CHAPTER 3 : INTERNET DATA CENTRE

This chapter provides an insight into what an Internet Data Centre is. Having defined what an iDC is, it goes on to describe the iDC infrastructure layout, facility, system infrastructure, iDC management and operation and iDC services. The chapter ends by looking at the iDC market in Malaysia and some other countries.

3.1 Definition

Nortel defines a data centre as a building that exists to provide space, physical security and connectivity to customers who wish to outsource a portion or all of their I.S. needs (Nortel 1999).

According to Whatis.com, a data centre could refer to one of the following:

(1) A centralised repository for the storage, management, and dissemination of data and information organised around a particular area or body of knowledge.

(2) A specialised facility that houses Web sites and provides data serving and other services for other companies. This kind of data centre may contain a network operations centre (NOC), which is a restricted access area containing automated systems that constantly monitor server activity, Web traffic, and network performance and report even very slight irregularities to engineers so that they can spot potential problems before they happen.

(3) In a company, data centre is a term sometimes used to describe the central data processing facility and/or the group of people who manage the companies' data processing and networks.

For the purpose of this study, the second definition is the most appropriate for a data centre. In the early days, data centres were constructed by huge

organisations mainly for internal use. In-house servers and Local Area Networking equipment were housed in such special and restricted areas to serve the company-wide needs.

As the Internet became an important and cost effective communication tool, data centres nowadays are incorporated with Internet access to provide a means of communication with external parties like a remote branch office, suppliers, customers and contractors. These data centres are then called the Internet Data Centres, to emphasize the difference.

A more detailed and clearer definition of an Internet Data Centre is an organisation that (IDCAP 2001):

- Designs, builds and operates IT and network systems on an outsourcing basis
- Manages core systems (e.g., networks, storage, servers)
- Provides and supports hardware, software and services needed to achieve quality of service, time-to-market, cost effectiveness
- Monitors application environments but does not manage the application
- May provide customised and utility-based services

The following picture (Figure 9) indicates the general layout of an iDC with its NOC.

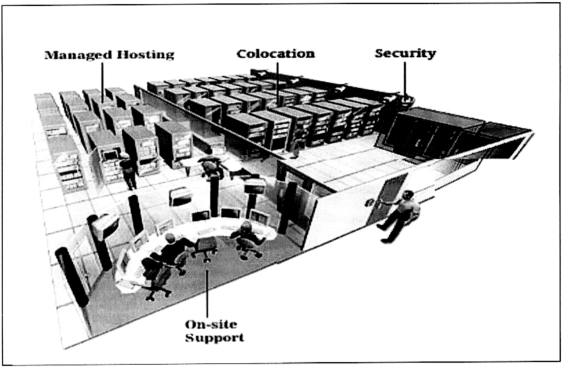


Figure 9 : The General Layout of a Typical iDC

However it is a hefty investment to construct a full fledge Internet Data Centre for use by an individual organisation. Many a time the capital outlay would not commensurate with the usage and hence would not be financially justifiable or viable. The costs are associated with the need to furnish and equip the Internet Data Centre such that it is able to facilitate a proper, secure and conducive environment for the costly servers to function in and to be housed in. That also entails a recurrent costs for maintenance, repair and upgrade. The computer and networking systems require regular maintenance and monitoring in order that the business is not affected as the IT services are interrupted. The company running the Internet Data Centre will have to hire experienced and skilled IT personnel to carry out such maintenance and monitoring work to ensure high availability and to minimise downtime. As an integrated system, a faulty component may render the system not functional unless the part is being replaced. Normally the part would be expensive and would not be stocked for backup. Firstly it is not justifiable to stock up expensive items, and secondly, IT equipment gets obsolete quickly. It may also be the case that the item is not immediately available from the vendors.

Such situation would hinder the smooth running of the business. Due to research and development, new IT standards and protocols, and hence new equipment will be rolled out within a short period. In order to catch up with the new technology, the organisation may have to upgrade its IT infrastructure. This involves also a huge expenditure and may not be good news to the investors or shareholders.

