DATA CENTRES ›
UNDERSTANDING THE ISSUES

TECHNICAL ARTICLE

Molex Premise Networks

molex®

EXECUTIVE SUMMARY

The term data centre usually conjures up an image of a high-tech IT environment, about the size of a football pitch, full of equipment from a vast array of vendors with enough air conditioning to keep the occupants of the penguin enclosure in a zoo happy. This technical article discusses issues around data centre technologies and concepts.

Definition of a Data Centre

The term data centre usually conjures up an image of a high-tech IT environment, about the size of a football pitch, full of equipment from a vast array of vendors with enough air conditioning to keep the occupants of the penguin enclosure in a zoo happy.

In fact, the term data centre applies to any space specifically allocated for cabinets or frames, housing network equipment that is either a source of services to other network devices (typically distributed over generic cabling) the receivers of services from an external telecommunications network (such as a PABX or ADSL connection) or a source of services to an external network (typified by data hosting facilities).

"Modern businesses are highly dependant on these IT facilities.."

We also generally assume a data centre to be a multi-client environment, with services to maintain that environment provided by a third party. The term is however equally applicable to the main communications room within an end-users internal network. In other words, a data centre may be a server room, an equipment room or a co-location facility.

The Rise of the Data Centre

Modern businesses are highly dependant on these IT facilities and care needs to be taken to ensure the environment created to house them supports their continued trouble free operation. In recent years there has been a growth of managed data centres. Whilst this may be an outsourcing move to save money, I believe it is more likely that network owner are increasing aware of their businesses IT dependency, but lack the budget or the cross-discipline expertise to cater for it in-house. This requires co-ordination between a number of technical services including electrical, HVAC, networking, fire detection and suppression and the wide area telecommunications service provider.

The technologies and concepts examined in this article are equally applicable to both single client and multi-client environments, making it easy to see why the later is an attractive option to a busy network manager with limited resources.

Applicable standards

Currently there are no standards specifically written to govern cabling implementation in these spaces, although EN 50173 Part 5 is on its way to fill this void. Using the familiar media of optical fibre and balanced copper cabling, a hierarchical approach is employed, similar to BS(EN)50173 Part 2, Generic cabling for office premises.

Within the data centre we will see Main Distributors (perhaps accommodating a core switch), supporting Zone Distributors (possibly a workgroup switch or cross connect supporting an aisle of racks), connecting to Equipment Outlets (expected to be located within the equipment racks). The will also be the addition of an External Network

Interface and its associated cabling, for connection to the outside world and the service providers network. None of this should prove problematic to a competent installation organisation, and is bound to be the subject of further articles after the document is published.

Key Issues for the Network Operator
Regardless of the size of the data centre there are three common priorities shared by their owner, operators and occupiers; Flexibility, Accessibility and Reliability.

"..there are three common priorities ..... Flexibility, Accessibility and Reliability"

Flexibility
A flexible infrastructure enables a wide range of types of equipment to be accommodated, and the hierarchical approach to data centre cabling that EN50173 Part 5 is proposing looks set to deliver that.

In a client owned and operated data centre there is often more control over the equipment deployed, the inherent flexibility being used as a safeguard against future developments in technology, or change of IT strategy. Within a co-location or hosting facility however, flexibility is a pre-requisite for day-to-day operation. Client equipment can arrive at short notice, and require immediate connection and commissioning to keep any down time to minimum, and to ensure that service level agreements are met.

The requirement to deploy a wide variety of equipment within the data centre can have an effect on the physical elements of the building. The load limit of the floor may need to be considered, whether that is the structural floor or any access floor system attached to it. The average server rack is unlikely to present any problems, but large un-interruptible power supplies and storage area network silos may need special consideration. This is clearly best achieved during the design stages of the building, not the fit-out.

Accessibility
Access is clearly important. The equipment will not install and configure itself, so personnel access will be needed for this scheduled event. This has a knock on effect on the sizing of the data centre, as space will be needed for the technicians to work and to manoeuvre equipment. BS(EN) 50174 is some help here, advising that a 1.2-meter clearance around cabinets is required. Ideally data centre sizing should then simply be a case of working of how many racks you have, then adding the required clearance to their overall dimension.

Access for equipment is also an issue with the size of doors, proximity to lifts and access to loading bays all needing consideration. Many installers will have encountered this problem, with a 800mm cabinet not fitting through a 2'6" door. Simply specifying double doors goes a long was to solving this sort of issue, and again this is much easier and

cheaper at the data centre design stage, rather than when equipment is being installed!

Having decided that the equipment within the data centre is mission critical to the business, the case of unscheduled downtime from equipment failure also needs consideration here. It is clear that in the event of a failure, the deployment of technicians will be required, so access to the site must be arranged often in compliance with strict security policies. Obviously access to the equipment and its associated cabling will also be required, which is likely to involve opening cabinets and raising floor tiles. It is important to understand that whilst this enables repair work to be undertaken, it also exposes other equipment (either directly or via a shared cabling infrastructure) to the technician, and the threat of human error cannot be ignored. Procedures need to be in place to minimise this risk.

