White Paper

10 Steps Towards An Optimal IT Infrastructure

R&M
Convincing cabling solutions

RITTAL

Convincing cabling solutions

Content

Executive Summary

This white paper leads in ten steps through the complete range of the physical infrastructure of data centers and offers a guideline how to select the optimal system components. Customer requirements are the basis for all questions for the definition of essential system components and selection criteria.

Network and server racks will be described in detail; special attention will be paid to all topics related to power protection and a dedicated climate approach. In addition, security aspects will be discussed including the monitoring and evaluation of all relevant data of the IT infrastructure which will be reported via the Data Center Infrastructure Management software (DCIM) on a central dashboard.

Data center cabling will be examined in step-by-step detail; special attention will be on structured planning and best practice approaches. In a major share of installations, management and inventory of the physical infrastructure is done with “on-board” tools by using Excel tables and Visio shapes; hence solutions for Automated Infrastructure Management (AIM) will be explained, enabling an on-demand visualization of the entire infrastructure.

Traffic Access Points will be shown as a critical system for network monitoring, explaining how a tapped network environment should be built.

Finally, service aspects within the system context of the complete solution will be investigated.

Introduction

An essential task of a data center administrator is the planning of the IT infrastructure depending on the actual and future requirements of their end customer. The question of level of availability and the redundancy concept to be implemented is crucial for the architecture of the data center.

A guideline has been given with the Tier Definition [

Ref. 1] provided by the Uptime Institute. A corresponding approach has been published by the German BSI with the so called “Availability Classes” [Ref. 2, Ref. 3]. Based on the redundancy concept - e.g. modular n+1 or independent 2n redundancy -, the critical supply chains for power and cooling have to be planned. It may start with two complete independent power-in feeds on customer premises and could end with separate A- and B-power lines at rack level.

A second and important aspect is the dimensioning and usage of the IT racks. A server rack features different requirements compared to a network enclosure. In that context, the planned and future installation of active components (server, storage, switches) has to be taken into account. All active components within a given rack define the electrical power consumption, and which climate concept has to be chosen in order to eliminate the waste heat.

In addition, the intended use of IT racks for the required cabling has to be defined. Consultants and data center operators have to structure the network cabling carefully and in a forward looking manner. The passive network infrastructure is also part of the Tier categorization and has to fulfill the typical audit and compliance requirements in accordance to the respective technical regulations. Especially the following references are relevant: Sarbanes-Oxley Act (SOX) [Ref. 1Ref. 4], Basel II [Ref. 5], HIPAA [Ref. 6] or PCI DSS [Ref. 7].

A corresponding documentation system for administration of the cabling infrastructure supports the safe and secure planning of changes or extensions, and a smooth audit. Such documentation could be created and maintained by various tools – from individual Excel lists to comfortable, fully developed documentation tools, indeed a complete AIM system. In the end it is crucial that the entire documentation is constantly up-to-date and corresponds to the reality of the installed cabling.

The detailed analysis of all security aspects is part of the essential requirements of a planned data center. It may start with the supervision of the building, the data center hall, down to rack level and covers also aspects of physical security, e.g. intrusion protection, resistance against fire, water, smoke, falling debris, to report only a few of them.

Under operation all parts of the physical infrastructure of a data center have to be monitored continuously. All relevant information must be collected, processed and reported on the dash board of the system administrator. By representing the hierarchical architecture of a data center all sensors – e.g. temperature, humidity, leakage, smoke can be assigned to a dedicated rack.

Against this background, IT infrastructure management software needs to meet the many and varied needs of IT administrators. It must be able to monitor all infrastructure components and to take corrective action, where necessary. A network of distributed sensors enables all relevant parameters and alarms to be captured, documented, and visualized in an easy-to-understand way.

Ideally, software of this kind offers IT administrators a complete picture of the data center as a single entity also for maintenance and service aspects. A guidance is given by the „de-facto standard“ ITIL [Ref. 8, Ref. 9], a collection of best practices for the IT Management of data centers.

The on-going transformation of data center networks towards cloud solutions is realized via increasing bandwidths on switch and router ports, accompanied by the virtualization of networks, server, and storage. The transformation facilitates defined and scalable systems for IT organizations enabling a smooth and consistent enhancement for future needs. While cloud technology and “software-defined-everything” dissolve the traditional concepts of individual network components and their related management, the effort to measure and control the application traffic and “End-User Experience” will increase continuously. In order to gain a holistic view of the logical network Traffic Access Point (TAPs) are a suited solution. Hence, this white paper also touches on the subject of TAPs – components with passive splitters -, splitting the optical signal for the sake of measurements and monitoring.

Step 1: Rack

In a server room or in a data center racks will be used according to the internationally standardized 19-inch format [Ref. 10]. The front panels of the racks are multiples of one height unit (U), equivalent to 1.75 inches. These enclosures have the task of stacking the built-in hardware in a mechanically secure way, of accommodating the cables needed for guiding the power and data in and out, of allowing sufficient air exchange for cooling, as well as protecting access to the front and back and only allowing access to authorized personnel. Depending on the purpose of the application, the interior installation differs drastically from that seen in the IT world.

Figure 1: Rittal TS IT Rack for server and network applications

Within the Rittal TS IT rack platform (Figure 1) two different options are available for the 19'' technology. The TS IT equipped with standard 19'' technology is approved for a total load of 1,500 kg without any additional screw joints. This is made possible by the depth stays that transmit the load to the TS frame.

As an alternative welded 19-inch mounting frames are available - which offer a higher flexibility in cabling inside the rack due to the fact that no depth stays are used. Based on the mounting frames, the TS IT is approved for a total load of 1,000 kg without any additional screw joints. The 19-inch mounting frame is based on the same 19-inch mounting angles and ensures a maximum compatibility for all accessories of the TS IT portfolio.