As a result, those companies with a huge capital venture into outsourcer business by investing in constructing a full-fledge Internet Data Centre. The others which cannot afford to construct and maintain an Internet Data Centre then outsource their IT services and infrastructure to these outsourcers.

3.2 Infrastructure Layout

(a) Building Layout

To provide state-of-the-art, scalable Internet facilities, it is essential that any building considered for the role of an Internet Data Centre provides:

- Raised floors to permit adequate cabling and trunking
- Redundancy of power, such as generator systems (and possibly batteries) to support the core main supply
- Availability of fibre-optic, high-speed data connectivity
- Temperature control with separate cooling zones
- Sophisticated smoke detection and fire suppression systems
- A wide range of physical access and security safeguards (swipe card restrictions, closed circuit television monitoring, 24x7 security and security breach alarms)

A number of redundant subsystems are necessary to deliver the highest levels of reliability. These include multiple fibre trunks coming into the building from multiple sources and multiple switching and routing of data within the building. Fully redundant power is also required on the premise, with multiple backup generators.

In addition, for a facility to be effective it is essential that it be located in very close proximity to major public and private Internet interconnects. This will keep interconnection overhead to a minimum and enable the service provider to remain competitive within the premium service marketplace.

(b) Operation

Operating a dedicated Internet Data Centre environment requires a specialised team. This should include security staff to manage access to the building as well as engineers with the skills to maintain the building infrastructure. For the network infrastructure, requirements include technical and support specialists to build and support the servers, as well as network specialists to deal with the routing, scaling and data security.

(c) Internal Layout

Floor design and layout for housing the servers should be related to the target market sector and price of the service. Floor layout is almost always a trade-off between security, rack density, revenue potential and manageability.

To offer a wider choice of services to meet customer requirements, while at the same time maximising efficiency in cabling, it is recommended that the floor layout be broken down into technical suites and racking neighbourhoods. The major benefits of this approach are scaling and flexibility.

Some of the technical suites can be kept vacant and outfitted later as the Internet Data Centre's capacity of number of servers under management grows. And by implementing new technical suites only when needed, the decision to equip them with racking neighbourhoods, private cages or secure vaults can be deferred.

A technical suite is an enclosed area of the Internet Data Centre with the infrastructure already in place to provide a secure location for hosting either managed or co-location customer systems. The standard specification in each

suite includes lighting, fire protection and security. Access to technical suites can be restricted via security access controls.

A secure vault is a technical suite designed to provide far higher levels of client and data security than a "standard" technical suite.

Racking neighbourhoods are generally located within a technical suite and comprise one or more floor-mounted racks capable of supporting a number of hosting servers. Each neighbourhood within a technical suite provides:

- dedicated network switching from the technical suite network trunking to the servers mounted in the neighbourhood
- dedicated power distribution to all rakes within the neighbourhood
- localised air conditioning
- secure, key lock access to individual racks within the neighbourhood

Neighbourhood racks can be located in a secure private cage within a technical suite. A cage offers higher security than a standard neighbourhood. Cages are more economical than setting up secure vaults.

A racking unit can house all servers of a customer, or can be shared among a few customers, thus allowing smaller customers to economise by paying only for the space they actually need to host their servers.

3.3 Facility

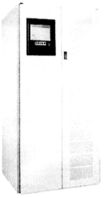
(a) Power specification

To reduce reliance on one feed from the electric power utility, which would present a single point of failure, separate feeds into the Internet Data Centre are employed. Within the building, electricity should be distributed via at least two means to the individual technical suite and other protected areas. Sometimes special considerations are given to customers who have special power requirements such as additional sockets or DC supplies.

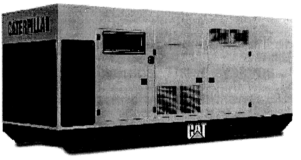
(b) Resilience

To offer higher service levels, a minimum two-fold resilience should be provided in the form of:

- Uninterruptible power supply (UPS) to each area, with the run time at least equalling to the time for the generator to kick in and go online.
- Diesel generator backup configured to kick in within seconds after a main power source failure to provide power to all relevant services.



