact.

Power over Ethernet



The consolidation of power and data transmission – Power over Ethernet – can lead to some surprising effects in terms of rationalization and savings. This technology requires application-based implementation, a topic to which a whole separate section is devoted. Data center planners and operators should seriously consider PoE. To be exact, the technology makes separate power feed for IP cameras, wireless access points, IP telephones and other network devices unnecessary.

More electrical energy on the data cable automatically means more heat to wire cores. One risk factor related to the technology is that anyone planning data networks that can support PoEplus must be especially careful when selecting a cabling system and take into account some limitations under certain circumstances. However, the heating problem can be managed through consistent compliance with existing and future standards. As a result, no problems will come up during data transmission. R&M offers a number of solutions to this problem.

However, one other risk factor must not be disregarded: the danger of contacts burning off when live connectors are plugged in. R&M tests show that high-quality, stable solutions will ensure continuous contact quality. The explanations presented in section 3.10.3 are intended to provide support when planning data networks that use PoE and point to as-yet-unresolved questions in the current standardization process.

Short Links in LAN

Another critical issue for data centers is that ISO 11801 2010 Amendment 2 no longer guarantees that the permanent link requirement will be satisfied if the link falls short of a length of 15 m. Does this mean if you want to use class EA, you are going to have to stow away a bunch of cables longer than 15 m? Shorter link lengths are common in various applications, especially in data centers.

Section 3.10.4 therefore provides information of the latest development in the area of standardized copper cabling solutions for short links. It also describes entirely new options intended to provide orientation for planning high-performance data networks and decision aids for product selection.

More Performance and Shielding in LAN



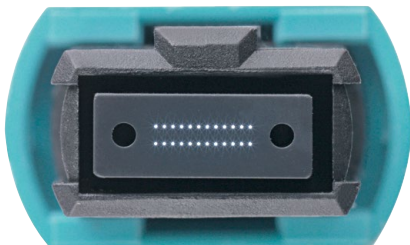
Two case examinations are presented below. First, the capabilities of class EA and FA cabling systems or Cat. 6_A and 7_A components are examined closely and compared with one another. In the process, a comparison of the transmission capacities of the different classes is carried out and critical cabling parameters listed. In addition, the EMC behavior of shielded and unshielded cabling systems for 10GBase-T is examined using an independent study.

3.10.1 Connection Technology for 40/100 Gigabit Ethernet (MPO / MTP®)

Footnote: MTP® is a registered trademark of US Conec Ltd.

Parallel optical connection technology with category OM3 and OM4 multi-fiber multi-mode glass fibers are paving the way to 40 and 100 Gigabit Ethernet (GbE) in terms of cabling. At the time this handbook was created, this technology was accepted as state of the art and appears to be the most cost-effective path for data centers. As described above, you multiply connections or consolidate 10 Gigabit Ethernet ports to be able to represent 40/100 GbE in the network. Here, the biggest challenge is that four or even ten times the number of plug connections that existed before must now be provided to ports.

This can no longer be managed using conventional single plug connectors. As a result, the IEEE 802.3 Section Six standard including specifications for the multi-fiber MPO plug connector, for both 40GBASE-SR4 and 100GBASE-SR10. This component has the ability to contact 12 or 24 fibers in just a tiny amount of space. This connector type and its differences with the clearly improved MTP® plug connector are described in greater detail below.



MPO plug connector with 24 glass fibers

The MPO plug connector (multi-fiber push-on or multi-path push-on) is a multi-fiber plug connector defined under IEC 61754-7 and TIA/EIA 604-5. Like an RJ45 connector, it has the ability to take in up to 72 fibers in a tiny amount of space. MPO connectors with 12 or 24 fibers are generally used in applications.

The connector is provided with a push-pull locking device with a sliding sleeve and two alignment pins allowing the component to be precisely positioned. It is designed for more than 1,000 mating cycles. Contacting can be implemented as PC (physical contact) or APC (angled physical contact) (see section 3.9.4).

Eight fibers are required for 40 GbE and twenty for 100 GbE. This leaves four contacts unwired, as the following connection diagram shows:



12-fiber (left) and 24-fiber (right) MPO connectors. Color highlighting shows fibers for sending (red) and receiving (green).

As in any plug connector, the quality of a connection that uses MPO connectors depends on precision contacting – in this case, however, the same whether the 12-fiber or 24-fiber version is used. Fibers are stuck into a bore hole in the connector body. This hole must be larger than the fiber itself so that the fiber can be inserted. As a result, the fiber always has a certain amount of play in the bore hole.

This tolerance results in two decided disadvantages for attenuation:

- **Angular error (squint angle):**

The fiber does not lie exactly parallel to the bore hole, but at a so-called squint angle. As a result, the fibers meet each other in the plug connection at an angle, and also show a radial displacement. This means a higher mechanical load when contact is made.

- **Radial displacement (concentricity):**

The two fibers in a plug connection do not meet each other in a congruent manner but are slightly displaced from one another. In order to improve concentricity, the center of the cylinder is taken and rotated once around a reference center. The diameter that is thus determined is defined as the value of concentricity. EN 50377-15-1 allows the concentricity of fiber holes in the MPO ferrule to be a maximum of 5 µm.

The concept of radial displacement is also often used in connection with radial displacement. This is a vector that specifies the distance from the actual radial center of the cylinder to the reference center and direction of deviation. Since the actual cylinder center used to determine concentricity is rotated once around the reference center, this value is therefore twice as big as that of eccentricity, but provides no information with regard to the direction of deviation.

Both cases result in a higher insertion loss (IL) and lower return loss (RL) since a fraction of the light is not transmitted but reflected instead. IEEE 802.3 Section Six requires that MPO plug connectors show a maximum insertion loss of 0.75 dB and return loss of less than -20 dB.

In view of their multi-fibrous filigree design and low permissible tolerances MPO plug connectors (as well as the MTP® connectors described below) cannot be assembled manually on site. MPO/MTP® plug connector therefore come already assembled in conjunction with trunk cables. Though this does require that cable lengths be precisely planned in advance, it also guarantees maximum quality and short installation times.

MTP® Plug Connectors with Elite Ferrules from R&M

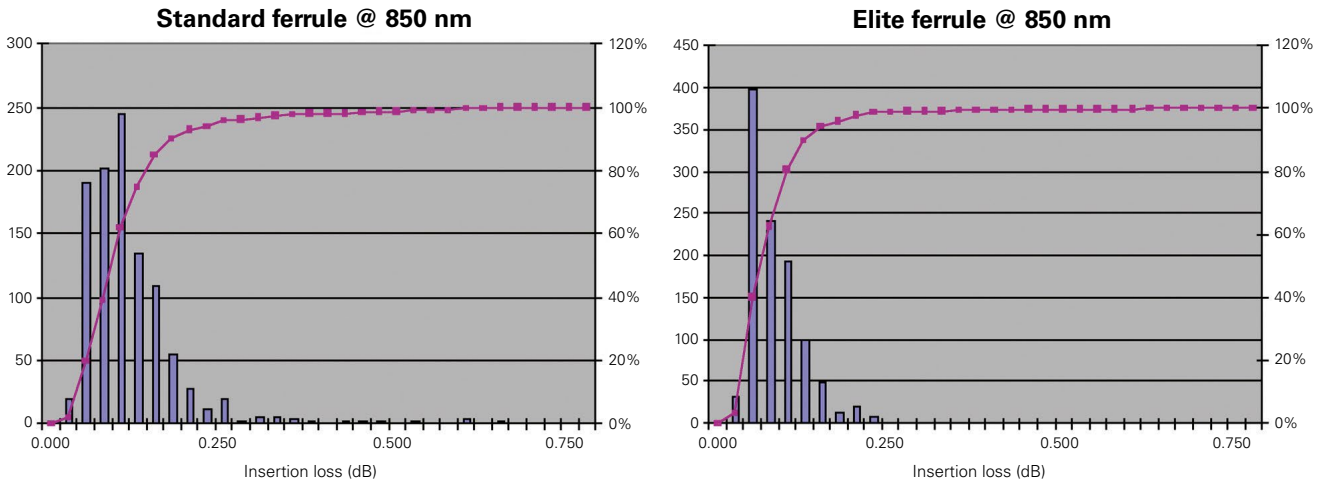
MPO connector fibers are inserted directly into the plastic body of the connector, thus making it difficult to adjust these fibers afterwards, and setting limits on manufacturing precision. Angular errors as well as radial displacement may only be minimized to a certain degree.

In order to achieve lower tolerances and better attenuation values, the American connection technology specialist US Conec developed MTP® plug connectors (mechanical transfer push-on). These components show a number of improvements over MPO with regard to optical and mechanical quality. An MTP® plug connector consists of a housing and a separate MT ferrule (mechanical transfer). Components in MTP® connectors, including pins and the oval pressure spring, are permanently anchored to the connector using a metal clip. This construction gives the connector a high degree of mechanical stability and also prevents the spring from making contact with the cable and damaging it, as the connector is inserted, for example.

The MT ferrule is a multi-fiber ferrule in which fiber alignment is based on the eccentricity and positioning of the fibers as well as the bore holes in the centering pins. As a result, fiber alignment can be controlled by the centering pins as the connector is inserted.

Since the housing can be removed, the ferrule can interferometrically measured right in the production process. This also makes it possible for the ferrule to be adjusted at a later time. In addition, the gender of the plug (male/female) can be altered on site in just a small amount of time. Other developments from UC Conec include the elliptical centering pins that provide for precision alignment of the fiber ends within the MTP® plug connection, as well as the movable ferrules positioned lengthwise in the housing, which makes a defined contact pressure possible.

The multi-mode MT Elite ferrule represents another improvement in this area. This component features a 50% reduction in insertion loss as compared to a standard MT ferrule at a typical 0.1 dB, with identical return loss. These improved values are based on tighter production tolerances. Test series from the R&M laboratory have confirmed the advantages of the Elite ferrule. "Random-mated" measurements with R&M MPO/MTP® patch cords were carried out in accordance with IEC 61300-3-45. The following charts show the results of these tests. The attached table lists the significant 50% and 95% values from the test series.



Insertion loss characteristic of standard (left) and Elite ferrules (right) from R&M test series

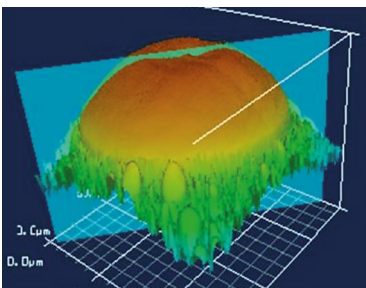
Ferrule Type	50%	95%
Standard	≤ 0.09 dB	≤ 0.25 dB
Elite	≤ 0.06 dB	≤ 0.18 dB

50% and 95% values of standard and Elite ferrules

Though R&M uses only MTP® plug connectors with Elite ferrules for its MPO solutions, it has improved its already good measurement values in an internally developed finishing process. As a result, not only the ferrule tolerances specified by the IEC for MPO plug connectors increased, but new parameters were defined as well. The finishing process is carried out in a special high-end production line.

R&M always sets more stringent criteria than the relevant standards for each production step and parameter and for statistical quality management processes, in order to guarantee users the highest possible operational reliability.

Core Dip



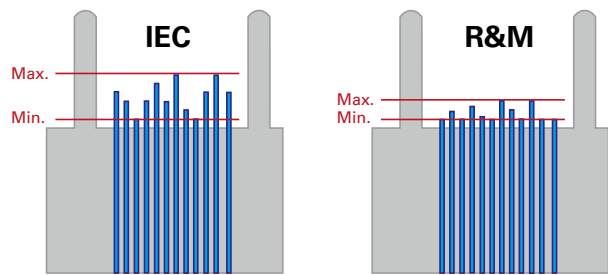
R&M devotes especially great care to the front end of fibers and the "core dip" that exists there (see illustration). After all, this is the point at which fibers come into contact with one another in the plug connection and effectively determine insertion loss as well as return loss.

As its name suggests, the core dip describes a "dip" in the center of the fiber. It is produced through a polishing process, since the core, due to its properties, is somewhat softer than the fiber cladding. The dip may deviate by a maximum of 100 nm, as specified by EN 50377-15-1.

Fiber Protrusion

The second important quality criterion is fiber protrusion, which specifies how far the fiber end should project over the ferrule. A protrusion that is too large can lead to the fiber being damaged when the connector is plugged in.

A variation in fiber heights results when fiber ends are polished. This variation may only be decreased if appropriate care is exercised in the polishing process, and only if high-quality polishing instruments and appropriate polishing agents are used. R&M was able to optimize this work step so well that the tight tolerances of 1 to 3.5 µm established under EN 50377-15-1 could be reduced even further.



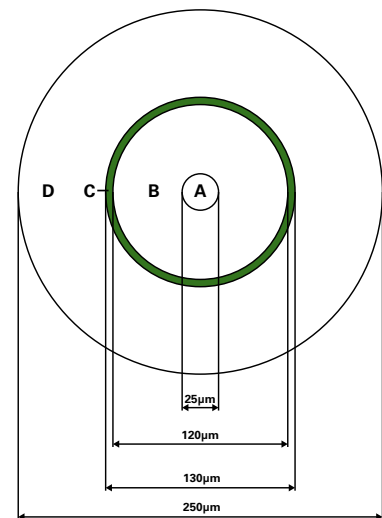
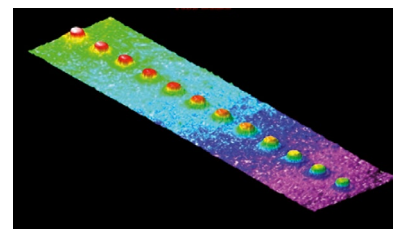
Other Parameters

There exist other parameters in addition to core dip and protrusion that are crucial to the surface quality of fiber ends and in turn to the transmission properties and service life of a connector. These include ferrule radius and fiber radius. The overall geometry of the fiber end must be examined during production and quality assurance processes.

R&M's tight tolerances, that exceed even those established under EN 50377-15-1, are an essential requirement in ensuring the maximum quality of its plug connectors. R&M's 100% test in the manufacturing process alone provides a guarantee that these tolerances will be observed. R&M therefore subjects all insertion surfaces to an interferometric inspection (see figure to right). Defective ferrules are re-processed until they comply with our specified tolerances.

We also check the insertion loss and return loss in all plug connectors. The displacement between two connected fibers must be as small as possible in order to reduce the insertion loss of plug connections. In addition, R&M measures the internal polarity of fibers in all MPO/MTP® cables to ensure they are correct. Polarity is the connection of fibers, e.g. that fiber Tx1 (transmission channel 1) leads to Rx1 (receiving channel 1), Tx2 to Rx2, Tx3 to Rx3, etc.

A fourth R&M test is the optical surface test which must be carried out even if the interferometric test shows 100%. This test examines fiber ends surfaces for scratches, outbreaks (shrinkage holes), adhesive residue and impurities. All zones must be absolutely dirt-free so that the defined optical properties of the connector can be achieved. The connector is divided into four zones, A through D, in which different impurities or damage are permitted (see figure to right).



Trunk Cable

An MPO/MTP® plug connector with 12 or 24 fibers cannot be manually assembled on site during installation. It comes completely pre-assembled from the factory and is normally connected to trunk cables (see figure to right) that are delivered in the required length.