In both versions, a consistent, tool-free assembly concept has been implemented. In the TS IT, the quick-release fasteners with snap-in technology save time during assembly and make subsequent conversion easier. This also applies for accessory components. For instance, the intelligent power strip (PDU) from Rittal can be mounted quickly and easily in the zero-U space of the rack by means of quick-release fasteners. For added safety, the tool-free installation accessories (cable duct, air baffle plate, cable route and floor holder) can also be screwed tight as an option. Without any tools, the slide rails, component shelves, telescopic slides and more are snapped into the rear sections and are hooked into the front sections.

In addition, pre-configured racks, empty enclosures for individual specific assembly, and racks with a high protection level for usage in harsh environments are offered. Even if current standard server enclosures are characterized by the 19" form factor for rack-mounted devices, rack dimensions are certainly not rigidly specified. Enclosures are always specified by outer width and outer depth. Only the installation height is stated in U. A typical enclosure, for example, would be 42 U, 600 × 800 mm. This means that the enclosure has a useful grid of 42 U, and on the other hand an outer width of 600 mm and an outer depth of 800 mm. If network components in particular need to be installed, depths of 600, 800 or 1000 mm are typically called for with widths of 800 mm. If mainly servers are used, widths of 600 and 800 mm and depths of 800, 1000 and 1200 mm are needed.

Step 2: Power Protection

The power supply chain (Figure 2) is a crucial element in the data center architecture. Depending on the level of availability and resilience required, power is supplied via one or more independent feeds. The low-voltage distribution board also distributes power to the various systems and functions of the IT infrastructure, e.g. the different primary supply chains, the UPS system and the backup diesel generator.

Figure 2: Power Supply Chain in a Data Center

Uninterruptible power supply (UPS) units ensure the continued availability of power in the event of outages. A UPS separates the primary grid (the power lines from the utility) from the power supply to the equipment in the data center. The latest UPS systems achieve this by converting the primary alternating current to direct current before converting this back to ‘clean’ AC free of spikes and noise with which to supply the equipment. The DC circuit has a battery for backup, should the primary feed fail. On the consumption side, the feed is subdivided until ultimately reaching the socket of an installed device (e.g. a server).

Companies are increasingly using intelligent PDUs instead of simple multiple sockets in racks with network and server equipment. Rittal's PDUs (Figure 3), can measure the distributed electrical parameters, switch loads, and identify environmental factors such as temperature and humidity. They allow a detailed view of the conditions inside the rack, and give administrators and data center operators the information needed so that they can quickly find faults, implement energy efficiency measures, and discover potentials for use.

When selecting PDUs, many parameters are important, ranging from the mechanical properties on the load capacity and switching capacity of the devices to redundant functions and accuracy. The integration into a higher-level management framework should also be considered and planned, as should the protection of the data and the switching functions from unauthorized access.

Figure 3: Rittal PDU mounted in the TS IT rack

Rittal’s range of PDU products consists of Basic, Metered, Switched and Managed models. It provides a continuous system solution, from power distribution to complex analysis functions. The functions of the PDUs are based upon and complement each other. Basic has a pure distribution function, Metered measures the overall consumption data, and Switched can also switch individual sockets. Managed also provides additional electrical data from each individual socket.

In addition, high flexible modular PDU systems support the exchange of PDU modules during operation without any interruption. By this it will be possible to switch e.g. from C13 to C19 outlets or to change from passive to active modules.

Step 3: Cooling

Much of the electric power fed into the data center is ultimately converted to heat by the IT hardware. This heat must be dissipated from the data center, which is accomplished by generating and distributing sufficient cooling.

Cooling can be produced in various ways. The most effective method and the most suitable combination of technologies are selected in accordance with the customer’s requirements. Chillers, like refrigerators, generate cooling by means of electric power, which makes them major energy guzzlers. In many cases, however, free cooling with outside air can drive down the temperature of warm water sufficiently to meet a data center’s cooling needs. Chillers and free-air cooling systems can complement each other very effectively, assuming appropriate control systems are in place.

Therefore, special attention has to be paid to the appropriate cooling technology in a data center (Figure 4); because a major share of operation costs is caused by cooling. Depending on the heat load and the number of IT racks an adequate cooling technology has to be selected for the data center.

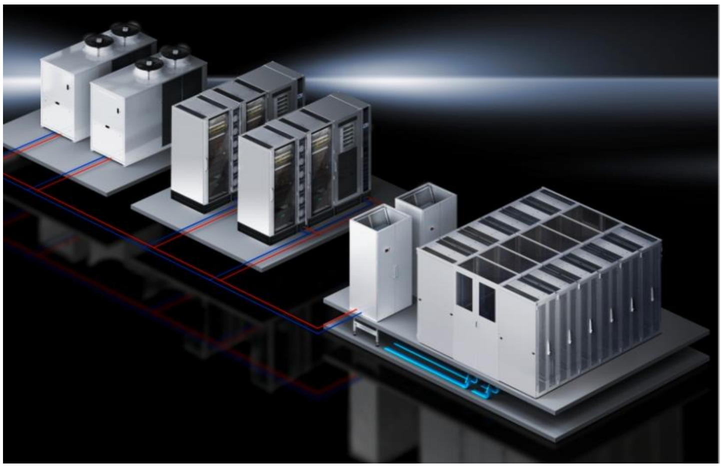

Figure 4: Cooling Chain within the Data Center

In case of a low heat load combined with a large scale implementation a raised floor climate system approach will be used. A pipe system feeds the cooled water into the data center. If the facility has a raised floor, the cold water is generally routed to the CRAC units’ heat exchangers. The warm air in the server room is drawn into the CRAC units, which cool it in their heat exchangers, and discharge the cooled air under the raised floor. The cold air emerges in front of the server enclosures through perforated floor tiles, where it is drawn in by the computer hardware.

It makes very good sense to strictly separate a data center's cold and hot air streams. This is done by containing the aisles between rows of enclosures by fitting ceilings, and doors at either end. In addition, sensors installed in the hot and cold aisles enable the temperature to be monitored and precisely controlled.

In case of a higher heat load the heat exchangers will be placed directly in the row of racks. In this configuration the amount of air circulating is reduced resulting in a higher efficiency.