An Uninterruptible Power Supply (UPS)
Source : Powerware

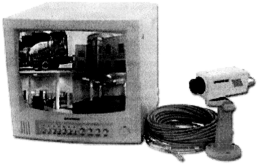


An Outdoor Generator Set
Source : Caterpillar

(c) Building Security and Access Control

A security policy is required to manage access to the Internet Data Centre and monitor activity within the building. Normally close-circuit television (CCTV) is used to provide a 24-hour surveillance on the exterior of the Internet Data Centre and also areas accessible by people.

Physical access to technical suites and other restricted areas are controlled by access control systems like swipe card access facility.



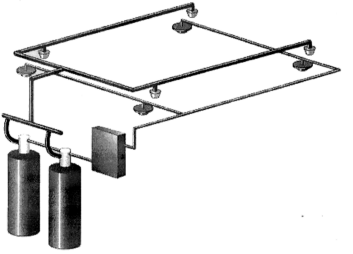
Closed Circuit Camera and TV
Source : COMERX

Magnetic Card Reader
Source : ELID

(d) Fire Control

The building should be protected by a fully automated fire detection and suppression system, but equipped with a manual override. These systems are typically zoned throughout the building and are backed up with batteries. The typical systems are those of FM200 (or equivalent) gaseous extinguishing systems.

FM200 Cylinders
Source : iadvantage

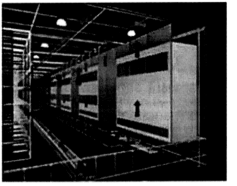


FM200 System Schematic Diagram
Source : Reliablefire

(e) Air Conditioning

An optimum environmental conditions will improve the equipment performance and lifespan. The ambience temperature is typical set at around 68±3°F (20±1.7°C) while the humidity at a constant 45% to 50%. Cooling units

are recommended to be placed over walkways or hallways and not over racks.



--- Precision Aircon System ---

Source : d1Asia

(f) Staff Facilities

The Internet Data Centre personnel will be required to walk on shift, be on call or put in longer than average hours. Therefore it is recommended to provide the staff a rest area away from the main technical suites, including a kitchen facility. Overnight secure parking is recommended for on-call staff.

3.4 System Infrastructure

Designing network access into the Internet Data Centre requires significant commercial and competitive consideration – greater resilience is gained by having multiple carriers, which include the Telco and ISP. The cost of bandwidth is the major driver for investing in products that allow more efficient management bandwidth in the facility. Typically the fibre cables entering the Internet Data Centre from both ends of the building come from competing Telcos and different Telco exchanges. Data access should also offer multiple connections to the Internet – such as nodes on the ISP's network.

Within the Internet Data Centre, the network infrastructure should be based on technology which offers scalability, resilience and manageability. The

options are the Gigabit technology or the more economical Ethernet technology.

Each server housed in a rack should be supplied with power and connectivity. Managed servers are provided with monitoring, management and backup facilities.

Server platforms should provide seamless interoperability with the operating systems, development tools and applications needed to run a successful Internet Data Centre.

3.5 Internet Data Centre Management and Operation

(a) Service Management Centre (SMC)

SMC is the core of the Internet Data Centre facility, providing systems management for all managed services and monitoring for the network. It provides first-level support for all alerts, incidents and problems, first-level contact for customers with the Internet Data Centre, direct feedback to customers on incident and problem resolution and dedicated network management and monitoring.

The SMC should be located within the Internet Data Centre itself and staffed 24 hours a day, seven days a week. During core hours, support should be provided as follows:

- SMC staff: incident and problem logging, first-level support/resolution
- Technical support staff: second and third level support

Outside of core support hours, the SMC staff should still provide initial logging and first-level support, with technical support staff providing second- and third-level support on an on-call basis.

In order to be effective, the SMC must be equipped with the following:

- Dedicated management and monitoring tools for all operational managed services (e.g. HP OpenView)

- Automated backup facilities for all managed services
- An on-line Call Management System (e.g. Remedy)
- An integrated Change Management / Asset Management / Configuration Tool
- If possible, integrated Call Management / Help Desk Management with Change Control

(b) Service Monitoring and Maintenance

Managed services customers would definitely need and want to know that their servers and applications are being monitored so that possible faults could be brought to the attention of the support staff, who could then take appropriate actions to prevent the faults or at least be ready to clear the inevitable faults.