What on the one hand requires more care during planning yields numerous advantages on the other hand:

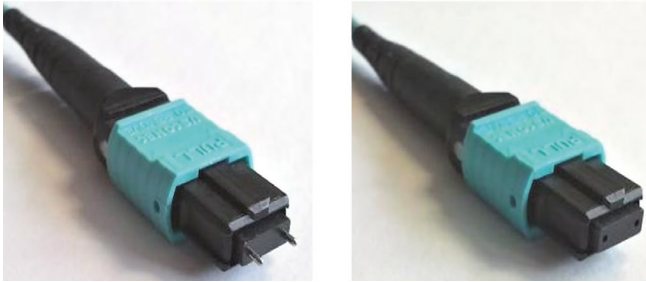


- **Higher Quality**
Higher quality is usually achieved through factory assembly and inspection of individual parts. A factory-prepared inspection certificate is also useful for long-term documentation and in turn quality assurance purposes.
- **Minimum Skew**
A crucial factor in achieving a successful parallel optical connection is keeping the signal offset (skew) between the four or ten parallel fibers to an absolute minimum. Only in this way can information be successfully re-synchronized and re-combined at its destination. Factory-assembled trunk cables allow skew to be measured, minimized and logged.
- **Shorter Installation Times**
Pre-assembled MPO cable systems provide plug-and-play advantages and can be inserted and set up immediately. This reduces installation time enormously.
- **Better Protection**
Because they are completely assembled at the factory, cables and plug connectors remain completely protected from environmental influences. Optical fibers that lie open in splice trays are at a minimum exposed to ambient air and may age faster as a result.
- **Smaller Cable Volumes**
Smaller diameters can be realized in MPO cabling systems that are produced from loose tube cables. The results are correspondingly smaller cable volumes, better conditions for acclimatization in the data center and a lower fire load.
- **Lower Overall Costs**
When splice solutions are used, a few factors that are not always foreseeable boost total costs: time-intensive, equipment-intensive splicing, needs for specialty works, bulk cables, pigtailed, splice trays, splicing protection, holders. In contrast, pre-assembled trunk cables not only bring technical advantages, but usually result in lower total costs than splicing solutions.

3.10.2 Migration Path to 40/100 Gigabit Ethernet

By way of introduction, we first present all components that are required for a parallel optical MPO connection and that therefore are also required in the process for migrating glass fiber cabling up to 40/100 gigabit Ethernet.

Plug Connectors

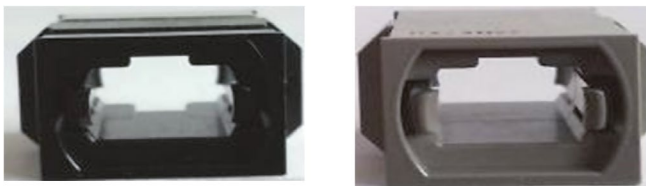


MPO male with pins (left) and MPO female without pins (right)

Since MPO plug connectors contact up to 24 glass fibers in only one connection, it is extremely important that the connection be both stable as well as correctly aligned so it maintains the required transmission parameters. A faulty connection can lead to component damage or even complete link failure. MPO connectors come in both male versions (with pins) and female versions (without pins). These pins guarantee that the fronts of plug connectors match up exactly so that fiber ends do not shift out of place. The catches or guide grooves (keys) located on the top of plug connector units are clearly recognizable, and ensure connectors are correctly aligned when they are inserted in an adapter.

Adapters

MPO adapters can be divided into two types, depending on how the guide groove (key) is positioned:



Adapters - Key-up to key-down (left), key-up to key-up (right)

- **Type A: Key-up to key-down**
The groove lies at the top on one side of the adapter and at the bottom on the other side, so that the two connectors are shifted by 180° toward one another when they are connected.
- **Type B: Key-up to key-up**
Both grooves are at the top, so both connectors are in the same position when connected.

Connection Rules

1. Always create an MPO plug connection using one male plug and one female plug, as well as an MPO adapter.
2. Never create a male-to-male or female-to-female connection. The fiber cores of the two connectors in a female-to-female connection will not be exactly at the same height, since guide pins are missing. This will result in performance losses. A male-to-male connection experiences even a greater loss in performance, since in this case guide pins bump up against guide pins. Not only does this prevent contacting, but plugs may also be damaged.
3. Do not disassemble MPO connectors. The pins in an MPO plug can be removed only with great difficulty, and fibers can become broken in the process. Not only that, the warranty becomes invalid when the connector housing is opened!

Cables

MPO cables come pre-assembled when delivered, so careful advance planning of these components is required. However, this additional effort is outweighed by the technology's clear advantages – shorter installation times, quality that is inspected and guaranteed, and increased reliability.

Trunk Cables/Patch Cables

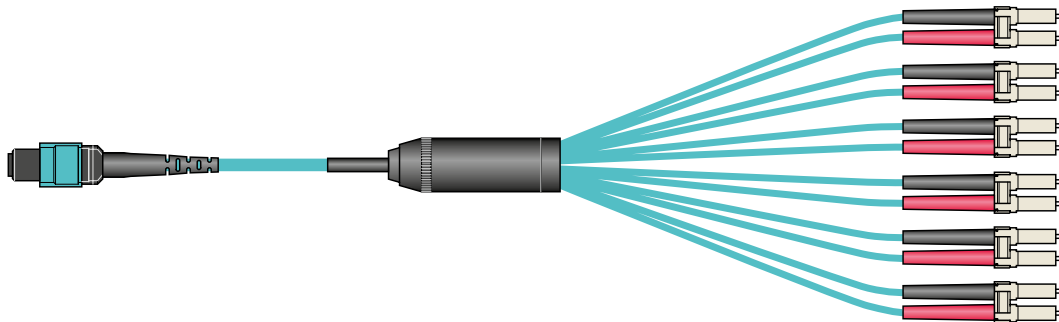
Trunk cables are used to establish the connection between MPO modules, as a permanent link. These cables are available in fiber counts of 12, 24, 48 and 72, with their ends fitted with either 12-fiber or 24-fiber MPO connectors. MPO patch cords are used only in applications with 40-gigabit and 100-gigabit active devices (with an MPO interface). The ends of MPO patch cords are likewise fitted with either 12-fiber or 24-fiber MPO connectors.



Trunk/patch cords come in male – male (left) and female – female (right) versions

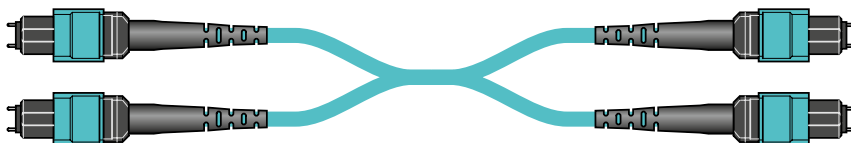
Harness Cables

Harness cables make it possible for multi-fiber cables to transition to single fibers or duplex connectors. The 12-fiber harness cables provided by R&M, for example, come pre-assembled with MPO-side male or female connectors; fan-out legs are available with LC or SC connectors.



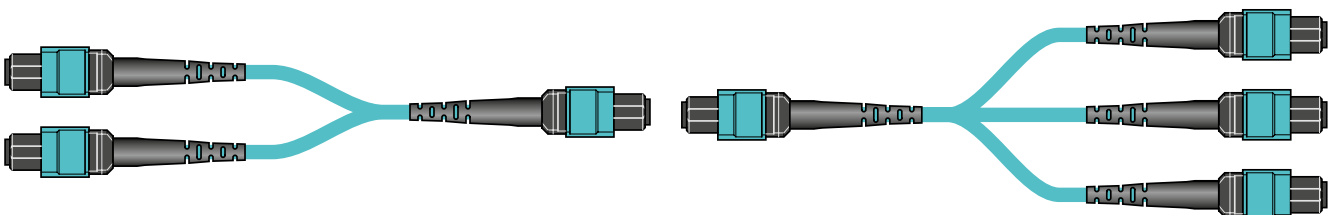
X Cables

24-fiber X cables are typically used to connect MPO modules. In this process, each of the two ends are terminated with two fan-out legs, and therefore two 12-fiber MPO plugs.



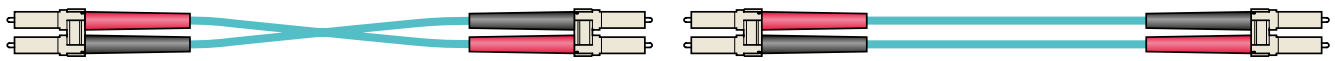
Y Cables

Y cables are normally used in a 2-to-1 design. One typical application of this design is combining two 12-fiber trunk cables into one 24-fiber patch cord when migrating up to 100 GbE. The 1-to-3 design is rather uncommon, but makes it possible to combine three 8-fiber MPO connectors with a 24-fiber permanent link, e.g. for a migration to 40 GbE.



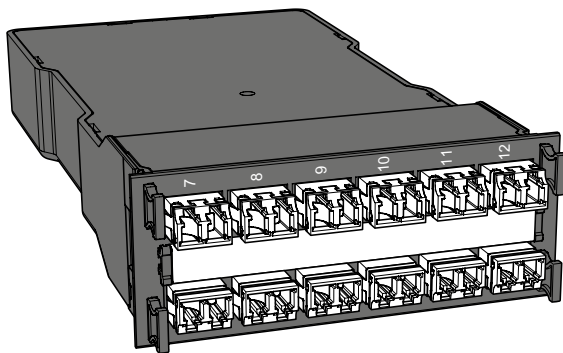
Duplex Patch Cables

These cables are not MPO cables, just conventional duplex cables. They are available in crossed (A-to-A) and uncrossed (A-to-B) versions, and come pre-assembled with LC or SC connectors.

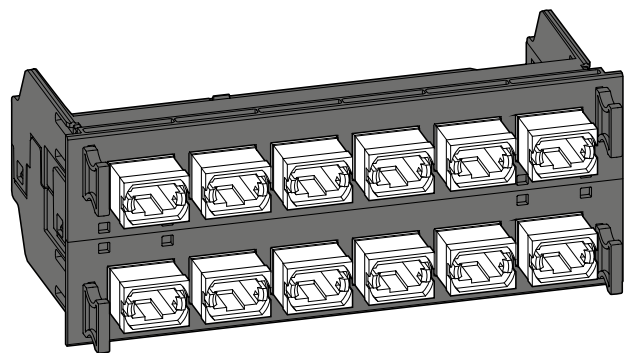


Modules and Adapter Plates

These devices represent the connection between permanent links and patch cords. The MPO module makes it possible to distribute the fibers supplied by trunk cables to duplex cables. Pre-assembled MPO modules come fitted with 12 or 24 fibers, front-side LC, SC or E-2000™ adapters and rear-side MPO.



MPO module with duplex adapters



MPO adapter plate (6 x MPO/MTP®)

An adapter plate connects MPO trunk cables with an MPO patch cord or harness cable. MPO adapter plates are available with 6 or 12 MPO adapters in Type A or Type B.

Polarity Methods

While the coding on MPO plug connectors and adapters are intended to ensure that the plug connection is always oriented correctly, the polarity methods A, B and C defined under TIA-568-C are intended to guarantee the bi-directional assignment is correct. This section contains a brief explanation of these methods.

Method A

Method A uses straight through-connected Type A backbones (pin1 to pin1) and MPO adapters of Type A (key-up to key-down). An uncrossed patch cord (A-to-B) is used at one end of the link, while a crossed patch cord (A-to-A) is used at the other end. The pairwise polarity inversion therefore occurs on the patch side. Note that only one A-to-A patch cord per link may be used.

R&M has been providing MPO components for method A since 2007. This method is very easy to implement, since, for example, only one case type is required, and the method is certainly the most widely distributed.

Method B

Method B uses crossed Type B backbones (pin1 to pin12) and MPO adapters of Type B (key-up to key-up). However, as the Type B adapters are used differently on both sides (key-up to key-up, key-down to key-down), a higher level of planning is required. An uncrossed patch cord (A-to-B) is used at both ends of the link.

Method B is not widespread, due to the higher amount of planning required and also because the method does not allow for use of single-mode MPO connectors. In addition, R&M does not support this method (or rather, only upon specific customer request).

Method C

Method C uses pairwise crossed Type C backbones and MPO adapters of Type A (key-up to key-down). An uncrossed patch cord (A-to-B) is used at both ends of the link. The pairwise polarity inversion therefore occurs in the backbone, which involves an increased level of planning in the case of linked backbones. An A-to-A patch cord is required when the number of linked backbones is even.

Method C is not very widespread, due to the increased planning effort required and also because the method does not provide for a migration path to 40/100GbE. R&M does not support method C (or rather, only upon specific customer request).

Method S

Method S (designation defined by R&M) has been available since April 2013. This method requires only one patch cord type (A-to-B). The fiber cross-over for duplex signal transmission (10GBASE-SR) takes place in the pre-assembled case. The connectivity scheme for trunk and patch cords or light guidance always remains the same, even for parallel transmission in the construction of 40/100 GbE systems.

As the twelve LC ports are divided up by Tx and Rx, all Tx fibers are routed to one 12-fiber MPO and all Rx fibers to the other 12-fiber MPO. These two MPOs can be bundled, for example into one X cable. The modules include Type B adapters.

This makes symmetric cabling for 1G, 10G, 40G and 100G possible when the method is implemented in combination with Type B trunks. As a result, a direct upgrade can be realized cost-effectively and completely without complication, since cases just need to be replaced with adapter plates.

The following table reviews and summarizes the methods described above:

	Polarity Method	MPO/MTP Cable	MPO Module	Duplex Patch Cord Type
TIA-568.C Standard (Duplex signals)	A	Type A	Type A (Type A adapter)	1 x A-to-B 1 x A-to-A
	B	Type B	Type B1, Type B2 (Type B adapter)	2 x A-to-B
	C	Type C	Type A (Type A adapter)	2 x A-to-B
	S	Type B	Type S (Type B adapter)	2 x A-to-B
	Polarity Method	MPO/MTP Cable	Adapter Plate	MPO/MTP Patch Cord
TIA-568.C Standard (Parallel signals)	A	Type A	Type A	1 x Type A 1 x Type B
	B	Type B	Type B	2 x Type B

Polarity Methods and Component Types



Type A Adapter
Key-up to key-down



Type B Adapter
Key-up to key-up



A-to-B duplex patch cord



A-to-A duplex patch cord

The construction of a completely new data center is definitely not an everyday occurrence. In this case, planners and decision makers have the possibility to immediately build upon the latest technologies and provide for higher bandwidths. By contrast, the gradual conversion and upgrade of an existing data center infrastructure to 100 Gbit/s will, indeed must, involve a broad-scale effort implemented over a number of years. A sensible approach in this case is a gradual replacement of existing passive components followed by a replacement of active components as soon as these become available and economically viable. This upgrade is normally carried out in three stages:

Upgrading Existing 10G Environments

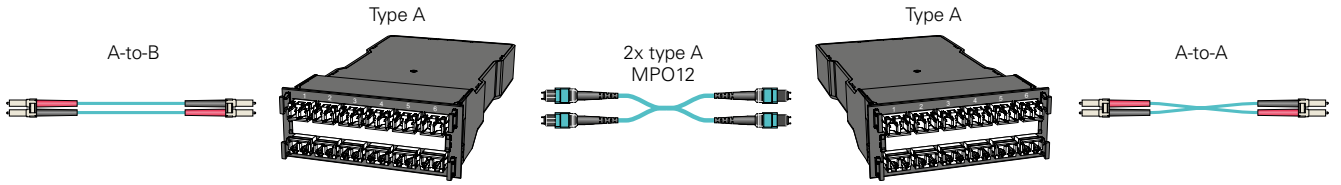
Guidelines for data center network planning can be found in the standards TIA-942-A, EN 50173-5, EN 501742:2009/A1:2011, ISO/IEC 24764 and the soon-to-be-available IEC 50600-2-4. The steps below only describe the steps involved in migration, and require that the network is appropriately planned and installed.