To cool high-performance servers, chilled water can be routed directly to the enclosure rows. Rittal's Liquid Cooling Package (LCP) is a heat exchanger that can be mounted on the side of an enclosure. This enables cool air to be discharged directly in front of the 19-inch racks, where the server fans draw it in. The hot air expelled from servers is returned to the heat exchanger. This efficient solution creates a closed air circuit in the enclosure. It is critical to ensure that any openings are sealed with blanking panels to prevent cold and hot air from mixing.

In general the major share of server and storage systems facilitates the classical "front-to-back cooling" approach (cold air is taken-in at the front, warm air is exhausted at the back). But a significant part of switches takes the cold air from the side using a "left-to-right cooling" technology, because the front panel is used for the high amount of ports.

Figure 5 depicts the integration of an air duct on the right side of the 19" rail supporting an air routing to the intake holes of the dedicated switch. The air duct supports the guidance of cold air behind the cold aisle/warm aisle partition. The approach shown above uses an extension of the air baffle plate to integrate additional air ducts, air channels.

Consequently, a combination of a "front-to-back" and "left-to-right" cooling can be realized by using the air baffles and air ducts – a classical approach of a mixed server rack including a switch in the upper part of the enclosure.

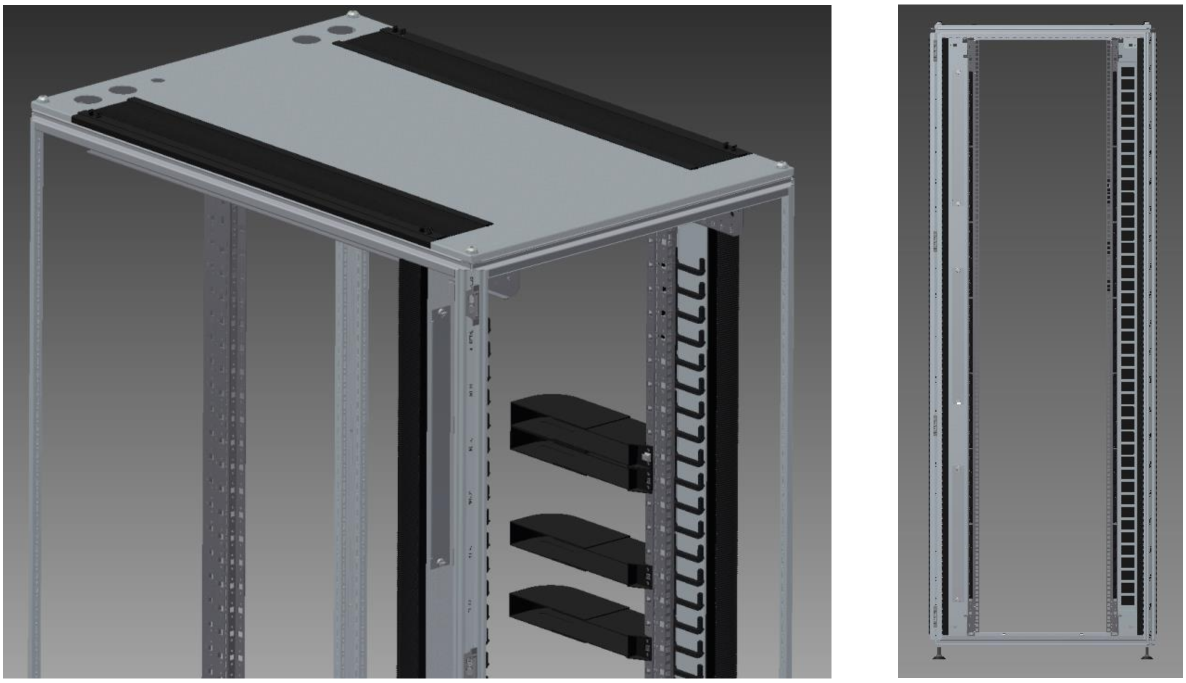

Figure 5: Air Baffle Plate (left of 19” rail) and Air Duct (right of 19” rail)

In addition, it is also possible to install network components in the rear 19” sections – facilitating shorter cables to the server ports. But, enough cold air has to be guided to the network devices by using a 19”-1U air duct, channeling the cold air from the front to the back side directly to the dedicated switch.

Step 4: Security

An equally important task for IT infrastructure management software is to gather and evaluate all safety- and security-related data obtained from sensors, and where necessary, to respond appropriately (e.g. by generating an alarm).

Preventing the misuse of data is a key concern for all organizations. The Rittal CMC system (Figure 6) controls access to the server racks and logs access requests by identified persons (authentication by smart card, transponder or magnetic card) and attempted access by unauthorized persons (vandalism sensor). The CMC also uses sensors to capture all safety-related parameters such as temperature, humidity, smoke, air flows and leakages. And it records all IT equipment power consumption data.

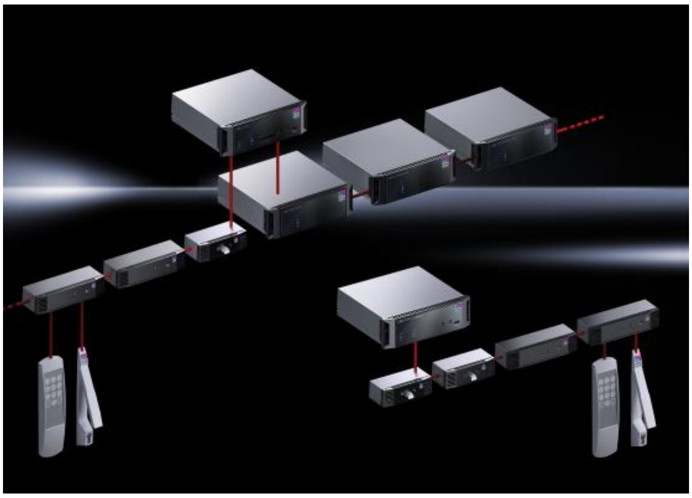

Figure 6: Rittal Monitoring System CMC with sensors

The Rittal CMC system also enables the IT infrastructure management software to take corrective action on the equipment being monitored – for example, to regulate fan speeds or pumping rates.