The major selling point for dedicated managed services is the ability to provide "package" standard service monitoring facilities and to offer customers more proactive monitoring and auto-correction of faults. This requires the deployment of the appropriate monitoring tools and software.

Basic monitoring allows the SMC to check whether the network or a server is up or down, to check the general health of the network in terms of parameters such as packet loss and to view all log files. Basic monitoring could also cover server metrics such as hard disk usage, CPU and memory usage. Incidents detected by this basic monitoring would then be entered into the Call Management system, allowing them to be resolved via the defined incident and problem management process.

Beyond the basic level, proactive monitoring and maintenance provides "value added" services to the managed service environment. Examples of proactive services include trends monitoring, automated responses to given conditions, net patches/service packs firewall monitoring for intrusions and input to the call logging system when required.

(c) Customer System Backups

Backups should only be provided for Managed Services. Furthermore, in order to be effective, it is essential that any backup solution deployed is capable of backing-up files and tables that may be open at the time the backup is made.

Backup strategies like Full, Incremental and Differential, as well as backup media rotation methods like Grandfather-Father-Son method (Veritas 1999) should be employed to ensure an effective backup job. Weekly, monthly and yearly backup media which are not recycled / reused within the period called the backup horizon, should be stored off-site away from the Internet Data Centre at a safe place.

(d) Storage Area Networks

Storage Area Network (SAN) is a relatively new approach of backing-up data in the Internet Data Centre environment. SANs are based on a network of fibre channels to facilitate high speed and switches connecting storage devices (i.e. disk arrays, optical disks, tape libraries) to servers on a many to many basis. This solution offers a number of advantages:

- Facilitates universal access and sharing of resources
- Support unpredictable, explosive information technology growth
- Provides affordable 24x365 availability
- Simplifies and centralises resource management
- Improves information protection and disaster tolerance
- Enhances security and data integrity of new computing architectures

(e) Network Attached Storage

Network Attached Storage (NAS) provide similar facilities, but the key difference between NAS and SAN are:

- SAN enable multiple servers to share central Fibre Channel RAID (Redundant Array of Independent Disks) storage for higher performance, lower management cost and provide unlimited capacity growth. SAN usually have dedicated network connectivity

- NAS provides direct Ethernet attachment of RAID storage without any disruption or downtime to existing servers

(f) Problem Management, Configuration Management and Change Control
Problem Management, through the implementation of a Call Management System (CMS), enables the Service Management Centre to log, track and resolve incidents either as they occur or as customers report them.

Through the implementation of a Configuration Management Database (CMDB), an Internet Data Centre can baseline build configurations (hardware, operating system and software) of all managed services. Updates and changes to individual configurations can be tracked.

Change Management enables correct logging and implementation of hardware and software upgrades, changes to the operational parameters in the Internet Data Centre and changes to monitoring services. This ensures that there is minimal impact on current services or to customers.

3.6 Internet Data Centre Services

The two fundamental services offered by Internet Data Centres are managed services and co-location services. Nowadays, customised services are also provided to cater for the various needs of the customers. There are web hosting, e-commerce hosting, database hosting, VPN secure web hosting, dedicated hosting and so on.

(a) Managed Services
Managed services are dedicated server products built to defined standard and offering a Common Operating Environment (COE) – standard operating system, standard network management, standard monitoring tools. Managed services are monitored and maintained in-house by the Internet Data Centre's own technical and support staff, with a complete maintenance and support contact. Reporting is provided to alert customers of any events and to respond to any calls for assistance from the customer.