"Network availability is of crucial importance to the operation of the data centre."

Reliability

Network availability is of crucial importance to the operation of the data centre. It underpins its very existence. It is important to realise however that the need for accessibility and flexibility can have a negative effect on Reliability. Ultimate accessibility can lead to a lack of control of personnel on site, making the data centre prone to human error. Ultimate flexibility can require multiple connections in a circuit to allow for reconfiguration. Having more connections builds in more points of failure. It would seem a balance needs to be struck, and a method needs to be found to quantifying the likely reliability of data centre based upon its constituent parts.

The four tiers described by the Uptime Institute in the USA is such a system, which is worth investigating further. Recognising both the impracticality and the extremely high cost required to achieve the holy grail of 99.999% (five-nines) availability, they instead propose four more attainable levels, as follows.

- Tier I - Single path for power and cooling distribution, no redundant components, 99.671% availability.
- Tier II - Single path for power and cooling distribution, redundant components, 99.741% availability.
- Tier III - Multiple power and cooling distribution paths, but only one path active, redundant components, concurrently maintainable, 99.982% availability.
- Tier IV - Multiple active power and cooling distribution paths, redundant components, fault tolerant, 99.995% availability.

It is easy to see how the Tier IV approach can deliver more resilience that a Tier I installation, demonstrated by its anticipated unscheduled downtime of under 27 minutes per annum, compared to Tier I at nearly 29 hours, but this is at significant cost. In its N+1 configuration, it is also

worth noting that during a failure in a Tier IV data centre, Tier II reliability is available. Designing to N+2 or N+N fixed this, but is generally cost prohibitive. An expedited repair would be in order, and this is where Intelligent Infrastructure Management (IIM) systems become invaluable. Network management tools have been available for many years to monitor data traffic, but the cabling has always been a blind spot. Now we are not only able to detect an unauthorised disconnection, but relate it to its physical location within the data centre and also inform the appropriate helpdesk services of the failure so that remedial action can be scheduled.

"No services, other than those used in the data centre, should pass through it..."

Associated Building Services

Before looking at the other services required within the data centre, it is worth pointing out what should not be there. No services, other than those used in the data centre, should pass through it, reducing the risk of flooding or contamination of the equipment environment. Whilst services such as access control, CCTV and lighting are required, the key services are seen as air conditioning, power and fire detection and suppression.

Air Conditioning

The aim of temperature control within a data centre is to cool the cabinet mounted equipment, keeping it within its operation temperature range, not to cool the air outside it. Enclosed cabinets can inhibit the free flow of chilled air enabling hot-spots to develop so some clever design is required to overcome this. The concept of hot and cold aisles is often adopted. Adjacent bays of cabinets are configured with their equipment facing forward towards a chilled air outlet in the aisle between them. The cold air is then drawn by the equipment fans through the rack. This exits as warm air to the rear with the resulting convection currents acceleration the whole process, thus creating alternating hot and cold aisles. How effective this is can depend upon the specific equipment which will effect air flow. Open frames can help here, as can forced ventilation with fan trays. Ideally any HVAC system should also create a slight positive pressure, to help reduce the ingress of dust and other contaminants into the room.

Power

A generous allocation of mains power will be required for any data centre. The exact power requirement will depend upon a number of factors, not just the consumption of the network equipment installed. Lighting will need to be factored in. A significant load is likely to be draw by the HVAC plant. Even on stand-by, UPS' will draw a load. The level of resilience within the data centre will also have an impact. Quite simply the more equipment that has been provided as a back up (be that network equipment or back up HVAC and lighting), the more power will be required to cater for it, and in turn the higher the running costs.

In the design of the power distribution system, it is not uncommon to have two feeds to each cabinet. In turn these may be fed from different distribution boards, even from different feeds from the energy company.

Several general-purpose power outlets to cater for the occasional power tool or vacuum cleaner should also be provided. These should be clearly labelled, and never used to power rack mounted equipment. The risk of inadvertent disconnection is unacceptably high.

“In the design of the power distribution system, it is not uncommon to have two feeds to each cabinet.”

Fire detection and Suppression

Although seldom mandated by fire regulations non-corrosive gas suppression systems are often desirable where high value equipment is located. Where a more conventional sprinkler system is used, a dry-pipe system is desirable, where by a POC (product of combustion) detector needs to be tripped to prime the pipes, in addition to an individual sprinkler head bursting due to heat build-up. This goes a long way to prevent the accidental discharge of the system, and the flooding that goes with it. The very minimum that should be considered are wire cages around the sprinkler heads if a wet pipe system is installed.

CONCLUSION

Clearly careful design is required in the planning of a data centre. Whilst it is possible to achieve almost total network availability, this comes at a price to high for most to pay. Managing the clients' expectations from the outset is crucial if an acceptable compromise is to be reached. Ultimately the question to ask is "How valuable is your data?".