Step 5: Structured Cabling

TIA-942-A [Ref. 13] and EN 50600-2-4 [Ref. 13] provide structured cabling guidance for data centers. To implement a structured cabling solution, a star topology is recommended. With a star topology, maximum flexibility in the network is achieved. The cabling infrastructure should be implemented to allow moves, adds and changes without disturbing the cabling itself. MACs include network reconfiguration, growing and changing user applications and/or protocols.

While the standards mentioned help in guiding the design of the physical infrastructure, the logical infrastructure does not have a standards body to fall back on. Logical architectures vary based on customer preference and are also guided by the network equipment manufacturers. Generally, modern logical architectures can be broken into four layers:

1. Core
2. Spine
3. Leaf
4. Storage

The critical job for many designers is to translate these logical topologies onto a TIA-942-A or EN 50600-2-4 structured cabling infrastructure. This translation will affect some of the key design elements of a structured cabling solution such as fiber counts, hardware considerations and cable routing. The first step is to translate the TIA-942-A / EN 50600-2-4 areas (MDA, HDA, ZDA, EDA) to the logical architecture areas (leaf, spine, storage). The following Table 1 shows a comparison between the two.

Logical architecture	EN 50600-2-4	TIA 942-A
Core & Spine	Main Distributor	Main Distribution Area (MDA)
Spine	Intermediate Distributor	Horizontal Distribution Are (HDA)
Leaf & Storage	Zone Distributor	Zone Distribution Area (ZDA)
Storage	Equipment Outlet	Equipment Distribution Area (EDA)

Table 1: Comparison between logical architecture and structured cabling topology

To translate the logical network into a structured cabling infrastructure, the data center will be segmented based on the logical topology. Each zone should use a Middle of Row (MoR) interconnect solution for the cabling, and within each zone, the EDAs will utilize a Top of Rack (ToR) interconnect. The EDAs will serve the network, server and storage equipment in each cabinet and the ZDAs will serve the EDAs. The ZDAs on the other hand will guide the cabling back to the main cross-connection cabinet(s) in the MDA.

The next step is to determine the number of fibers that are needed to implement this structured cabling solution. In order to determine the overall amount, both redundancy and networking requirements have to be taken into account.

The resulting design will probably lead to a high number of individual fibers that have to be guided in the trunk cables. Data center trunk cabling is usually routed in raised floors and overhead ducting. The cable routing system in many data centers has grown historically, and is therefore rarely at an optimal level. The reasons for this include:

- Cables were put in long after the initial roll-out, not following any structured planning and not being bundled in a neat fashion.
- Documentation on the deployed cabling does not exist or is poor. As a result, cables that are defective or no longer required cannot be removed.

Cabling solutions that take up less volume provide a solution: Multi-core, fiber optic 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.

One key question remains: Where should patch cords be installed? A device connection should always supply only one element (e.g. a server) in the same cabinet. As a result, no patch cords should be stowed in the floor. It should be avoided putting these in the raised floor whenever possible. One of the following options should be used instead:

- Conventional or mesh cable trays installed overhead.

- Trough systems such as the Raceway System from R&M. Like conventional trays or mesh cable trays, these are installed above cabinets.
- Under floor systems such as the Raised Floor Solution from R&M. These keep patch cords in one box that is installed in the raised floor in front of cabinets.

Data centers can often arrange distribution panels and active network in either the same rack, or in two racks located directly next to one another. As the following Figure 7 shows, 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.

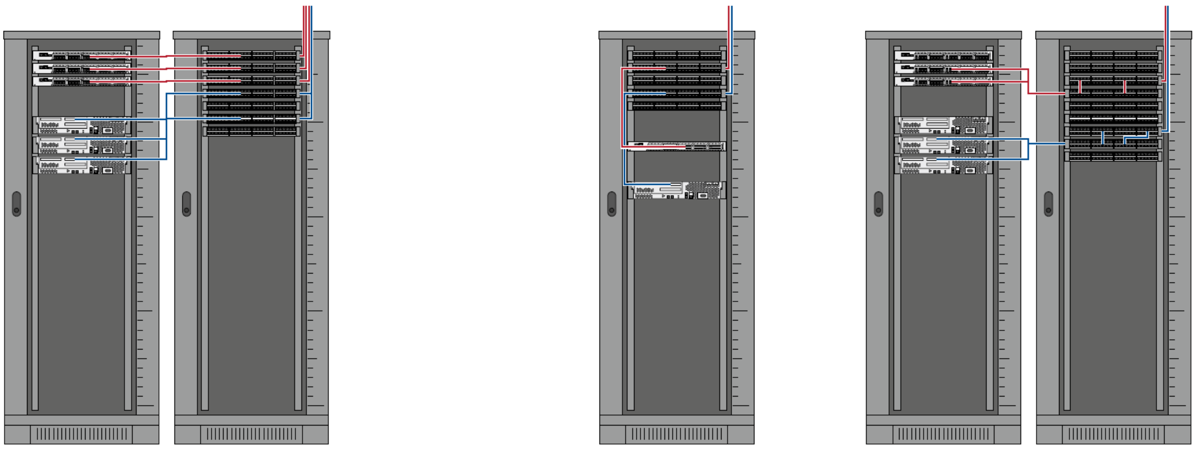

Figure 7: Three flexible ways to patch equipment

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 – especially if everything is monitored by an automated infrastructure management solution.

Step 6: Polarity Management

Migrating to the next generation of switches will require careful planning for fiber counts. State-of-the art systems such as 40G Ethernet and 100G Ethernet require six or twelve times the amount of fiber per individual link. 40G Ethernet systems will utilize a 12-fiber MTP® connector as the interface into the transceivers.

With the latest generation of 100G Ethernet also utilizing a 12-fiber MTP® connector as the interface into the transceiver modules, the fiber count would be the same as with 40G systems [Ref. 11].