(b) Co-location Services

Co-location is the provision of racking space, power and network connectivity (frequently referred to as "power, ping and POP") to servers supplied by the customers. The attraction to the provider is that co-location offers relatively straightforward revenue generation against a minimal outlay. However, in order to be effective, co-location services must be supplied on the following basis:

- All switches and network management equipment for the co-location systems should be owned and managed by the Internet Data Centre
- Customers are responsible for installation and management of the equipment in the racks
- Services are governed by a clearly defined "Terms and Conditions Contract" which clearly specifies the extent to which the service is being supplied, the limitations of liability and the support and reporting from the Internet Data Centre to the customer

These services could be differentiated by identifying the providers of each of the components, namely the facilities, network, servers, operating systems, management and applications, as shown in Figure 10 below:

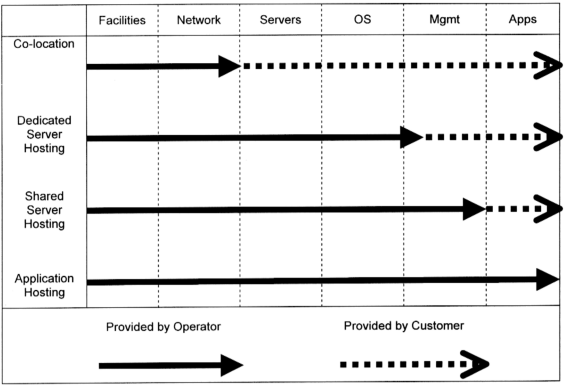


Figure 10 : Differentiating iDC services (Source : EIX presentation slides)

IDC categorise Internet Data Centre services into two types as follows (IDCAP 2001):

(a) Outsourcing services.

When delivered as an outsourced service, iDCs manage customer-owned or leased systems (increasingly vendors are also choosing to own these systems.). Under these conditions, the iDC takes responsibility for managing customer IT and network systems (the computing infrastructure) based on customer-defined SLAs (service level agreements). This type of service is generally billed on a monthly or fixed-fee basis.

(b) Utility-based services.

When delivered as a utility-based service, the iDC owns the infrastructure and essentially leases back to the customer IT/network capacity. An example of utility-based services include enabling ASPs/ISVs to deliver ASP services;

provisioning for server-on-demand or infrastructure-on-demand. Typical characteristics of a utility-based service include:

- Delivery of IT capacity from a location other than the customer site back to the customer
- Ownership of some or most of the IT and/or network infrastructure by the utility provider
- Remote delivery of services typically associated with IT equipment
- Pricing and payment plans that resemble traditional leasing agreements in some respects (i.e., a "pay-as-you-go" program)

IDC listed further specific activities provided by Internet Data Centres as the following:

- *Consulting services.* Architecture system/site design; security assessment; capacity planning; operations assessment; strategy and planning; change management; network (e.g. LAN/WAN, VPN) design
- *Integration.* Network provisioning; remote system administration setup; change control; load balancing setup; database setup; backup and restore setup; application monitoring setup; security installation; performance tuning and measurement; scalability and load testing; site integration and stress testing; system deployment; systems integration (O/S, middleware); site preparation; system configuration; relocation services; system migration; server consolidation
- *Operations.* Account management; program management; change control; systems administration; storage management; systems monitoring and management; automatic tape backup and restore; network management; data center connect; backbone connect; VPN; database administration; dedicated caching; network caching; problem management; fault management; performance management; configuration management; load balancing; asset inventory and control/management; security management; technology refresh/migration; backup and recovery services; content

management and distribution; fail-over services; help desk management; procurement and deployment, data center management

- *Monitoring.* Systems health monitoring; Web/application/database server monitoring; application monitoring; network monitoring; database monitoring; remote monitoring; cross connect; applications monitoring (e.g. systems software – HP OpenView; business applications – ERP, SCM, CRM)
- *Reporting.* Capacity planning; systems performance; network (bandwidth)
- *Provisioning of hardware/software.* Provisioning and support of both hardware (e.g. routers, hubs, servers) and software (e.g. O/S, middleware)

3.7 The Internet Data Centre Market

Mentioned earlier in the report, research figures from IDC indicate that the global trend is heading towards outsourcing, with Asia-Pacific leading the fastest growing regions in this area, increasing by 20% annually between 2000 and 2005. More specifically in the iDC market, IDC predicts that the Asia-Pacific iDC market will grow from US$713 million in 2000 to exceed US$3.3 billion in 2005 (IDCAP Press 2001). The reason quoted was that it was mainly fuelled by the regions' healthy demand for outsourcing and utility services. According to IDC, Australia, Singapore and Korea look set to dominate the market by 2005.