Without a doubt, the first step in migrating from 10 GbE to 40/100 GbE is to upgrade the existing 10 GbE environment. In this process, the backbone is replaced by a 12-fiber MPO cable, and LC/MPO modules and patch cords establish the connection to 10G switches.

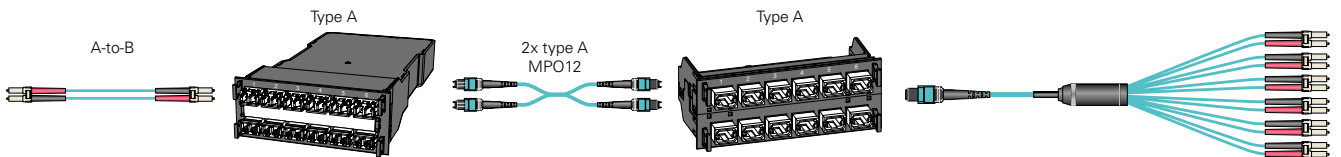
It is important to note here that the TIA-568-C standard for duplex signals refers to female trunk cables and male modules. However, for reasons of simpler migration, R&M recommends that trunk cables be installed as male versions and modules as female versions, so that female-female MPO patch cords can be connected to the trunk during the migration up to parallel optical signals. This is one step to reducing the complexity of the cabling systems. Migration is also possible using conventional methods and female-female trunk cables. However, because transceivers have an MPO male interface, either the existing trunk cables must be replaced or "hybrid" patch cords (male-female) used.

A number of different configurations result depending on the existing infrastructure and polarity method used.

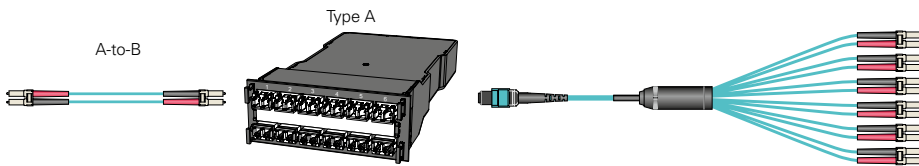
Method A



10G, case 1 – MPO trunk cables (Type A, male-male) replace the existing duplex trunk (center), MPO modules (Type A, female) enable the transition to the existing A-on-B (left) and A-on-A (right) LC duplex patch cords. Since HD MPO modules have two trunk-side MPO adapters, the option is available of consolidating the two 12-fiber MPOs into one 24-fiber X cable.

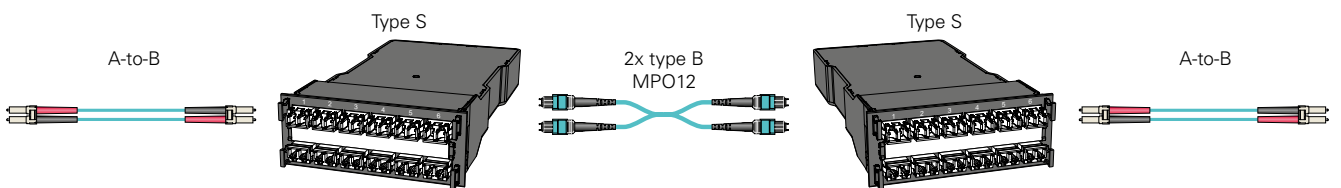


10G, case 2 – MPO trunk cables (Type A, male-male) replace the duplex trunk (center), an MPO module (Type A, female) enables the transition to the existing A-to-B LC duplex patch cord (left), adapter plate (Type A) and harness cable (female) replace the LC duplex patch cord.



10G, case 3 – Connection from A-to-B LC duplex patch cord, MPO module (Type A, female) and harness cable (male).

Method S

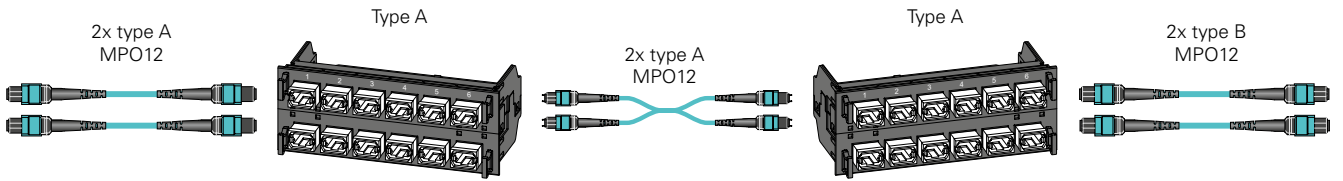


10G – MPO trunk cables (Type B, male-male) replace the duplex trunk (center), MPO modules (Type S, female) enable the transition to the existing A-to-B LC duplex patch cords (left, right). Since the Type S module divides Tx and Rx up onto one MPO each, an X cable, or two trunks, is required.

Upgrade from 10G to 40G

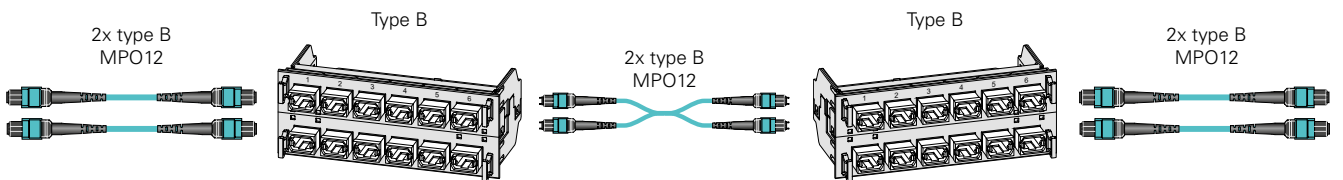
If the next step involves replacing 10G with 40G versions, the next adaptation can be carried out very easily by using MPO adapter plates in place of MPO modules. In addition, the polarity method in use must be observed.

Method A



Replacement of MPO modules with Type A adapter plates and LC duplex patch cords by MPO patch cords of Type A, female-female (left) and Type B, female-female (right). An existing X cable can now serve two 40G links.

Method S and Method B

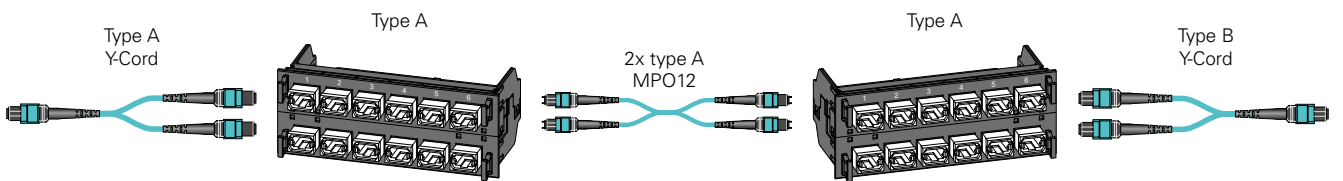


Replacement of MPO modules with Type B adapter plates and LC duplex patch cords by MPO patch cords of Type B, female-female (left, right). When this configuration is compared to the TIA-568.C standard, we notice immediately that methods S and B are identical for parallel optical signals. An existing X cable can serve two 40G links in this case as well.

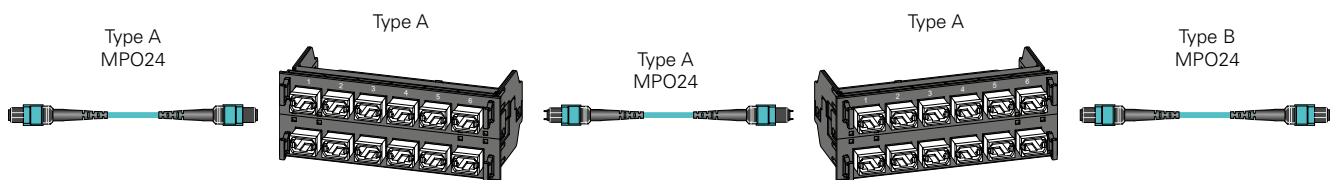
Upgrade from 40G to 100G

In the final step, the use of 24-fiber MPO cables may also be necessary when 100G switches are being implemented¹⁾. In this case, either the existing 12-fiber connection can be extended by a second 12-fiber connection, or replaced by one with 24 fibers.

Method A

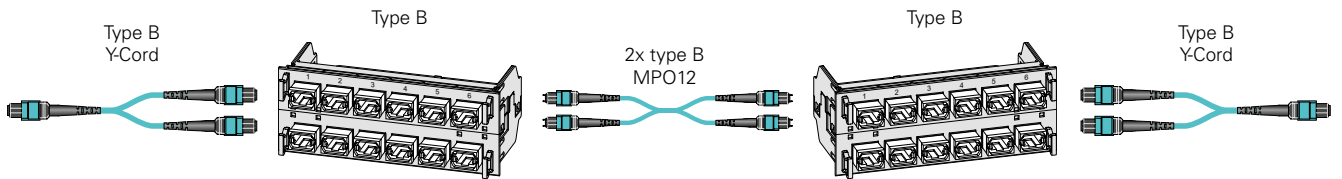


Extension of MPO trunk cable (male-male) by a second one, Type A adapter plates remain as is, patch cords are replaced by Y cables.

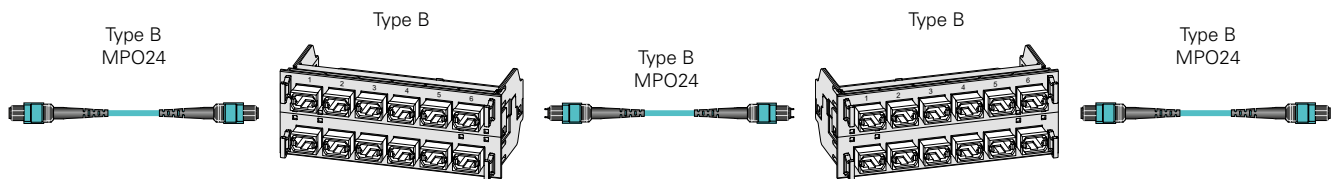


The MPO-24 solution – Use of an MPO-24 trunk cable of Type A male-male, Type A adapter plates remain as is. MPO-24 patch cords of Type A, female-female (left) and Type B, female-female (right) are used as patch cords.

¹⁾ This will be the case for 100GBASE-SR10 (10x 10G) applications. On the other hand, if 100GBASE-SR4 (4x 25G) applications should be used, the scenario would correspond to that in section 3.2, since cabling can be realized with 12-fiber MPOs.

Method S and Method B

Extension of MPO trunk cable (male-male) by a second one, Type B adapter plates remain as is, patch cords are replaced by Y cables.



The MPO-24 solution – Use of an MPO-24 trunk cable of Type B male-male, Type A adapter plates remain as is. MPO-24 patch cords of Type B, female-female are used as patch cords on both sides.

Summary

The implementation of MPO components and parallel optical connections translates into new challenges for data center planners and decision makers. Cable lengths must be carefully planned, MPO types correctly selected, polarities maintained over the entire link and insertion loss budgets calculated precisely. Short-term changes are either barely possible or are not possible at all, while errors in planning can be expensive.

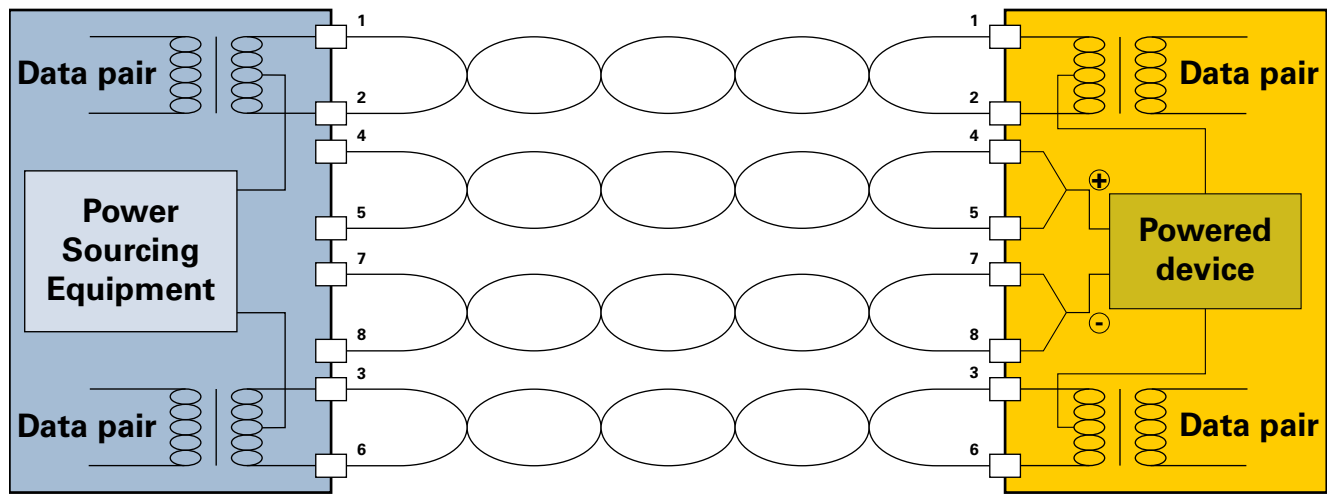
Nevertheless, it is very worthwhile to switch to the new technology, especially since it is already becoming a technological necessity over the medium term. It therefore makes sense to have switch points already placed early on, and to at least adapt passive components to future requirements. The high expense is more than offset by the technology's short installation times, quality that is inspected and documented for every single component, and operational reliability and investment security that will bring peace of mind for years to come.

3.10.3 Power over Ethernet (PoE / PoEplus)

PoE and PoEplus can be used in data centers to remotely supply power to infrastructure and monitoring devices. The standard and performance of the supported device (powered device = PD):

- **IEEE 802.3 Section Two:** Power over Ethernet (PoE) = 12.95 W power
- **IEEE 802.3 Section Two:** Power over Ethernet (PoEplus) = average 25.50 W power

The new standard, IEEE 802.3 Section Two, was released in October 2009. The definitions of PD (powered device) and PSE (power sourcing equipment) are the same as in the PoE IEEE 802.3 Section Two standard.



An endspan example as defined in the PoE IEEE 802.3 Section Two standard.

Compatibility between PoE and PoEplus PD/PSE Versions

PD operation on PSE		
	PoE-PSE	PoEplus-PSE
PoE-PD	Operational	Operational
PoEplus-PD < 12,95 W	Operational	Operational ^{Note}
PoEplus-PD > 12,95 W	PD with active display for users	Operational ^{Note}

PD = Powered Devices

PSE = Power Sourcing Equipment

Note: Operation with extended performance classification

The terminology makes a distinction between devices with low power consumption and those with high power consumption:

- Type 1: Low power consumption
- Type 2: High power consumption

The following table shows some of the differences between PoE and PoE-plus. Heat generation is a problem with these technologies due to the higher current flow into cabling. Some suppliers recommend using higher category cables in order to mitigate this effect.