Polarity management is the task of ensuring that the signal sent by one transceiver on the transmitter (Tx) port is received on the receiver (Rx) port by the other transceiver. The primary goal of polarity in the cable infrastructure is to ensure that in every panel, the Tx port ends up at an Rx port. This ensures that when equipment is connected, Tx on the panel is simply connected to Rx on the equipment, and Rx on the panel to Tx on the equipment. If polarity is not actively managed, the only way to install the patch cabling would be through trial and error.

To ensure that polarity is maintained in a structured cabling environment, TIA/EIA 568-C.0 describes three methods to manage this challenge. However, each of these methods has the downside of having to cross-out somewhere. This means that either two differing patch cords, or two differing MTP® modules, or a complicated trunk cable design has to be employed.

To simplify this challenge, R&M has innovated a smart polarity management MTP® module, the Type S HD MTP® Module. This method requires only one patch cord type and one MTP® module type. The fiber cross-over for duplex signal transmission (such as in 10GBASE-SR or 16GFC) takes place in the pre-assembled module. The connectivity scheme for trunk and patch cords always remains the same, even for parallel transmission in the construction of 40/100G Ethernet systems.

Step 7: Network Monitoring and TAPs

As the cloud and software-defined everything continuously dissolve the concept of individual devices and device management, application traffic and end-user experience become more and more difficult to monitor and manage. Data center network managers are challenged with gaining superior visibility of their networks, enhancing application performance, and ensuring integrity of the security system.

To maintain extensive visibility in this environment, traffic access points (TAPs) are the most accurate, reliable and OpEx-saving way to access the data. A TAP is a passive fiber optic splitter to establish an identical copy of the optical signal passing through it. The fiber optic cable with the incoming signal is connected to the splitter input. The split signal is then separated into the live output which is connected to the receiving in-band device, and the monitor output which is connected an out-of-band device. Due to the fact that a TAP utilizes such splitters in a duplex fashion, a complete copy of all traffic between two devices can be produced.

Figure 8 depicts the signal path schematics of 24-fiber multimode fiber HD TAP Modules. The MTP® connectors on the right side of the illustration provide two connections for serving the live traffic channels via trunk cables, and two MTP® connectors (red) serve the TAP channels for connecting to monitoring equipment via MTP® trunk or MTP®-LC harness cables. The left side of the illustration shows the front surface of the modules providing 12 LC-duplex ports for patching.

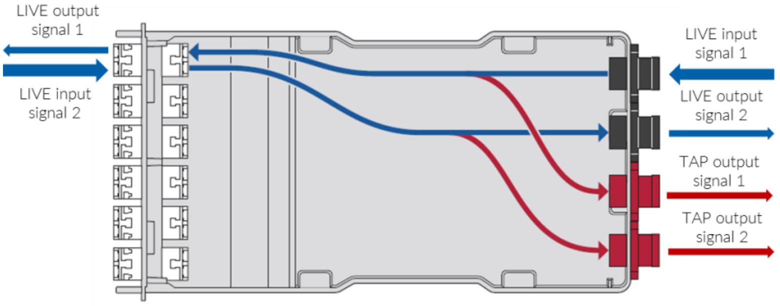

Figure 8: HD TAP Module signal path schematics

The proportion at which the splitter divides the incoming optical signal between the two outputs is called "split ratio". R&M's standard TAPs use a 50/50 ratio, meaning that 50% of the incoming light goes to the live port and 50% to the TAP port. Clearly, a split ratio of 50/50 represents a loss of 3dB by definition. With these additional losses, the overall fiber budget needs to be carefully assessed.

Besides the losses associated with the division of the optical signal, the splitter introduces no latency or other alteration of the signal. Its performance prevails whether or not monitoring equipment is connected to the TAP port, so that one can "deploy and forget" these HD TAP Modules.

TAPs are usually placed between two given network devices such as switches, routers, and storage, to provide network and security personnel a connection for monitoring. By deploying TAPs as part of the infrastructure, one also eliminates downtime needed to insert TAPs ad-hoc between monitoring and network devices. To complete the visibility eco-system, the TAPs have to be connected to monitoring and analysis equipment, including receivers, analysis hardware and software.

Although TAPs are not explicitly mentioned in the relevant standards as sources of loss for the link planning, they can be budgeted under the same conditions as connectors or conversion modules.

Figure 9 shows a typical 10GBASE-SR link including an optical cross-connect with an integrated 50/50 HD TAP Module.

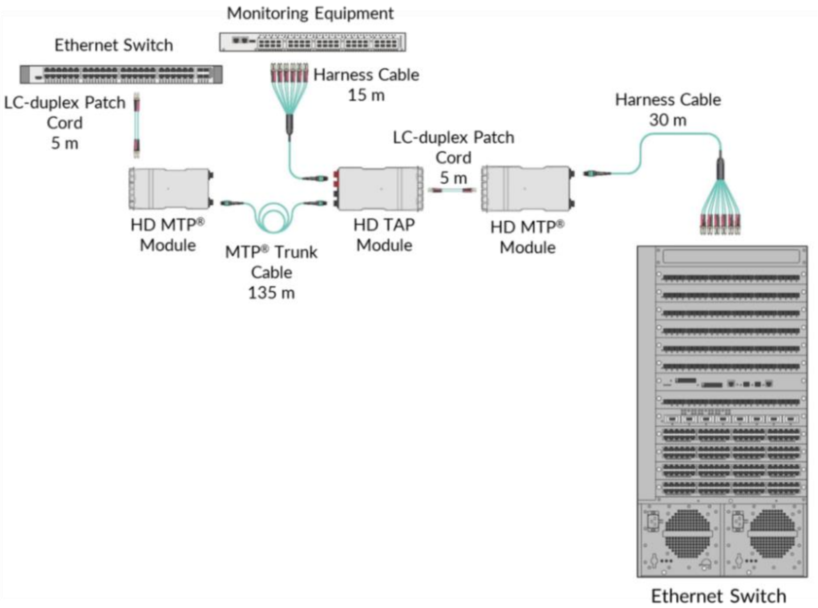

Figure 9: A typical 10GBASE-SR link with 50/50 HD TAP Module at the cross-connect

The 50/50 TAPs introduce additional insertion loss of 3.9dB to both the live and the TAP path. These additional losses drastically reduce the channel length limit for 10GBASE-SR. In this topology configuration, the live traffic channel (running from a core switch to an aggregation switch) is made up of one HD TAP Module, two HD MTP® Modules, two LC-duplex patch cords, one MTP®-LC-duplex harness cable, and one MTP® trunk, all with a total length of 175 meters. All cables are based on OM4 fiber.