Massive opportunities actually exist for iDCs and potential entrants across the region. Companies in the communications, banking and finance and manufacturing sectors are driving the market, which will grow at a Compound Annual Growth Rate (CAGR) of 36% from 2000 to 2005.

Besides the traditional services powerhouses of Australia and New Zealand, investment and development of iDC have been occurring throughout People's Republic of China, India and Korea. Smaller nations like Singapore and

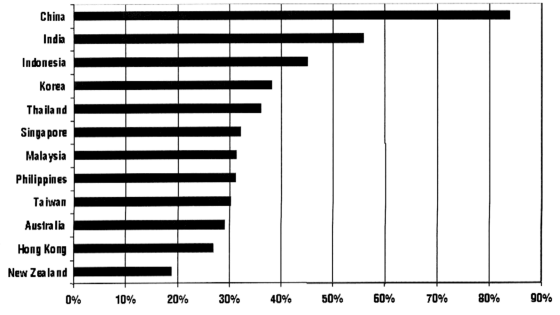
Malaysia are also developing strategies at a national level to ensure that they win a share of this marketplace. According to IDC, the CAGR for the Malaysian market is expected to be over 30%, as shown in Figure 11.

In IDC's opinion, the competitive climate looks set to change over the next few years. Small but nimble players are starting to give the leaders a run for their money by ranking in above-average revenues vis-à-vis the market. Consolidation is looming on the horizon and with regional economies on their descents into recession, some mergers, acquisitions and alliances are likely to take place over the period from the end of 2001 till the beginning of 2002.

A key trend observed by IDC is that the iDCs are managing the core infrastructure for customers on an outsourcing or managed services model. Most iDCs have a set of service offerings that designs, builds and operates the network and IT systems needed to support the ongoing performance of a business. In other words, more of these iDCs are providing services that manage customer systems on a dedicated and customised basis, as part of its competitive set of utility-based offerings.

While this growth, according to IDC, is creating significant opportunities for vendors in the marketplace, no one player can lay claim to market dominance across the region.

Figure 11 : Compound Annual Growth Rate (CAGR) of Internet Data Centers in Asia/Pacific (ex. Japan), 2000 to 2005 (Source : IDC 2001)



Looking at the Malaysian scenario specifically, majority of the companies (60% of 213 respondents) said that the Internet has impacted the way they do business today either moderately or completely changed their businesses (17%) (IDCAP 2001).

The above figure tends to also suggest that these companies are receptive to the idea of using the Internet to do business. IDC found that Malaysian companies are very open to the concept of using an iDC (IDCAP 2001). Although only 8% of companies are currently using an iDC today, a healthy 64% of them will consider using this type of facility in the future.

The perceived benefits of using an iDC were (in order of importance)

- less IT management
- cost savings
- greater reliability

Those that did not want to use an iDC felt that it was more appropriate to run their Internet applications in-house, or their hands were tied by their

headquarters' IT policies. Besides that, some felt that there was no need to change their existing infrastructure in place already in light of uncertainties of price.

A surprising finding indicated that only about 7% of those that did not want to use an iDC, is not due to the fact that they felt it was not safe. Compared with another finding in the survey, most companies believe that security will be somewhat reliable (38% of respondents) or no different (24% of respondents) from their in-house operations. Only 4% believed that it would be extremely unreliable and 16% believed it to be somewhat unreliable.

It was also learned that the top criteria for choosing a service provider is the security of their data centre, which according to IDC, shows that the Malaysian market perceives security can be managed just as well, if not better by the service providers.

The key accelerators for the increased trend of outsourcing to iDCs found to be relevant to Malaysia are those listed below (IDCAP 2001):

- The pervasive use of the Internet
- eCommerce growth despite the dot com bust
- Changes licensing agreements in the software industry
- SME participation in B2B as encouraged by the government
- Lowered telco rates

On the other hand, the inhibitors to the local market likewise are (IDCAP 2001):

- Use of iDCs overseas
- Vendors not used to working with iDCs
- The question of trust
- Lack of professional services skills in iDCs