	PoE	PoEplus
Cable requirement	Cat. 3 or higher	Type 1: Cat. 3 or higher Type 2: Cat. 5 or higher
PSE current (A)	0.35 A	Type 1: 0.35 A Type 2: 0.6 A
PSE voltage (Vdc)	44-57 Vdc	Type 1: 44-57 Vdc Type 2: 50-57 Vdc
current (A)	0.35 A	Type 1: 0.35 A Type 2: 0.6 A
PD voltage (Vdc)	37-57 Vdc	Type 1: 37-57 Vdc Type 2: 47-57 Vdc

Differences between PoE & PoEplus / Source: Ethernet Alliance, 8/2008

Problems Due to Cable Heating

The transfer of energy via a universal communication cabling system leads to a temperature increase in the cabling, based on the amount of energy transferred and the conductor cross-section. The cable in the center of a bundle naturally heats up more since heat cannot be dissipated here. With heat increasing in the cable bundle (ambient temperature + temperature increase), insertion loss increases as well, which can lower the maximum permissible cable length.

In addition, the standard limits the maximum temperature (ambient temperature + increase) to 60° C.

Cable Type	Conductor Cross-Section	Approx. Temperature Increase
Cat. 5e / u	AWG 24	10° C
Cat. 5e / s	AWG 24	8° C
Cat. 6 / u	AWG 24+	8° C
Cat. 6A / u	AWG 23	6° C
Cat. 6A / s	AWG 23	5° C
Cat. 7	AWG 22	4° C

Temperature Increase in PoEplus

These effects result in two limiting factors:

- Reduction in the maximum permissible cable length due to higher cable attenuation as a result of the higher temperatures
- The maximum temperature of 60° C established in the standard

The temperature increase for different cable types was determined by tests carried out by the IEEE 802.3 Section Two PoEplus work group (as measured in bundles of 100 cables).

Tests have shown that the use of AWG23 and AWG22 cables for PoEplus is not strictly necessary at room temperature. The problem of increased cable temperatures caused through the use of PoEplus must be taken into consideration when long installation cable and/or patch cord lengths are used, and at extra-high ambient temperatures, e.g. in the tropics.

Given a shielded Cat. 5e/u cable, an additional temperature increase of 10° C resulting from the use of PoEplus at an ambient temperature of 40° C means a reduction in permissible link length of approximately 7 m. With a shielded Cat. 5e/s cable and an ambient temperature of 40° C this reduction would only be about 1 m.

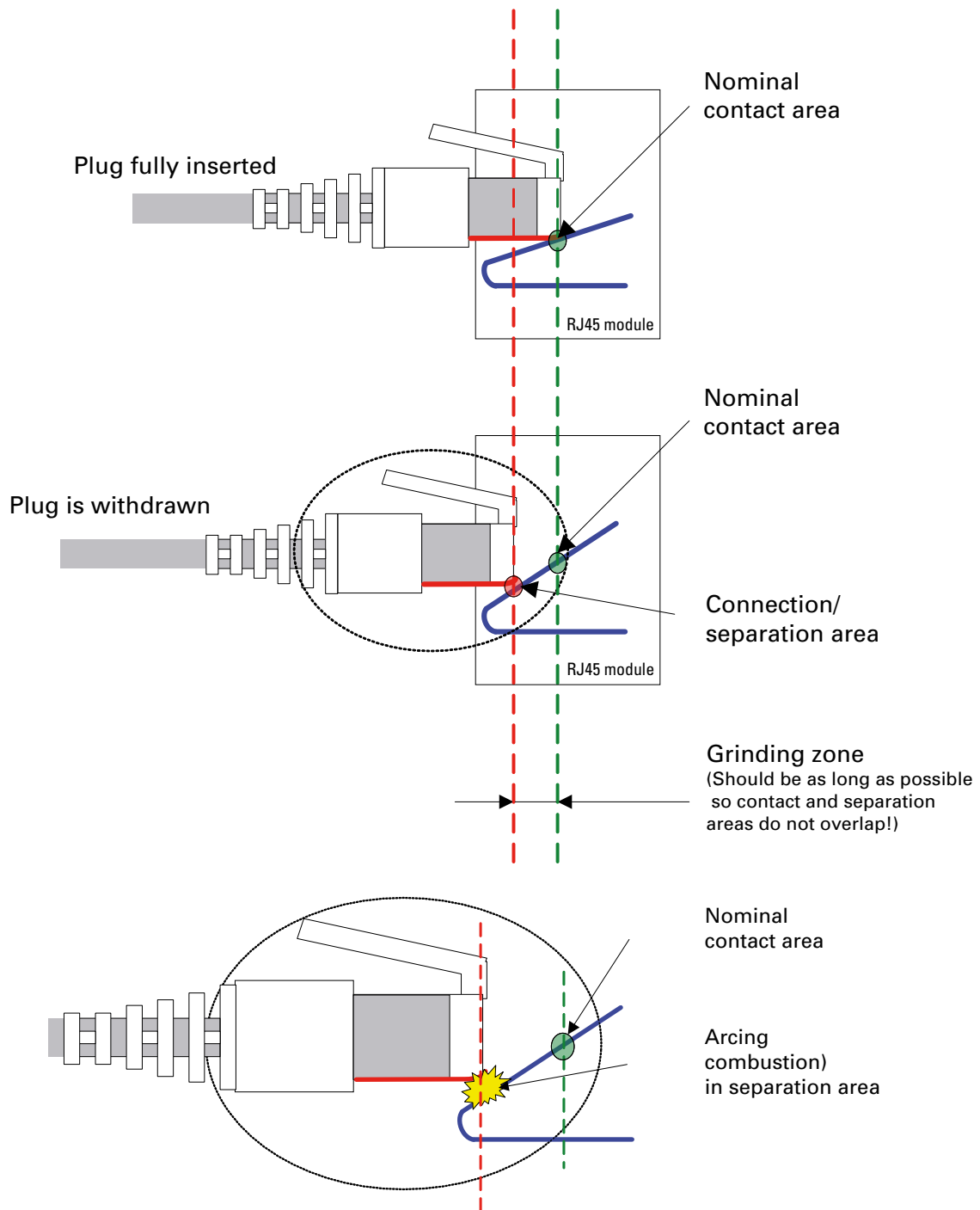
This 7-meter or 1-meter reduction in cable length can be compensated for by a cable of a higher category with a large core diameter. Nevertheless, a careful study of the cost-benefit ratio of such a solution is recommended. In addition, planners should take into account the fact that the length restrictions for class E and F are much more severe than for PoEplus and can limit the usable link length of the cable.

In all cases, the effects of heat dissipation both in cables and in the surrounding environment must receive special consideration when planning an installation for PoEplus. This applies regardless of the cable type to be used.

Note Regarding Plug Connectors

R&M has studied the effects of PoE on plug connectors, in particular the damage that results from the arcing which may occur when a current-carrying line is disconnected. In addition, R&M was co-author of a technical report on this subject, IEC SC48B published under the title "The effects of engaging and separating under electrical load on connector interfaces used in Power-over-Ethernet (PoE) applications".

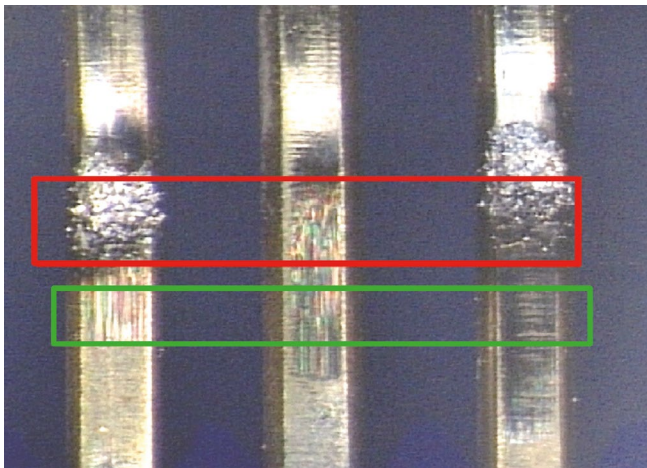
This document introduced the concept of nominal contact area. As a plug is inserted, the contact point between A (plug) and B (socket) moves along the surface of the contacts from the first contact point (connection/separation area) to the final contact point (nominal contact area). These two areas are separated by the grinding zone.



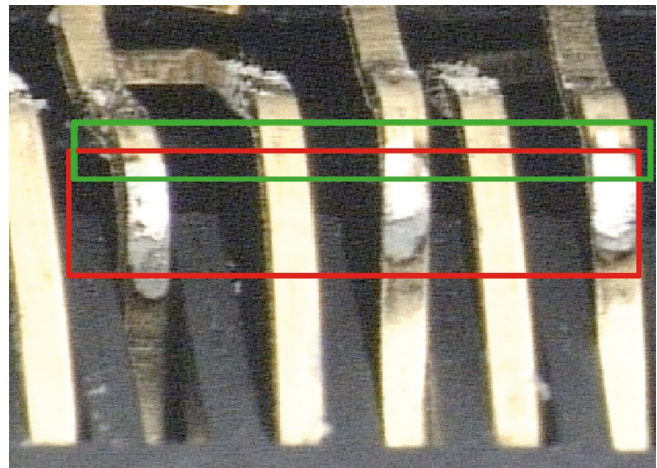
Depiction of concept of nominal contact area

Studies have shown that the design of the modular plug connectors described in the IEC 60603 standard are a more conventional way of ensuring that the zone in which contact is broken and in which arcing may occur remains separated from the zone in which contact is created between the plug and socket during normal operation (nominal contact area).

The image to the left (figure below) shows an example of a good contact design in which damage does not affect the contact zone (R&M). The image at the right shows a poor contact design in which the two areas "nominal contact area" and "connection/separation area" overlap, so that the contacts in the contact area may be damaged if arcing occurs as the plug is inserted or removed.



Good contact design (R&M module)



Poor contact design due to overlap of two areas
(nominal contact area and connection/separation area)

- Nominal contact area
- Connection/separation area

Photos: R&M

The increased performance provided by PoEplus can lead to heavy arcing during disconnection, which makes this problem worst. In addition with new connection hardware in categories 6A, 6A, 7 and 7A contact design deviates significantly from a traditional/conventional design and is therefore affected by electrical discharges.

Unfortunately, standardization committees have not yet taken this problem into account sufficiently. Test methods and specifications for ensuring that connection hardware will fulfill PoEplus requirements have not yet been adopted.

Up to this point, efforts in both IEEE and ISO/IEC committees have concentrated mainly on defining limit values for cable heating. A guarantee of PoEplus support for a cabling system is premature as long as connection hardware is not included in these considerations.

Conclusions

The success of PoE up to this point and the demand for PoEplus show that these technologies are meeting a need in the market that continues to grow. A number of facts exist that must be taken into consideration when this technology is implemented. These include the supply and safeguarding of power to server racks as well as management of the additional heat produced there through the use of PoEplus-capable switches.

Careful consideration is also required for the cabling system itself. Substantial efforts have been undertaken to study the effects of increased heat in cabling system. As we have seen, the combination of higher ambient heat and the effect of PoEplus lead to length restrictions for all cabling types. Planners and users are therefore required to select cabling systems according to their use and requirements, after checking the specifications and guidelines that have been provided.

Substantial efforts are also required to study the effects that arise when current-carrying connection hardware is disconnected. This work has unfortunately not been performed to date by standardization committees, so no specifications or testing methods exist for ensuring compatibility with the PoEplus standard.

3.10.4 Short Links

ISO/IEC 11801 Amendment 2 from 2010 promises compliance with class E_A when Cat. 6_A components are used only if the minimum length of 15 m is maintained for the permanent link (PL). The standard allows the use of shorter PLs if the manufacturer has guaranteed the PL requirement will be observed.

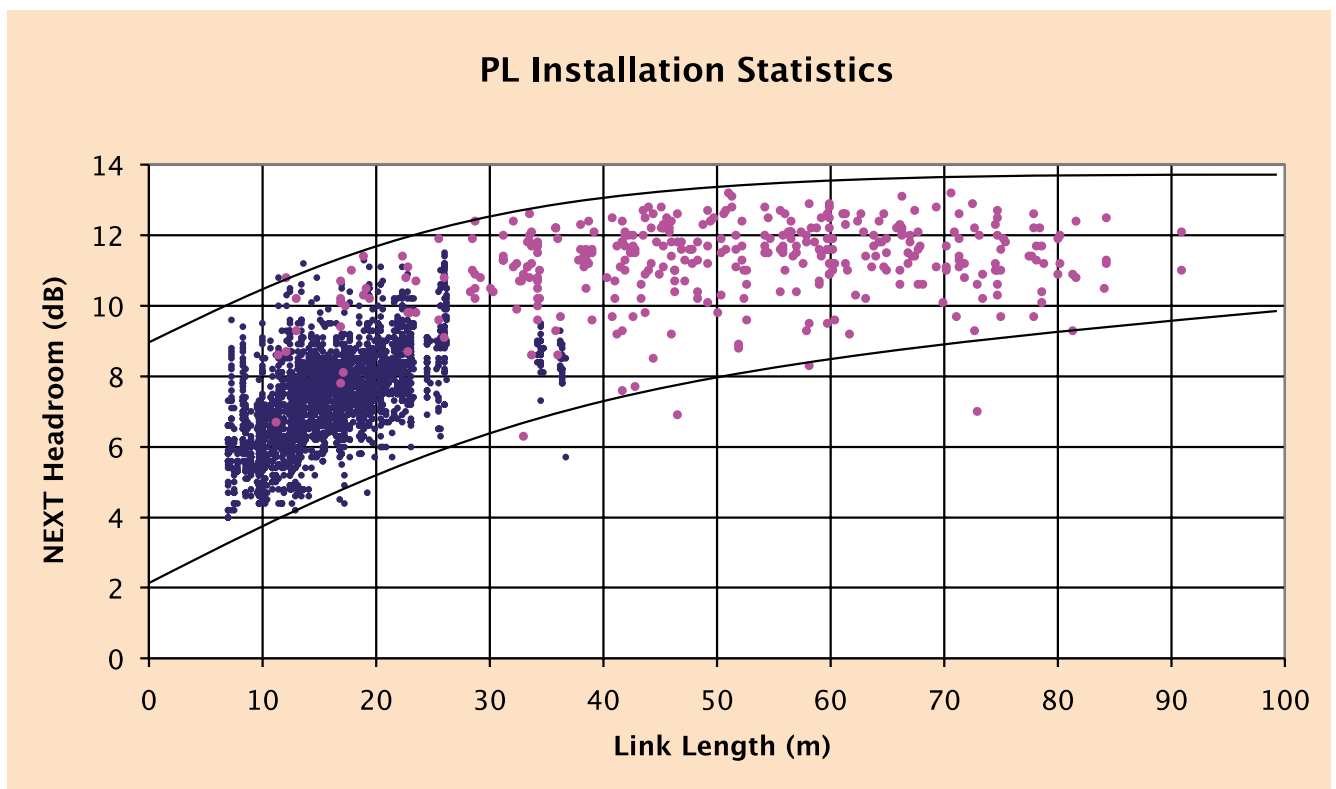
Desire for Short Links and Demand for Reserves

Many data centers are moving towards shortening links in order to save materials, energy and costs. How does this affect network performance and transmission reliability? This section will examine that question since it plays a critical role in network planning.