The near end TAP path (here, running from core switch to monitoring equipment) has the HD TAP Module, one HD MTP® Module, two MTP®-LC-duplex harness cables and one LC-duplex patch cord, and its total length is 50 meters. The far end TAP path (here, connecting the aggregation switch with the monitoring equipment) includes the TAP, one HD MTP® Module, one LC-duplex patch cord, an MTP® trunk and one MTP®-LC-duplex harness cable, resulting in a total length of 155 meters.

The corresponding insertion loss is calculated for each of these three paths. These calculated insertion loss values can then be used to compare with the maximum possible channel length. The maximum lengths for the example (Figure 9) are listed in Table 2.

Live path insertion losses from left to right are:

0.35dB + 3.9dB + 0.35dB = 4.6dB

Near end TAP path insertion losses from left to right are:

3.9dB + 0.35dB = 4.25dB

Far end TAP path insertion losses from left to right are:

0.35dB + 3.9dB = 4.25dB

Signal path	Connector insertion loss [dB]	Maximum channel length [m]	
		OM3	OM4
Live path	4.60	170 m	230 m
Near end TAP path	4.25	190 m	260 m
Far end TAP path	4.25	190 m	260 m

Table 2: Channel length limits for a monitored 10GBASE-SR link with 50/50 TAP

Comparing the maximum channel lengths with the topology in Figure 9 reveals that the power budget supports all paths – provided the corresponding cables include OM4 fiber.

Step 8: AIM / DCIM

As the average surface area of data centers is currently between 1,000 and 2,500 m^2, often with thousands of network ports, manual cable tracking is no longer a viable option. Yet all too many network managers still carry out inventory and management of physical infrastructure with Excel sheets - or even paper, pencil and post-it notes. Developing realistic expansion plans and carrying out risk analysis are impossible, let alone complying with legislation and best practices governing data security and availability.

Automated Infrastructure Management (AIM) systems provide the solution, offering functions for mapping, managing, analyzing and planning cabling and network cabinets. These systems improve operational efficiency and facilitate the ongoing management of the passive infrastructure. The integrated hardware and software system automatically detects when cords are inserted or removed and documents the cabling infrastructure, including connected equipment. This enables ongoing, granular management of infrastructure as well as data exchange with Data Center Infrastructure Management (DCIM), Building Management Systems (BMS), IT Service Management (ITSM), asset lifecycle and security management systems and other platforms. Everything can be monitored and administrated from a common software tool.

The entire infrastructure is represented in a consistent database, offering precise, real-time information on the current state and future requirements of the data center. This 'single source of truth' brings benefits in a number of specific areas. Administration of cabling infrastructure and connected devices is always up to date. Furthermore, this approach provides a basis for efficient facilities and IT management processes and systems, as well as other networked management processes and systems such as intelligent building systems and business information systems. Constant asset tracking and asset management in combination with event notifications and alerts assist with physical network security.

A recent study carried out at one of R&M's large European installations has shown a reduction of 85% in the time required for tracking and documenting data center connectivity. Following the adoption of R&M*inteliPhy*, an RFID-based AIM, accuracy was very close to 100%.

R&M*inteliPhy* can be mounted on the HD platform from the R&M range at any time in the future. The entire system is illustrated in Figure 10 and made up of:

- Analyzer
- R&M*inteliPhy* Manage Server
- R&M*inteliPhy* Manage Clients
- RFID tags
- Sensor strips

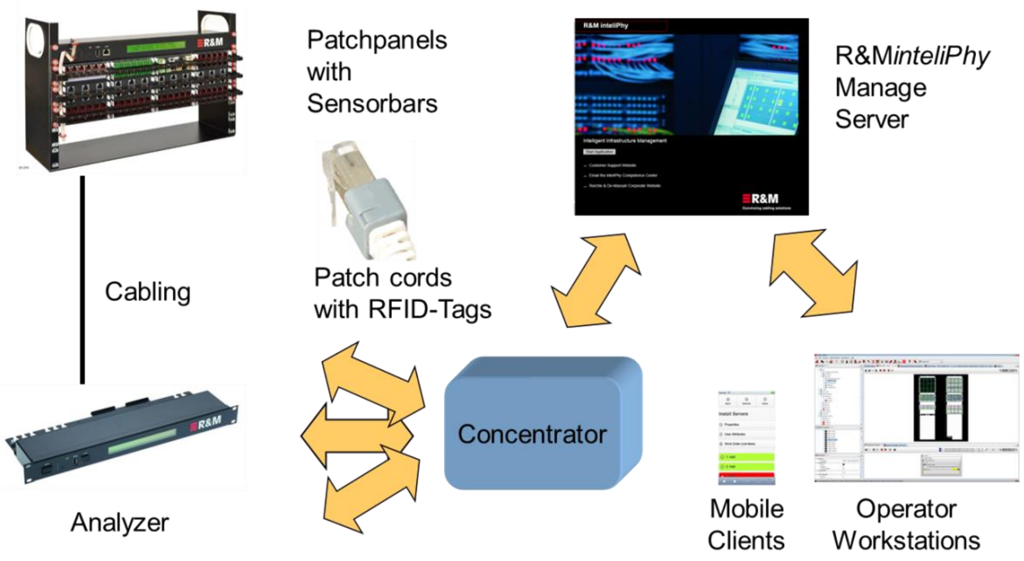

Figure 10: The schematic system setup of R&M*inteliPhy*

The Analyzer is connected with all sensor strips via a cable system. It reads out the sensor strips and provides the server with the latest connection data. Its site of operation: in a 19'' cabinet or saving space on top hat rails within the cabinet. An Analyzer can cover several cabinets and up to 2000 ports. If there are several Analyzers in one installation, a concentrator is used that compiles the information of all Analyzers and communicates with the server.