First note that the distance between the two modules in a 2-connector permanent link are shorter, so cable attenuation between the two modules drops. As a result, the interference from the remote module increases.

However, since the standard only provides one module in its calculation model, shortening of the link can lead to difficulties. In particular, it is no longer possible to maintain limit values for NEXT (near end cross talk) and RL (return loss). The standard assumes a minimum link length of 15 m for this.

So what happens now if a module of extremely high quality is paired with a cable of extremely high quality? This results in a PL with extremely high reserves in the length range from 15 m to 90 m. For example, R&M's Cat. 6_A ISO connection module can achieve typical NEXT reserves of 6 dB at cables lengths of 15 m, and 11 dB at cable lengths of 90 m (see graphic below).



NEXT reserve for permanent links, measured at an installation using the new Cat. 6_A module from R&M.

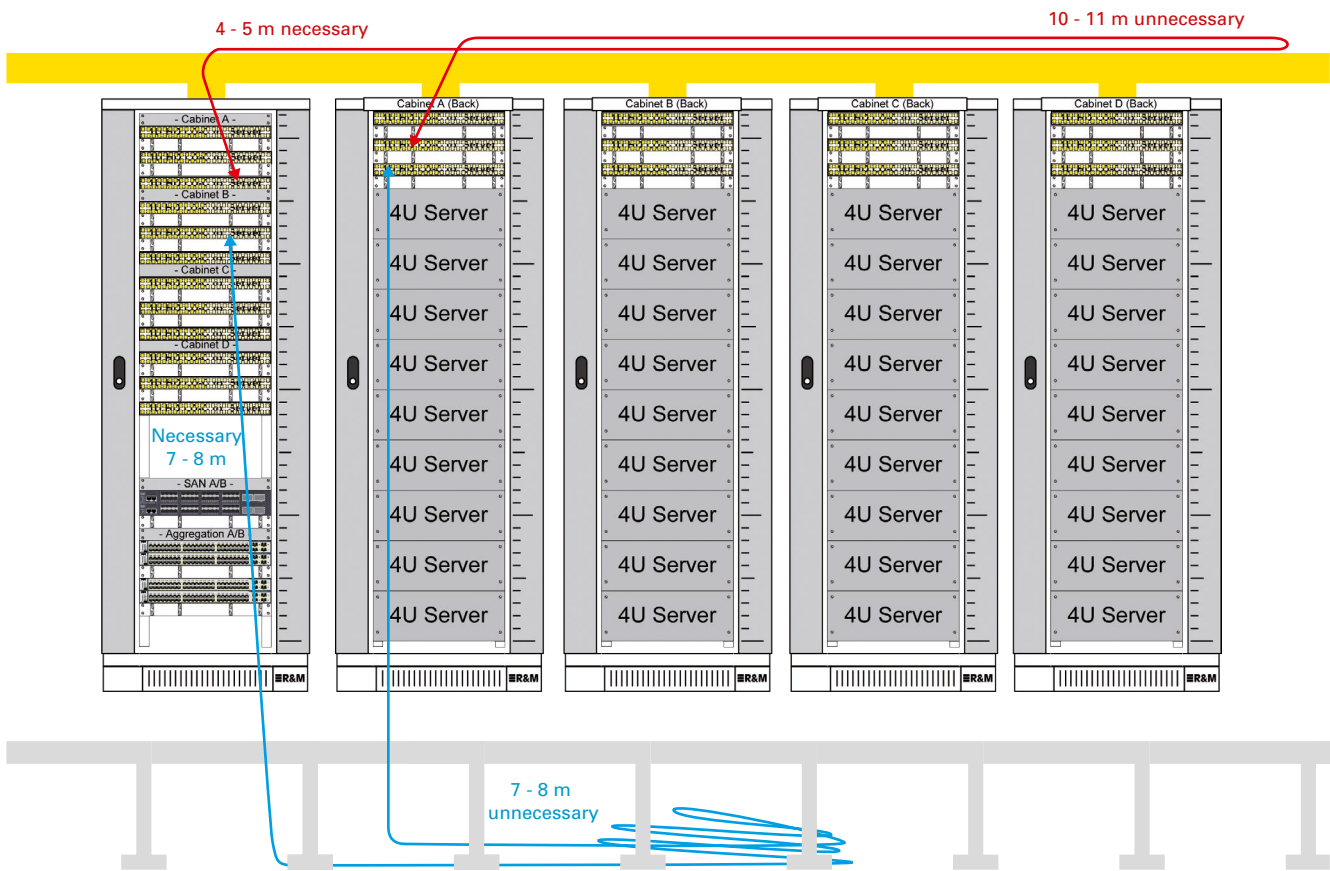
The zero line corresponds to the limit value defined under ISO/IEC 11801 Amendment 2.

R&M offers a guarantee program for qualified partners which guarantees a minimum NEXT Reserve of 4 dB for minimum cable lengths of 15 m, if the permanent link is properly installed using our Cat. 6_A ISO connection module. Nevertheless, the high reserves of the system give users the option of installing even shorter PLs which fulfill all ISO/IEC 11801 Amendment 2 requirements.

The Advantage of Additional Reserves

It is always a good idea to design permanent links to only be as long as necessary. In many cases, however, permanent links fall short of the minimum length of 15 m, which is frequently the case in data centers. When data centers make use of components that only fulfill standard requirements, permanent links must be artificially extended to 15 m using loops. This is one way to ensure compliance with limit values. However, this extension does not only result in additional costs, but the cable loops also fill cable runs unnecessarily and obstruct ventilation. This in turn increases infrastructure costs and energy consumption.

R&M's Cat. 6A ISO module now makes it possible, thanks to its large reserves provided for standard length, to reduce minimum lengths down to as much as 2 m. This length is sufficient for covering the usual distances encountered in data centers.



Use of short links in a typical end of row cabling architecture in a data center

An average cable length of 4 to 5 m is sufficient for cabling installed between server cabinets and the network cabinet if cables are inserted from above into a cable routing system. An average length of 7 to 8 m is sufficient for cable that is routed through a double floor. The class E_A/Cat. 6_A solutions developed by R&M saves data center operators from having to use unnecessary loops to extend cable lengths to 15 m.

How Are Short Permanent Links Measured?

ISO/IEC 11801 Amendment 2 (Table A.5) has eased requirements for short 2-connector permanent links under 12 dB insertion loss starting from 450 MHz. Even when the effect only concerns the range from 450 MHz to 500 MHz, the field measurement device should always be set to "Low IL" during measurements. Easing of NEXT requirements maximum 1.4 dB. The following images show a measurement setup as well as tests.



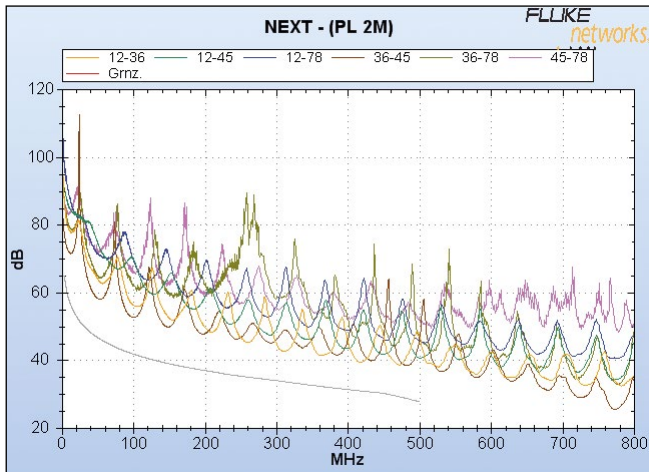
Test for a short permanent link (PL2) using the DTX 1800 Cable Analyzer

Übersicht		PASS
PL 2M		
ISO11801 PL2 Class Ea Low IL		
✓ Wire Map		
✓ Widerstand		
i Länge	2,1 m	
✓ Laufzeit		
✓ Abweichung		
✓ Einfüg.-Dämpf.	(38,0 dB)	
i Rückflussdämpf.	(3,0 dB)	
i NEXT	(6,4 dB)	
Element markieren, ENTER drücken		
	Seite nach oben	Seite n. unten

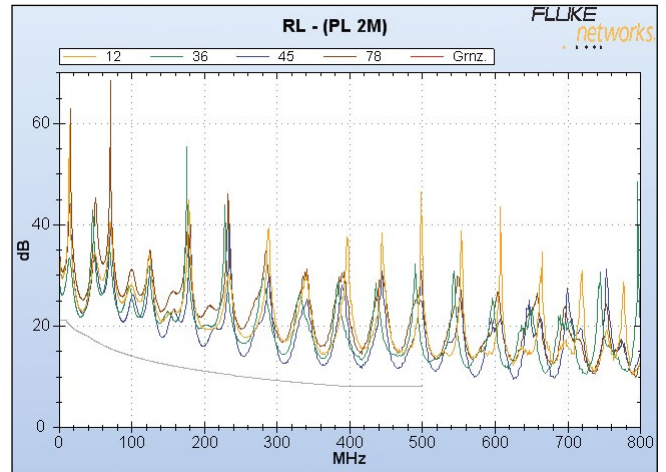
Übersicht		PASS
PL 2M		
ISO11801 PL2 Class Ea Low IL		
i NEXT	(6,4 dB)	▲
i PS NEXT	(7,5 dB)	
i ACR-N	(16,1 dB)	
i PS ACR-N	(17,5 dB)	
✓ ACR-F	(19,3 dB)	
✓ PS ACR-F	(19,5 dB)	
i HDTDR-Analyser		
i HDTDX-Analyser		
Element markieren, ENTER drücken		
	Seite nach oben	Seite n. unten

Test results: The permanent link with length 2.1 m fulfills all ISO/IEC 11801 requirements.

Permanent Link Measurements



NEXT measurement for a permanent link 2 m in length, set up using R&M components.



RL measurement at same permanent link.

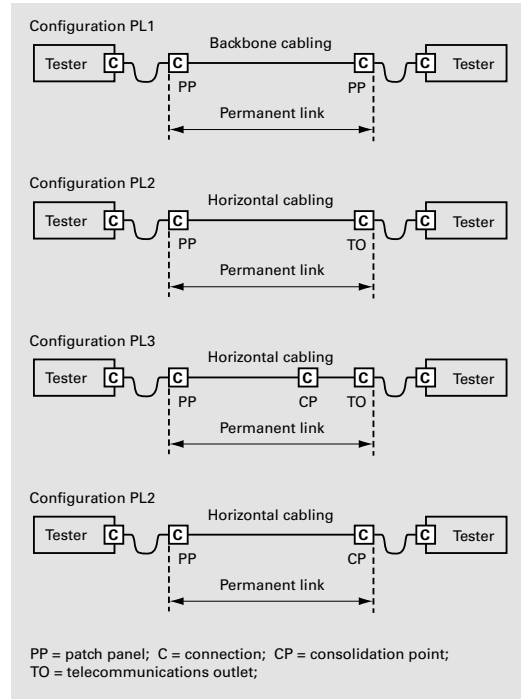
Permanent Link Configurations Established under ISO/IEC 11801 Amendment 2

ISO/IEC distinguishes between four permanent link configurations (right), which may be relevant for network planning. Parameters that determine transmission quality include NEXT and RL.

ISO/IEC calculates NEXT limit values for all four configurations [in dB] for the frequency range $1 \leq f \leq 300$ [MHz] according to the formula:

$$NEXT > -201g \left(10^{\frac{74,3 - 151g(f)}{-20}} + 10^{\frac{94 - 201g(f)}{-20}} \right)$$

The two terms in the bracket take into account the effect from the module at the near end as well as the effect from the cable. ISO/IEC expressly states that these values should not be considered individual limit values. Overall limit value can also be achieved using cables of extremely high quality and modules of poorer quality, or by using modules of extremely high quality and cables of poorer quality.



Other formulas apply for the frequency range $300 \leq f \leq 500$ [MHz]. ISO/IEC calculates NEXT limit values [in dB] for the configuration PL2 as follows:

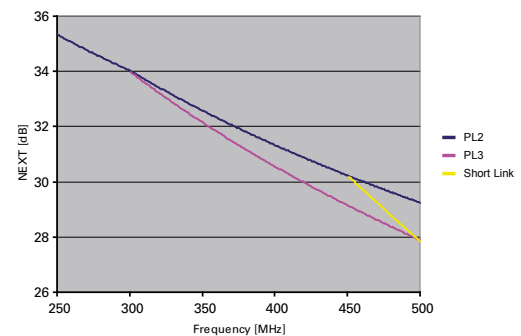
$$NEXT > 87,46 - 21,57lg(f) \quad (\text{Blue curve in graphic})$$

A more moderate requirement exists for configuration PL3, with its added consolidation point. The following formula applies in the frequency range $300 \leq f \leq 500$ [MHz] with the formula:

$$NEXT > 102,22 - 27,54lg(f) \quad (\text{Violet curve in graphic})$$

Eased requirements exist for configurations PL1, PL2 and CP1 starting from 450 MHz: If insertion loss (IL) at 450 MHz is less than 12 dB, the following value should be subtracted from the NEXT progression required by formula [2]:

$$NEXT = 1,4((f - 450)/50) \quad (\text{Yellow curve in graphic})$$



NEXT limit values for permanent link configurations 2 and 3 and for short links as defined under ISO/IEC 11801 Amendment 2.

Conclusion

Short links in structured cabling systems are not only possible, but recommended, through the use of high-quality Cat. 6_A components. Cat. 6_A modules and installation cables from R&M make it possible to implement short PLs of up to 2 m. This provides the following advantages:

- No unnecessary cable loops
- Easier installation
- Lower costs
- Significant material savings
- Better ventilation, lower energy consumption

The use of shorter PLs is permitted if the manufacturer guarantees they comply with PL requirements

3.10.5 Transmission Capacities of Class E_A and Class F_A Cabling

A migration path to 40 Gigabit Ethernet in data centers may also lead data center operators and planners over copper cabling. At a minimum the market is increasingly discussing implementing 40GBASE-T in connection with class F_A and Cat. 7_A. This handbook will therefore examine solutions other than just glass fiber. The following section examines what transmission capacities are possible using a high-performance class F_A copper infrastructure.

Starting Point

Transmission technologies these days are becoming higher performance and making better and better use of copper cabling. 10GBASE-T applications alone are approaching the theoretical transmission capacity of class E_A closer than any other application.