In a central position, the R&M*inteliPhy* Manage Server controls and monitors the entire infrastructure in real time. Furthermore, it offers a complete set of administration and automation tools. Third-party systems are easy to integrate using standardized interfaces. The server does not depend on an operating system and is also available as a cloud-based service (Software as a Service).

A browser or smartphone is all that is needed to operate R&M*inteliPhy*. The graphical user interface features intuitive operation and provides access to all functions, from automatic routing to the scheduling of modification projects. Several users can be working with the system at any time.

An RFID tag on the connector contains all the necessary information to identify cables and connectors without any doubt. The retrofit-able plastic guard with the tag fits all R&M copper and fiber optic connectors. A sensor strip detects the RFID tag in a non-contact operation. It can be retrofitted to all R&M*inteliPhy*–compatible patch panels. The strip records connectors and connections. LEDs indicate the operating state of the ports and support the technician in patching.

A deployed AIM system enables organizations to optimize business processes from an IT infrastructure perspective. It eliminates stranded capacity, facilitates end-to-end analysis and agile infrastructure management and supports predictive analysis and dynamic infrastructure. Since the entire infrastructure is represented in a consistent database in an AIM system, inquiries into resources such as free ports in network cabinets ducting capacity, or cabinet space can be answered quickly and easily.

In addition, as a complementary tool to AIM is RiZone, Rittal's DCIM software for data centers. RiZone is the ideal tool to help IT administrators master their day-to-day challenges – everything from monitoring and management of single devices and components to the optimization of the entire data center with regard to cost-effectiveness, availability, reliability and security.

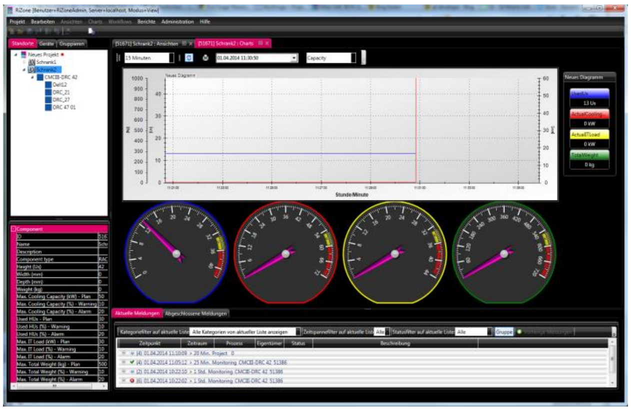

Figure 11: DCIM Dashboard

RiZone monitors and manages all the IT infrastructure components required to ensure the secure and reliable operation of the servers, storage systems, routers and switches. These include:

- Power supply and backup
- Cooling and air conditioning

- Room and enclosure monitoring
- Data center safety and security
- Efficiency and energy consumption

IT administrators need to be aware of the interdependencies between the various systems and facility functions of a data center, such as physical IT infrastructure, networks, servers, central building control systems and ERP software. RiZone offers intelligent interfaces that help to build a complete and up-to-date picture of data center resources.

RiZone can analyze trends and visualize the data center's overall consumption data (kW/h, euros, CO_2 emissions) and efficiency level. The software allows users to define control loops for maintaining the ideal operating point in line with changing conditions. This enables the IT infrastructure to be continuously optimized to drive costs down and keep them as low as possible.

RiZone's standard SNMP interface enables the software to be integrated with higher-level server or network managing systems.

Step 9: Lifecycle

For IT managers, the useful lifetime of a server may be four to five years. For an IT service enterprise, an outsourced management contract might last four years. Evolving technologies and the demand for new business applications create an environment where servers, switches, storage and cabling are being provisioned, retired, serviced and moved among facilities in a frenzied way.

In such an environment it is easy to lose track of assets. There have been cases where organizations were paying for extended maintenance on physical servers that were no longer part of the data center. Without an infrastructure management system, an asset removed from a cabinet might be placed into stock for several months without following actions.

At the same time the typical data center lifecycle is 10 to 15 years, and cabling architectures have a tremendous effect on the data center's ability to adapt to network architecture changes, evolving bandwidth needs, and technology moves, additions, and changes.

Cabling standards are regularly written and reviewed. For instance, TIA standards are reviewed every five years and may be reaffirmed, withdrawn or revised. ISO/IEC standards are written with a target lifespan of 10 years. IEEE application standards are written, and regularly revised on current product capabilities. These reference the current cabling standards.

Cabling architectures, if not chosen correctly, could force an early replacement of the infrastructure to meet connectivity requirements as network technologies evolve. Forward-looking IT departments should therefore prepare their networks for the future by integrating support for 40/100 Gigabit Ethernet and an AIM system to document and track IT assets into their strategy.

An often overlooked aspect is stocking spare patch cords. It is best practice to keep a small stock of patch cords in multiple lengths. Experience tells, that 1 m, 3 m, and 5 m are the most frequently used patch cable lengths. The types will depend on the specific application but generally, the stock should include RJ45 Cat 6_A and OM4 LC-duplex cords with potentially already 12-fiber OM4 MTP® cords.

With the predictive analysis function of AIM systems, a precise count on the installed cabling and port count usage can be used to forecast what spares need to be kept on hand.

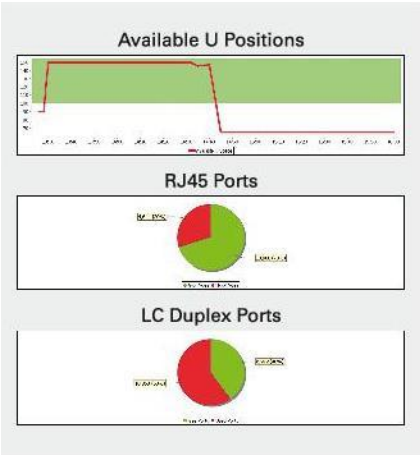

Figure 12: R&M*inteliPhy* dashboard illustrating the availability of ports

At the end of the lifecycle, product lifecycle management shall select those equipment items for decommissioning that are affecting optimal operations, either by its behavior in monitoring and event management, or by its non-optimal maintenance or energy costs. Age of the equipment can be a parameter, too, as maintenance costs can rise at the end of the lifecycle.