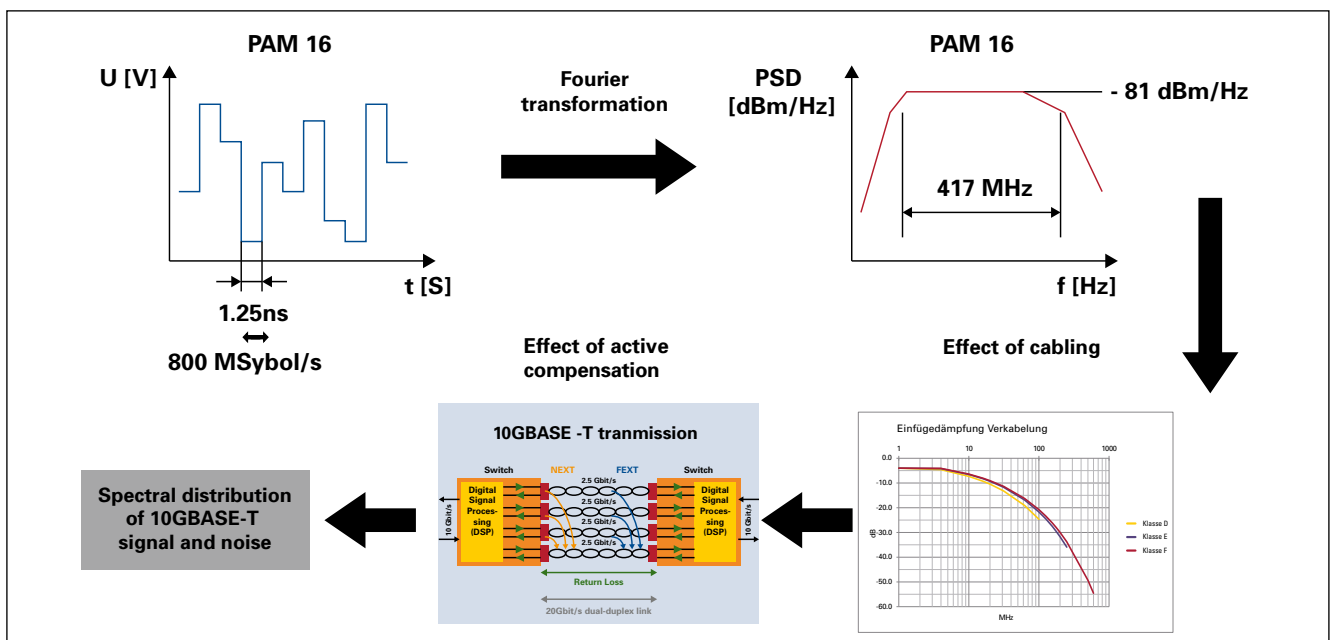
So that 10GBASE-T can run on a class E_A cabling system, an active noise suppression system must be installed for reflection and crosstalk. When the connection is being established, a known test signal is transmitted over the cabling and the effects on other pairs are stored. During operation, the stored disturbance signals are used as correction values in digital signal processing (DSP) and subtracted from the actual signal. The improvements that can be thus achieved are 55 dB for RL, 40 dB for NEXT and 25 dB for FEXT. DSP cannot be implemented between neighboring channels since no connection/synchronization exists there, so active compensation of the crosstalk from one channel to the next (alien crosstalk) is not possible.

10GBASE-T Signal and Noise Spectrum

The data stream in 10GBASE-T is split over the four pairs then modulated using a (pseudo) random code (Tomlinson-Harashima Pencoding/THP) to achieve an equivalent spectral power distribution regardless of the data.

A Fourier transformation can be used to calculate the power spectrum density (PSD) of the application, based on the PAM-16-like time domain signal. The IEEE has defined this spectral power distribution over the frequency in the standard. That is important in this connection, since all cabling parameters are specified as a function of frequency and their influence on the spectrum can therefore be calculated.

For example, the spectrum of the receiving signal can be calculated by subtracting attenuation from the transmission spectrum. The spectrum of different noise components can be found through subtraction of RL, NEXT, FEXT, ANEXT, AFEXT etc. parameters. If DSP also takes active noise suppression into account, actual conditions can be calculated from the signal and disturbance signal (noise) at the receiver. The following schematic diagram illustrates this relationships.

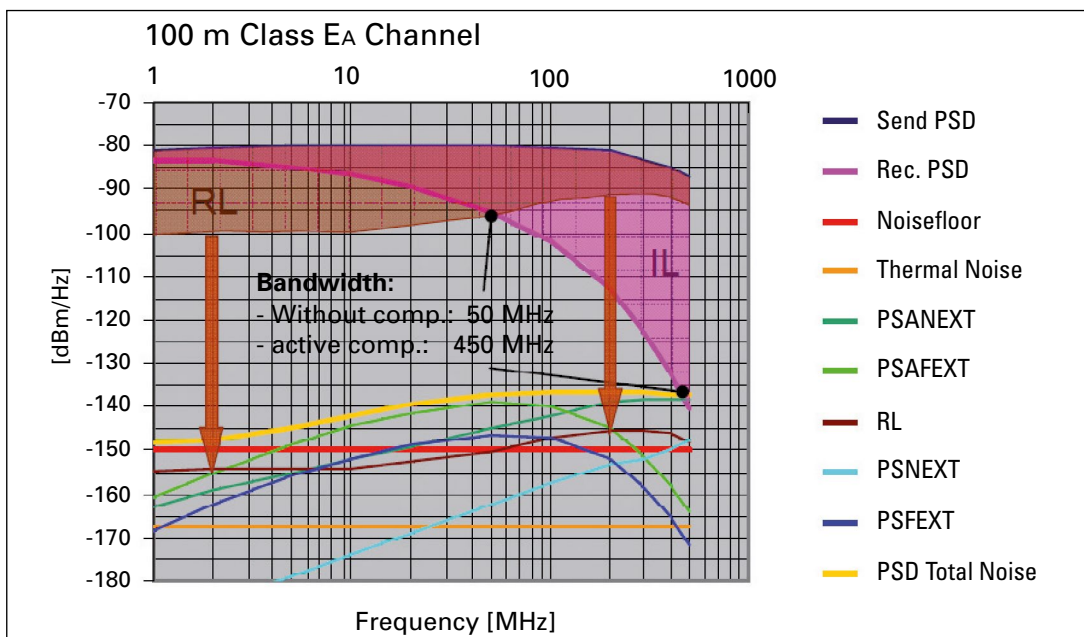


Theoretical process for determining spectral distribution of signal and noise

This method allows the relative values of signal and different sources of interference to be compared to one another.

The following graphic shows the signal spectrum, the noise spectrum total and the different noise components in an unshielded 100 m class E_A channel. This example uses IL and RL to show how cabling values are subtracted from the transmission spectrum and, in the case of RL, how the effects of active compensation are also taken into consideration.

The intersection between signal field strength and noise field strength is frequently used in cabling technology to define bandwidth. If active compensation is not used, return loss then becomes the parameter used to define noise power. This then results in a bandwidth of 50 MHz. Active return loss compensation is necessary just for 1 Gigabit Ethernet 1000BASE-T in order to ensure the 66 MHz bandwidth that technology requires. If the active compensations realized by 10GBASE-T are used as a basis, bandwidth improves to 450 MHz (see chart).



Comparison of spectral noise components

If the influence quantities of the different parameters defined for class E_A are compared with one another, it becomes apparent that alien crosstalk is the main contributor to noise. This means that the achievable bandwidth in a modern data transfer process that includes active compensation is limited by the alien crosstalk that cannot be compensated. An increase in bandwidth is then only possible by improving alien crosstalk (ANEXT/alien NEXT or AFEXT/alien FEXT).

Unshielded cabling meets its limits of acceptance in this regard. This is because this technology requires large cable diameters to fulfill specifications and to contain alien crosstalk. Large diameters then translate into larger and more expensive space requirements. It is therefore essential for data centers who want to increase bandwidth to change over to shielded systems. Alien crosstalk in shielded systems is so low that, for the time being, it no longer needs to be taken into account in our discussions.

In terms of noise that is caused internally, return loss (RL) contributes the highest percentage at 61%, followed by FEXT (27%) and NEXT (12%). Unfortunately, RL is a parameter that has already been exhausted is in use and not easily realizable for improvements. As a result, exactly the same RL must be accepted in class E_A and F_A, and the largest noise component cannot be improved by changing over from class E_A to F_A.

Transmission Capacity provided by Different Cabling Classes

C.E. Shannon was one of the scientists who developed mathematical principles for digital signal transmission back in the 1940s. The so-called Shannon capacity is a fundamental quantity in information theory that builds upon the laws of physics (entropy). It defines the maximum data rate that can be sent over a given transmission channel. The Shannon capacity cannot be exceeded through any technical means.

Maximum channel capacity according to Shannon can be calculated as follows: $KS = XT * B$

$$KS = B * \log_2 \left(1 + \frac{S}{N} \right) \text{ [Bit/s]}$$

Abbreviations:

KS = Channel capacity according to Shannon

XT = Channel-dependent factor (based on media, modulation method and other factors, moves between 0 & 1) B = bandwidth of signal used (3 dB points)


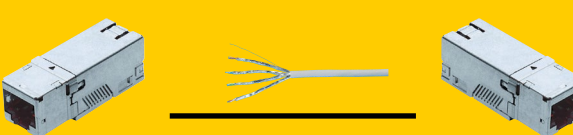
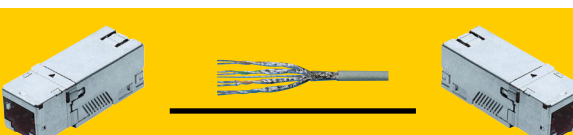
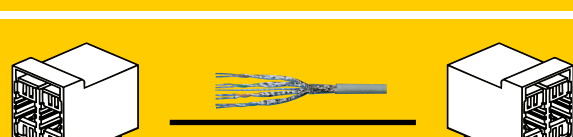
S = Signal power at receiver in W

N = Noise (interference) power at receiver in W

The higher the bandwidth of the signal used, the greater transmission power will be, and the smaller the interference power experienced, the higher the possible data transmission rate will be. The signal-noise ratio in this case cannot be improved by increasing transmission power if interference power, as is usual in cabling, results from transmission power in accordance with a fixed ratio, as in RL.

Signal power and noise power can now be calculated from the power density spectra of receiving signal and total noise. The integral of the area under the signal spectrum corresponds to the signal power S, and the area under the noise spectrum to interference power N. The quantities S and N can be used directly in Shannon's formula.

The method of calculating S and N on the basis of the power density spectrum provides a big advantage; individual cabling parameters can now be changed independently of one another in order to examine their effect on channel capacity. This allows the Shannon capacities of different cabling variants to be calculated.

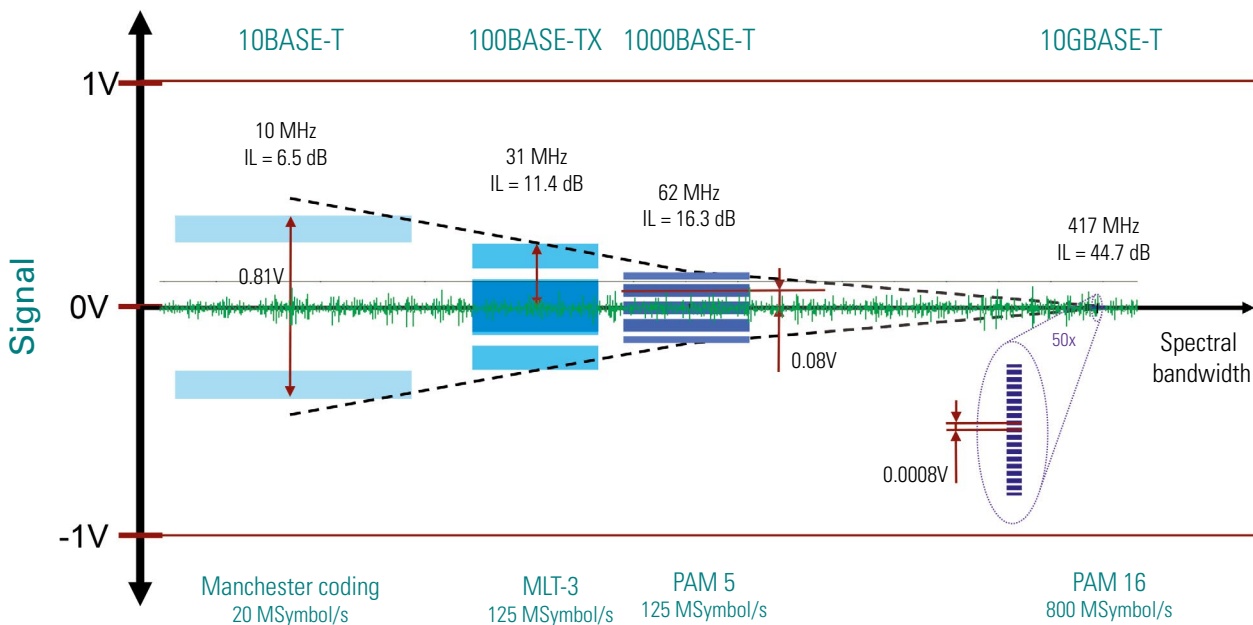
Shannon Capacity		Comparison in%	Shannon-Capacity
Module Cat. 6A/u Cable Cat. 6A/u		100% (ISO/IEC class EA)	21.7 Gbit/s
Module Cat. 6A/s Cable Cat. 6A/s		114%	24.8 Gbit/s
Module Cat. 6A/s Cable Cat. 7A/s		119%	25.8 Gbit/s
Module Cat. 7A/s Cable Cat. 7A/s		120% (ISO/IEC class FA)	26.0 Gbit/s

Comparison of Shannon capacities of different cabling channels at 400 MHz

3.10.6 EMC Behavior in Shielded and Unshielded Cabling Systems

Because network technology is pushing forward into totally new, much more sophisticated dimensions, data center planners and operators who wish to implement 10 Gigabit Ethernet over copper cabling must now devote more attention than ever before to the issue of shielding. The following section takes a look at the EMC behavior of shielded and unshielded cabling systems and shows why the new 10GBASE-T technology requires special protection.

We must first show that how the use of higher and higher modulation levels makes the new protocols susceptible to external interferences. It is remarkable to note that the symbol distance of 10GBASE-T is approximately 100 times smaller than that of 1000BASE-T (see graphic below).



Comparison of signal strength at receiver for different Ethernet protocols

The graphic shows the ratios of signal field strengths at the receiver for different protocols after the signal was sent through 100 m Class E_A cabling. Basically, the higher the frequency or bandwidth of the signal, the greater the attenuation that will result through cabling.

For reasons of EMC, the output signal level cannot be increased over +/- 1 V. Depending on cable attenuation and frequency, a smaller and smaller portion of the signal reaches the receiver from this 2 V span. In addition, the voltage differences from one symbol to the next become smaller and smaller due to the higher modulation. While in the past the symbol distance at the receiver decreased by an approximate factor of 3 per level as technology grew from 1 M to 100 M to 1 G, this distance dropped by a factor of 100 over the last stage in the development, from 1 G to 10 G.

If some noise is added to the symbolization, it immediately becomes obvious that sensitivity to interferences is massively increasing with the faster data transmission protocols. As a result, susceptibility to interference in the area of EMC becomes higher as the data transmission rate increases.

In the middle of 2008, a number of cabling providers, including R&M, got together to compare EMC behavior of different cabling variants on a neutral basis. In order to ensure the independence and objectivity of result, these providers hired an independent external laboratory for the study – the *Gesellschaft für Hochfrequenz Messtechnik* (GHMT) society for high-frequency measurement technology based in Bexbach, Germany. The study attempted to answer the following questions with regard to selecting a cabling system:

- What parameters for shielded and unshielded cabling systems can be provided to meaningfully assess EMC behavior?
- What special measures are required in using shielded or unshielded cabling to ensure operations will conform to standards and legal regulations?
- What should emerge from the comparison of the EMC behavior of shielded and unshielded cabling systems when running 1G and 10GBASE-T?

The study did not involve playing shielded and unshielded systems against one another. It was intended instead to show the basic conditions required for trouble-free, legally compliant operation of 10GBASE-T. This should then give planners and users a useful guide in for avoiding confusion and uncertainty when selecting cabling systems.

Though the results themselves are exclusively from the independent EMC study carried out by GHMT, the interpretations and conclusions drawn from the results are based on R&M analyses.

Test Objects and Testing Setup

The test plan was to examine 6 cabling systems:

- 1 x unshielded Cat. 6
- 2 x unshielded Cat. 6_A
- 3 x shielded Cat. 6_A with pair shielding (foil) and different degrees of GS braided shield coverage (U-FTP without GS, S-STP "light" with moderate GS, S-STP with quality GS)

The table shows the results of preliminary measurements in accordance with ISO 11801 (2008-04), provided as reserves to the class E_A limits. Coupling attenuation is specified as an absolute value.

	System 00		System 01		System 02		System 03		System 04		System 05	
Type	U/UTP Legacy Cat6		U/UTP Cat6A		U/UTP Cat6A		F/UTP Cat6A		S/FTP Cat6A		S/FTP Top Cat6A	
Channel	long	short	long	short	long	short	long	short	long	short	long	short
Insertion loss (margin) [dB]	8.4	34.4	8.8	35.4	8.6	35.3	8.6	35.5	10.5	34.9	15.5	36.5
NEXT (margin) [dB]	1.1	1.2	4.2	4.2	6.2	7.4	7.3	7.5	5.6	4.6	5.0	5.4
PS NEXT (margin) [dB]	3.2	3.8	5.5	5.3	8.2	8.0	7.8	7.6	5.8	4.8	6.2	6.0
TCL (margin) [dB]	6.4		9.2		8.9		9.6		5.45		10.4	
RL (margin) [dB]	4.3	6.6	8.8	8.1	9.5	8.5	3.4	3.0	6.9	9.4	8.2	7.2
PS ANEXT (margin) [dB]	-17.7		-7.6		0.93		27.44		31.37		37.92	
Coupling Attenuation [dB] to 500 (1000) MHz	21.5 (21.5)		45.0 (33.5)		47.5 (42.0)		78.0 (69.0)		76.0 (71.0)		79.0 (79.0)	

ISO/IEC 11801 cabling parameters (2008-04)

Surprisingly, transmission parameters (IL, NEXT, PSNEXT TCL and RL) for Cat. 6_A-UTP cabling systems were at a similar level to those of shielded systems. Apart from the older Cat. 6 system, these values are more or less comparable with one another. It was notable that shielded systems just barely reached PSANEXT requirements, and in some cases not at all. As soon as shielding is provided, ANEXT values are improved by about 30-40 dB to the extent that they no longer represent a problem.

The systems differ significantly with regard to the EMC parameter of coupling attenuation. The Cat. 6 system is far off from required values, while the newer UTP systems do comply with requirements. Here as well, a clear difference between shielded and unshielded cabling systems is obvious.

TCL is used in international standardization for unshielded systems as an EMC parameter in place of the coupling attenuation used for shielded systems. However, a comparison of TCL and coupling attenuation values in systems 0–2 puts this practice in question. The relative small difference in TCL between systems 0 and 1 and 0 and 2 contrasts with a huge difference in coupling attenuation between the same systems (pass with TCL, fail with coupling attenuation).

Due to poor result, no further measurements were carried out for system 0 after that point.

Cabling systems undergoing EMC tests cannot be examined on their own, but must be tested as an overall system that includes active components. The following active components were used in the GHMT test:

- Switch: Extreme Networks; Summit X450a-24t (Slot: XGM2-2bt)
- Server: IBM; X3550 (INTEL 10Gigabit AT Server Adapter)

The two servers, which generated data traffic of 10 Gbit/s, were connected together over cabling via a switch. A diagram of the test setup is presented below:

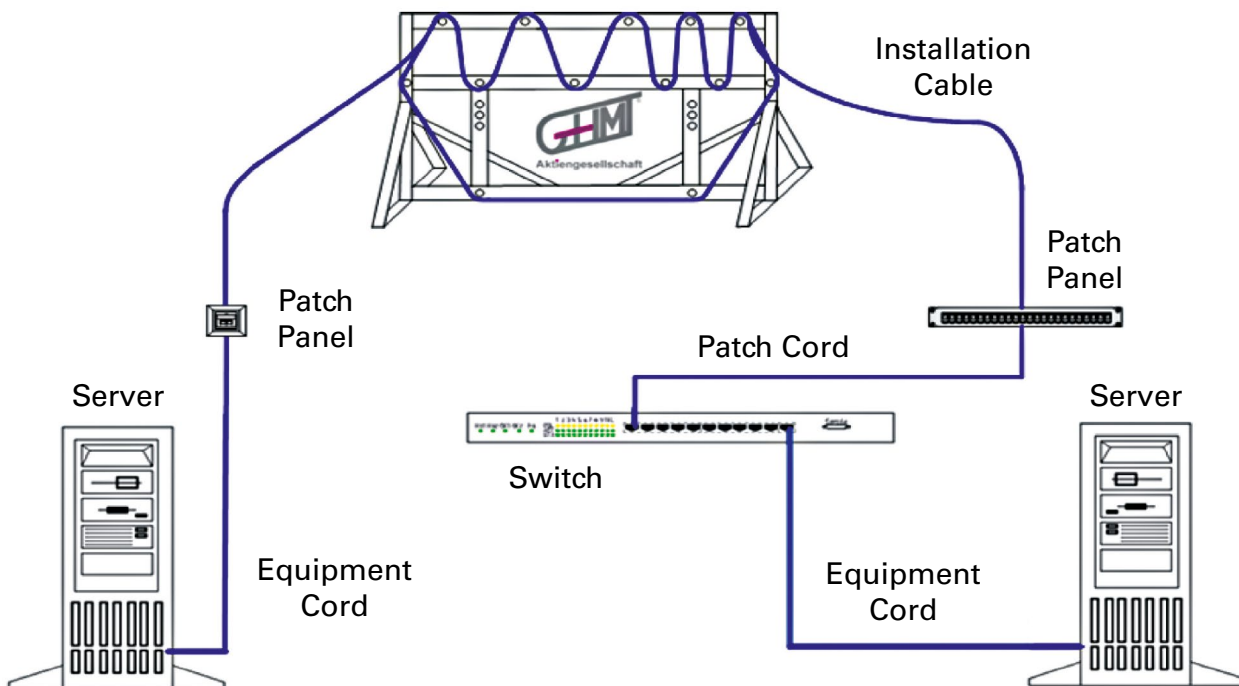


Diagram of test setup

In order to be able to examine EMC properties from all side, all data transmission components for the test were installed on a turntable (d = 2.5 m) in an anechoic EMC measurement chamber. An anechoic EMC measurement chamber is a room whose electrical and acoustic reflections are prevented by means of an absorbent wall coating, and which is shielded off from external influences. A 19" cabinet with servers and switches is placed in the center of the turntable, each with an open 19" cabinet with cabling panels on both sides. 2 m patch cords are used for the connections between the panels and active components.

Each 90 m section of the different installation cables was set up on one of the RJ45 panels at both ends. In order to achieve a high degree of reproducibility and obtain a well-examined test setup, the cables were pulled tight on a wooden cabling routing framework, which was the test setup recommended by CENELEC TC 46X WG3. This frame was positioned behind the 19" cabinets.

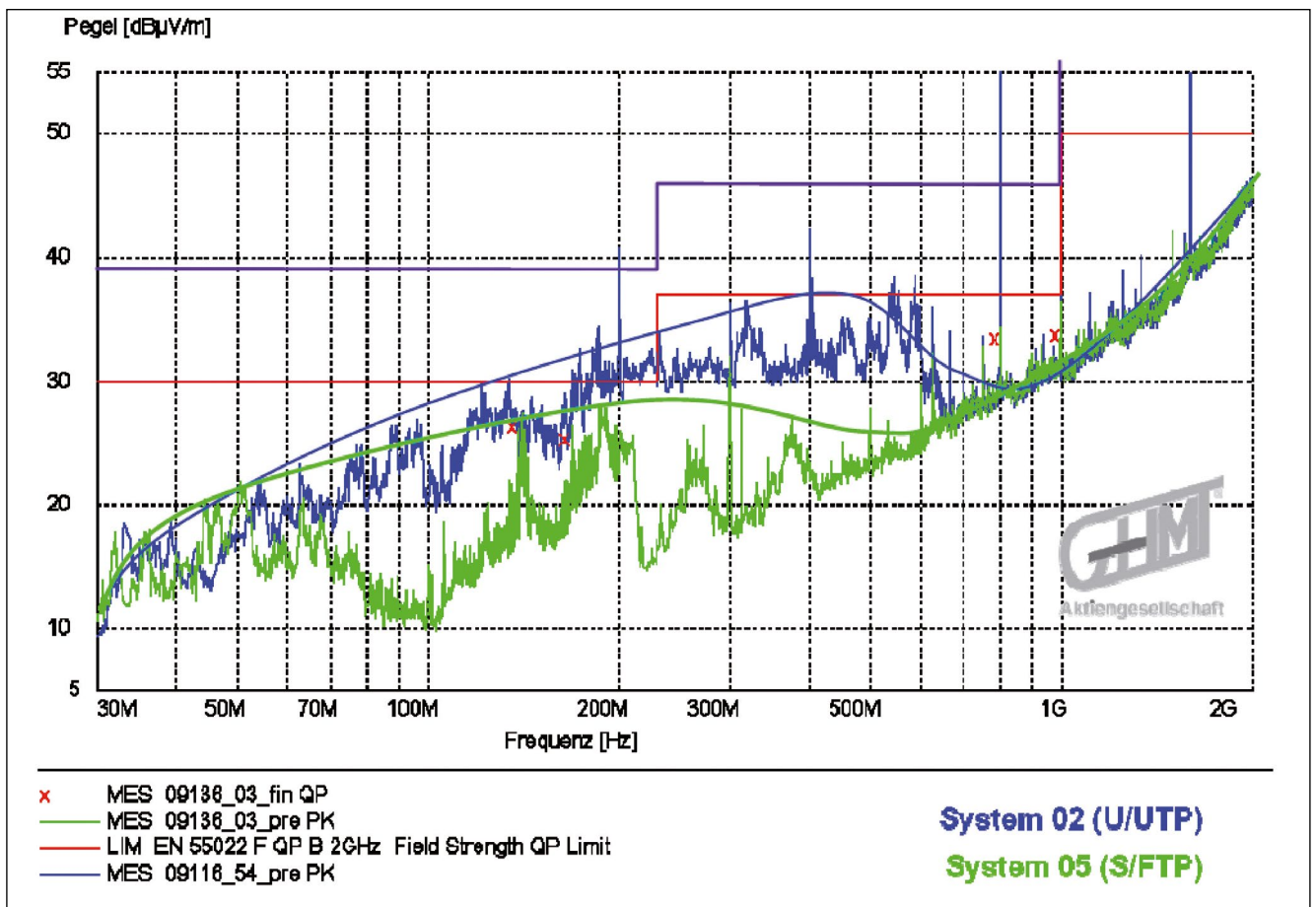
This system setup was intended to simulate the situation in an actual data center.

Radiated Power in Accordance with EN 55022

This test is prescribed in the EU's guideline on EMC, and is therefore required under law. Devices and systems which do not pass this test are prohibited in the EU.

The test is designed to identify interference emissions that may interfere with operation of the receiving devices used by radios, televisions and telecommunication installations.

The receiving antenna of the measurement system in mounted at a distance of 3 m from the test object. The power radiated in horizontal and vertical polarization is recorded. Two limit values exist for this test: Class A (for work environments) with somewhat stricter requirements and class B (for residential areas) with corresponding higher requirements.



Emission measurement for a typical unshielded system and shielded system. Limit values: Red = class B, violet = class A.

The graphic shows an example of emission measurements of systems 2 & 5 given a 10GBASE-T transfer. It is obvious that the unshielded system exceeds class B limit values many times over, while the shielded system provides better protection, primarily in the high frequency range, and thus fulfills requirements. It is irrelevant here whether the shielded cabling system was earthed on one or both sides.

Since 10GBASE-T uses a frequency range of at least 400 MHz for data transmission, we can assume that no improvements can be achieved for unshielded systems, even if filtering measures are used. By contrast, both cabling types were able to maintain class A limit values.

Other measurements have shown that both shielded as well as unshielded cabling systems for 1000BASE-T have the ability to maintain the limit values for class B.

We may therefore conclude that unshielded cabling systems should not be used with 10GBASE-T in private homes, at least in the EU. In work environments, including data centers, an unshielded cabling system may be used with 10GBASE-T as well.

Immunity to External Interferences

EMC immunity tests are based on the testing standards in the EN 61000-4-X series, and were carried out using E1/E2/E3 stresses as defined under the MICE table for environmental stresses in accordance with EN 50173-1 (see table below). A protocol analyzer monitored a continuous data transmission between servers for the purpose of these tests. The transmission system was observed under defined test loads. Tester noted the times at which these test loads began to affect the data transmission rate.

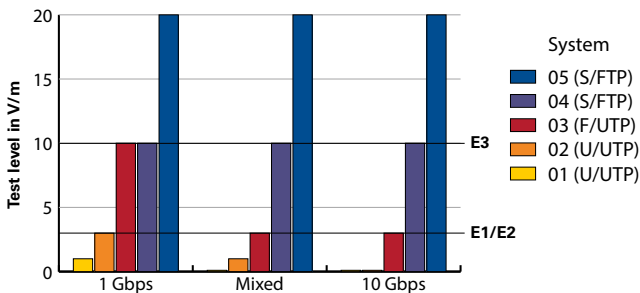
	E1	E2	E3
Electrostatic discharge-contact (0.667) µC	4 kV	4 kV	4 kV
Electrostatic discharge-contact (0.132) µC	8 kV	8 kV	8 kV
Radiated high frequency, amplitude-modulated	3 V/m at 80 - 1,000MHz 3 V/m at 1,400 - 2,000MHz 3 V/m at 2,000 - 2,700MHz	3 V/m at 80 - 1,000MHz 3 V/m at 1,400 - 2,000MHz 3 V/m at 2,000 - 2,700MHz	3 V/m at 80 - 1,000MHz 3 V/m at 1,400 - 2,000MHz 3 V/m at 2,000 - 2,700MHz
Conducted high frequency	3 V at 150kHz - 80 MHz	3 V at 150kHz - 80 MHz	10 V at 150kHz - 80 MHz
Fast transient (burst)	500 VAC	1,000 VAC	2,000 VAC
Surge voltage (transient, earth potential difference)-signal line / earth	500 V	1,000 V	2,000 V
Magnetic field (50/60Hz)	1 A/m	3 A/m	30 A/m
Magnetic field (60Hz to 20,000Hz)	f.f.s.	f.f.s.	f.f.s.