Step 10: Management Processes and Services

To keep the data center always operating at normal levels, an overall maintenance plan for all infrastructure elements should be established. This maintenance plan has to be compliant with the requirements of the individual vendors and can be implemented in DCIM or AIM systems. The following clauses shall highlight the individual management processes covered by these systems.

Operations management has to implement a monitoring infrastructure to provide information about the status and failures of all data center infrastructure elements. Additional data for use in management processes such as energy management; lifecycle management, capacity management and availability management can be acquired by sensors and logged in a central database.

Incident Management is key to removal of failures and recovery to normal operation state. These systems receive messages about failures. Incidents are registered, monitored, solved and closed. Incident logging registers the beginning and the end of every failure for the purpose of analysis in availability management. It is recommended to review each incident and the response to it and where possible changes made to prevent the incident from re-occurring and to improve the response should the incident be repeated.

Of course, the aim of Incident Management is to minimize the time of outages. Therefore, the key performance indicator (KPI) mean time to repair (MTTR) shall be reported for every incident. Where a Service Level Agreement (SLA) is in place then compliance to the SLA is an advanced KPI for incident management.

Processes like incident management, capacity management, energy management or availability management can register changes for the change management process. The creator of a change shall give a description and the desired effects for a change at registration. Changes shall be planned in order to enable proper coordination. Downtimes should be minimized by coordinating changes relating to the same system. Resources shall be made available to ensure that the change can be completed successfully. Change management shall provide information about planned changes to operations management [Ref. 12].

Such an approach is only feasible if all changes are monitored and the creator is automatically informed about the status, esp. when the change is implemented successfully.

The last aspect that shall be mentioned in this section is capacity management which aims to optimize the usage of the data center's provisioned capacity. Therefore, it has to monitor, analyze, manage and report the capacity of the data center's infrastructure.

In capacity management three categories of capacity must be distinguished:

a) Total capacity of the data center: the maximum capacity that it was designed for at full use;

b) Provisioned capacity: the capacity of the actual installed infrastructure;

c) Used capacity: the actual capacity used by the IT and facility.

Ideally, the granularity of capacity management is not limited to the room level but already allows gaining insight into the individual height units – or even better: the port level.

R&M
Convincing cabling solutions

Literature

Ref. 1 Uptime Institute, Tier Definition: http://uptimeinstitute.com/TierCertification

Ref. 2 BSI: Verfügbarkeitsklassen: https://www.bsi.bund.de/DE/Themen/weitereThemen/Hochverfuegbarkeit/HVKompendium/hvkompendium_node.html

Ref. 3 BITKOM Leitfaden betriebssicheres Rechenzentrum: http://www.bitkom.org/files/documents/131213_Leitfaden_BRZ_web.pdf

Ref. 4 Sarbanes-Oxley Act legal text: http://www.sec.gov/about/laws/soa2002.pdf

Ref. 5 Basel II: http://www.bis.org/publ/bcbs107.pdf

Ref. 6 Health Insurance Portability and Accountability Act legal text: http://www.gpo.gov/fdsys/pkg/CRPT-104hrpt736/pdf/CRPT-104hrpt736.pdf

Ref. 7 Payment Card Industry Data Security Standard: http://www.bis.org/publ/bcbs107.pdf

Ref. 8 ITIL Best Practices: https://www.axelos.com/itil

Ref. 9 IT Service Management: ISO/IEC 20000 Norm: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=60329

Ref. 10 19“ Standard: EIA 310-D, IEC 60297 und DIN 41494 SC48D

Ref. 11 IEEE 802.3bm: http://standards.ieee.org/about/get/802/802.3.html

Ref. 12 EN 50600-2-6: Management and operational information

Ref. 13 ANSI / TIA-942-A: Telecommunications Infrastructure Standard for Data Centers

Ref. 14 EN 50600-2-4: Telecommunications cabling infrastructure

About R&M

As a global Swiss developer and provider of connectivity systems for high quality, high performance data center networks, R&M offers trusted advice and tailor-made solutions that help Infrastructure and Operation Managers delivering agile, reliable and cost-effective services for a business-oriented IT infrastructure.

R&M's Convincing Cabling Solutions approach helps organizations to holistically plan, align and converge office, data center and access networks. Its fiber optic, copper and infrastructure monitoring systems ensure the most stringent standards in product quality. Knowing that highest quality products alone are not enough to guarantee faultless operation, R&M works with you on a thorough analysis followed by a structured and forward-looking design of the physical network to provide efficient solutions.

If you are looking for trusted advice and enduring post-sales service – R&M can help.

For additional information, please visit **datacenter.rdm.com**.

About Rittal

Rittal, headquartered in Herborn, Hessen, Germany, is a leading global provider of solutions for industrial enclosures, power distribution, climate control and IT infrastructure, as well as software and services. Systems made by Rittal are deployed across a variety of industrial and IT applications, including vertical sectors such as the transport industry, power generation, mechanical and plant engineering, IT and telecommunications. Rittal is active worldwide with 10,000 employees and 58 subsidiaries.

Its broad product range includes infrastructure solutions for modular and energy-efficient data centres with innovative concepts for the security of physical data and systems. Leading software providers Eplan and Cideon complement the value chain, providing interdisciplinary engineering solutions, while Kiesling Maschinentechnik offers automation systems for switchgear construction.

Founded in Herborn in 1961 and still run by its owner, Rittal is the largest company in the Friedhelm Loh Group. The Friedhelm Loh Group operates worldwide with 18 production sites and 78 international subsidiaries. The entire group employs more than 11,500 people and generated revenues of around €2.2 billion in 2014.For the seventh time in succession, the family business has won the accolade "Top German Employer" in 2015.

Further information can be found at **www.rittal.com** and **www.friedhelm-loh-group.com**.