Class E1 to E3 stresses in accordance with EN 50173-1 MICE table (MICE: Mechanical Ingress Climatic Electromagnetic)

Immunity to High-Frequency Radio Waves

The test defined by EN 61000-4-3 is used to check the test object's immunity to electromagnetic fields that are emitted in the frequency range from 80 MHz to 2.0 GHz. This test simulates the effect of sources of interferences like radio and TV transmitters, radio equipment, mobile phones, wireless networks, etc.

The transmitting antenna was set up at a distance of 3 m from the test object. The test object was exposed to radio waves from all four sides. Stress levels, measured at the site of the test object, were selected in accordance with the MICE table (see above table). The results:



Results in accordance with EN 61000-4-3



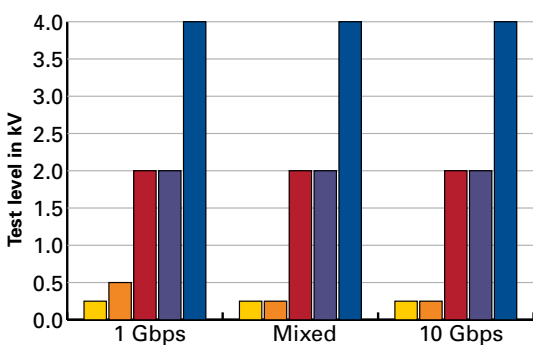
Practice test with mobile phone

All shielded cabling systems proved to be suitable for 10GBASE-T operation in the office and in light industrial areas. An additional braided shield (S-FTP construction) is required for heavier industrial areas. Single-sided or double-sided earthing has no effect on immunity to external irradiation. Well-shielded cabling systems are suitable for 1000BASE-T in the office environment and in light industrial areas. However, additional protective measures such as metal cable routing systems as well as increased distances from sources of interference are required for unshielded cabling systems for use with 10GBASE-T.

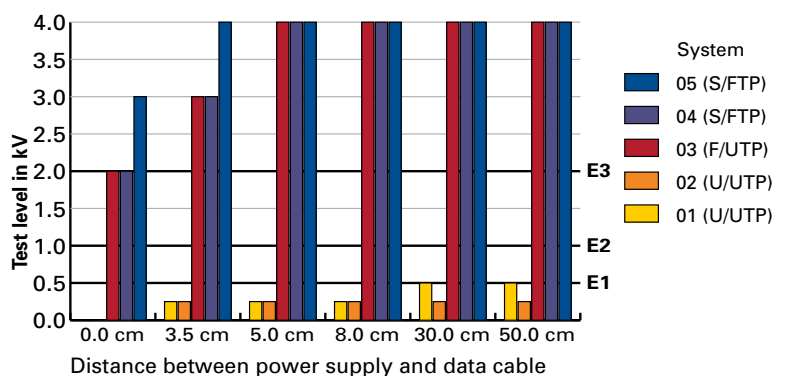
An additional practical test also confirms the sensitivity of unshielded systems to wireless communication devices in the 2 m to 70-cm band when using 10GBASE-T. When a radio unit or mobile phone was used at a distance of 3 m from unshielded cabling systems, this led to an interruption in the data transmission, while none of the shielded systems showed a loss in transmission.

Immunity to Interferences from Power Supply Cables

An additional test was carried out in accordance with EN 61000-4-4 in order to test the immunity of the test object to repeated fast transients. Transients can be caused by switching operations involving inductive loads (engines), switching confusion and ballasts for fluorescent lamps. In order to obtain a reproducible coupling between the power cable and the test object, a normalized, capacitive coupling clamp was used for this test. Interferences included voltage peaks of 260 to 4000 V with a wave form of 5/50 ns and an interval of 0.2 ms. The voltage sizes were designed in accordance with the MICE table (fast transient [burst]).



Results in accordance with EN 61000-4-4



Results of practice test with mesh cable tray

The graphics above show the results of this test. All shielded systems allowed the use of 10GBASE-T in all environmental ranges (E1, E2, E3). Better shielding quality results in improved immunity against fast transients. An unshielded cabling system of good quality allows the use of 1000BASE-T in the office environment. A shielded cabling system is necessary for an industrial environment and for 10GBASE-T. Unshielded cabling systems that want to support 10GBASE-T require additional measures, such as carefully separating data cables from power cables.

Double-sided earthing improves the immunity of a shielded cabling system to fast transients from external sources, beyond minimum standard requirements. If shielding is not applied to the cabling system consistently, its effectiveness is canceled out when 10GBASE-T is used. Protection in this case is exactly as low as that in an unshielded cabling system. Non-continuous shielding still does show a certain protective effect at lower frequencies (as those in 1000BASE-T), especially when double-sided earthing is implemented.

A practical test using fluorescent tubes (set up at a distance of 0.5 m from data cabling) confirmed that the test conditions in the standard test were realistic throughout. The interferences that arose when the fluorescent lamp was turned on affected the 10GBASE-T data transmission in the same way as in the standard test. Both the lamps themselves as well as their electrical power supply lines caused interference. As a result, the distance of data cabling to both components must be considered.

In order to obtain a comparison between the normalized test with the coupling clamp and an actual installation situation, an experiment was also carried out using a mesh cable tray. Data cables and a power supply cable with a different constant distance of 0 to 50 cm were mounted in the channel in a mesh cable tray with a total length of 30 m. The interference signal defined by the standard was then applied to the power supply cable. The graphic above (right) shows the results of these measurements.

Comparison of these measurements with those of the standard test (left graphic) shows that the standard test simulated a cable distance of approximately 1–2 cm. In order to ensure 10GBASE-T operation, unshielded systems must maintain a minimum distance of 30 cm between data cables and power supply cables. Shielded cabling systems meet requirements even when these cables are not separated.

EN 50174-2 would prescribe a distance of only 2 cm for the unshielded system in this arrangement, but this would not be sufficient for 10GBASE-T. Distances that are much greater than those prescribed by the standard must therefore be maintained by unshielded cabling systems that want to support 10GBASE-T.

An additional test was carried out in accordance with EN 61000-4-6 to test system immunity to conductive radio frequency interferences in the 150 kHz to 80 MHz range over power supply lines in the vicinity. Power supply cables can be used as antennas for HF interferences from external sources (such as short-wave transmitters, VHF transmitting stations), or even be intentionally applied by means of a power line signal. A capacitive coupling clamp was used for this test as well. Stresses were specified in accordance with the MICE table (conducted high frequency).

The results corresponded to the common pattern that shielded cabling systems fulfill all requirements for 10GBASE-T. Unshielded cabling systems fulfill office and light industrial environment requirements for 1000BASE-T, but additional protective measures such as increased distance between data cabling and the power supply are required for 10GBASE-T transmission.

Immunity to Magnetic Fields from Power Supply Lines

The test as defined under EN 61000-4-8 checks the ability of a system to function in the presence of strong magnetic fields at 50 Hz. These magnetic fields may be generated by power supply lines (cables or power distribution rails) or power distribution equipment (transformers, power distributors). Stress values were selected in accordance with the MICE tables.

The results: All cabling systems fulfill the highest environmental class E3 with both 1000BASE-T as well as 10GBASE-T. No difference was determined between the sensitivity of shielded cabling systems and that of unshielded systems. Increased sensitivity of shielded cabling systems due to earthing loops is indiscernible.

Immunity to Electrostatic Discharges

The test defined under EN 61000-4-2 tests the immunity of a system to electrostatic discharges. The common everyday occurrence in which an electrical discharge jumps from your finger to a conductive surface can be reproduced using a testing device that includes a metal test finger. Ambient and climatic conditions, such as low humidity, floors insulated with plastic, and clothing with synthetic fibers, can increase this electrical charge. Test items were selected so as to simulate cabling contact through normal operation and maintenance. 10 flashovers for each polarity were generated for each test item, at intervals of greater than a second. Test quantities in accordance with the MICE table (electrostatic discharge - contact/air) were used.

Shielded cabling systems did not react sensitively to electrostatic discharges. No interferences occurred. Active components in unshielded cabling systems reacted very sensitively to discharges as soon as these could take effect on the signal conductor. The good discharging qualities of the shielded cabling system can be explained by the shield acting as a discharge pad for the flashover so no energy penetrates inside the cable. Electrostatic discharges must be prevented for 10GBASE-T operated using unshielded cabling systems. Suitable cabling measures that are common in the electronics manufacturing industry should be used: Discharge stations, ESD armbands, anti-static floors, etc.

Summary

It has been shown that implementing 10GBASE-T actually has a significant effect on selection of a cabling system. The increased sensitivity of the 10GBASE-T transmission was clearly noticeable with unshielded cabling systems. Other issues in addition to cabling must be taken into consideration in order to ensure 10GBASE-T operation. Ambient conditions must be considered, and cabling components selected appropriately. Coupling attenuation can serve as a qualitative comparison parameter in this area for the EMC behavior of cabling systems.

To sum, this study showed that 10GBASE-T can be used with a shielded cabling system without a problem in all environmental classes. In this scenario, the better the shielding quality, the smaller irradiation will be and the better immunity the cabling system will have to interferences. By contrast, unshielded cabling systems are suitable for 10GBASE-T use only if additional protective measures are implemented. In the EU, they may only be used outside of private residential areas, in dedicated work environments (offices, data centers). The effects and expenses resulting from additional protective measures as well as relevant operational limitations must be taken into account in any decision between shielded and unshielded cabling for 10GBASE-T.

Recommendations for use of 10GBASE-T

	Home Environment	Office Environment and Data Centers	Industry	Heavy Industry
Shielded cabling	Well-suited	Well-suited	Recommended	Recommended ¹
Unshielded cabling	Not suitable	Not suitable ²	Not recommended	Not recommended

¹ S/FTP cables and earthing on panel and socket side

² - Laid in metal cable ducts
 - Distance to power cables < 30 cm
 - No radio equipment allowed in vicinity
 - ESD protection installed

4. Appendix

References

This handbook is based on R&M's own research, experiences and specialized knowledge. Various encyclopedias, studies, guides, technical journals and technical articles were also consulted in order to verify and support information. Some of the most essential sources include:

BFE	<ul style="list-style-type: none"> Energy-efficient data centers through sensitization via transparent cost accounting
BITKOM	<ul style="list-style-type: none"> Operationally reliable data centers Compliance in IT outsourcing projects Energy efficiency in data centers IT Security Compass Liability Risk Matrix Planning Guide for Operationally Reliable Data Centers Certification of Information Security in the Enterprise
CA	<ul style="list-style-type: none"> The Avoidable Cost of Downtime
COSO	<ul style="list-style-type: none"> Internal Monitoring of Financial Reporting – Manual for Smaller Corporations – Volume I Summary
IT Governance Institute	<ul style="list-style-type: none"> Cobit 4.1
R&M	<ul style="list-style-type: none"> Contents from various white papers published from 2009 to 2012 - see www.rdm.com
Symantec	<ul style="list-style-type: none"> IT Risk Management Report 2: Myths and Realities
UBA	<ul style="list-style-type: none"> Material Stock of Data Centers in Germany Future Market for Energy-Efficient Data Centers
Wikipedia	<ul style="list-style-type: none"> Entries on relevant IT themes

Specifications from manufacturers including IBM, HP, CISCO, DELL, I.T.E.N.O.S., SonicWall and many others were also used

Standards

- ANSI/TIA-942-A Telecommunication Standard for Data Centers
- ANSI/TIA-942-1, Data Center Coaxial Cabling Specification and Application Distances
- ANSI/TIA-942-2 Telecommunication Standard for Data Centers Addendum 2 – Additional Guidelines for Data Centers
- ANSI/TIA-562-B.2 & -B.3 LC Connectors
- ANSI/TIA-568-C.0 Generic Telecommunication Cabling for Customer Premises
- ANSI/TIA-568-C.1 Commercial Building Telecommunication Cabling Standard
- ANSI/TIA-568-C.2 Balanced Twisted-Pair Telecommunication Cabling and Components Standard
- ANSI/TIA-568-C.2 Optical Fiber Cabling and Components Standard
- ANSI/TIA-604-5 MPO Connectors & ANSI/TIA-604-10 LC Connectors
- ANSI/TIA/EIA-606-A & -B Administration Standard for Commercial Telecommunications Infrastructure
- ANSI/EIA/TIA-607-A & -B Grounding and Bonding Requirements for Telecommunications
- ANSI/TIA 569-B & -C Commercial Building Standard for Telecommunications Pathways and Spaces
- EN 50310 Application of equipotential bonding and earthing in buildings with information technology equipment
- EN 50173-1 + EN 50173-1/A1 (2009 Information technology – Generic cabling systems – Part 1: General requirements
- EN 50173-2 + EN 50173-2/A1 Information technology – Generic cabling systems – Part 2: Office premises
- EN 50173-5 + EN 50173-5/A1 Information technology – Generic cabling systems – Part 5: Data centers
- EN 50174-1 Information technology – Cabling installation – Part 1: Specification and quality assurance
- EN 50174-2 Information technology – Cabling installation – Part 2: Installation planning and practices inside buildings
- EN 50346 +A1 +A2 Information technology – Cabling installation – Testing of installed cabling
- EN50600-1 Information technology - Data center facilities and infrastructures - Part 1: General concepts
- IEEE 802.3 Section Four
- IEEE 802.1aq, IEEE 802.1ax, IEEE 802.1d, IEEE 802.1Qau, IEEE 802.1Qaz, IEEE 802.Qbb, IEEE 802.1w
- IEEE 802.3 Section Two, IEEE 802.3 Section Three, IEEE 802.3 Section Four, IEEE 802.3 Section Six
- ISO/IEC 11801 2nd Edition Amendment 1 (04/2008) + Amendment 2 (02/2010) Information technology – Generic cabling for customer premises
- ISO/IEC 24764 Information technology – Generic cabling systems for data centers
- ISO/IEC 14763-1 AMD 1 Information technology – Implementation and operation of customer premises cabling – Part 1: Administration; Amendment 1
- ISO/IEC 14763-2 Information technology – Implementation and operation of customer premises cabling – Part 2: Planning and installation
- ISO/IEC 14763-3 Information technology – Implementation and operation of customer premises cabling – Part 3: Testing of optical fiber cabling (ISO/IEC 14763-3:2006 + A1:2009)
- ISO/IEC 18010 Information technology – Pathways and spaces for customer premises cabling
- ISO/IEC 61935-1 Specification for the testing of balanced and coaxial information technology cabling – Part 1: Installed balanced cabling as specified in EN 50173 standards (IEC 61935-1:2009, modified); German version EN 61935-1:2009

You can find additional information on R&M products and solutions on our website: www.rdm.com

www.datacenter.rdm.com

Headquarters

Reichle & De-Massari AG
Binzstrasse 32
CHE-8620 Wetzikon/Switzerland
Phone +41 (0)44 933 81 11
Fax +41 (0)44 930 49 41

www.rdm.com

Your local R&M partners

Australia
Austria
Bulgaria
China
Czech Republic
Denmark
Egypt
Finland
France
Germany
Great Britain
Hungary
India
Italy
Japan
Jordan
Kingdom of Saudia Arabia
Netherlands
Norway
Poland
Portugal
Romania
Russia
Singapore
Slovakia
Slovenia
Spain
Sweden
Switzerland
South Korea
Thailand
Turkey
United Arab Emirates