



# Technical Operating Environment

Date: 09.09.2008

Prepared by: ICON

Email: [info@icon.com.mt](mailto:info@icon.com.mt)

Document Version: 2.9

## 1.0 About us

ICON is an innovative web application development company.

We have provided consistent, results-oriented technology for the business community for almost a decade. Our approach is driven by the **passion** to transform complex business strategies into simple and accessible online encounters. It's no accident that time and time again, clients have described our work as: remarkable, clever, fresh.

ICON is a **Microsoft Gold Partner**. This status represents a high degree of competence and expertise with Microsoft technologies and offers you the confidence of reliable, standards-based proposals.

Our clients come from a broad range of industries giving us the opportunity to work in different industries and markets. Some of our satisfied customers are shown below, further details can be found in our [online portfolio](#).



## 2.0 Overview

Our business has always been about our customers. This means that our creative solutions are based on a sound technical infrastructure which is robust and reliable.

Not merely on a software level, but also in terms of hardware platform, we offer a comprehensive technical infrastructure configured for high-end performance. Our **dedicated data-centre** is based on a multi-tiered enterprise class network that provides security, performance and reliability. Our data centre's infrastructure comprises of:

- Quad Core Dedicated Servers
- Bandwidth redundancy via multiple peering partners
- Triple data redundancy and daily backups
- Enhanced Traffic management
- Enterprise class routers and switches providing state-of-the-art scalability and management
- Enterprise class firewalls, intrusion protection systems and anti-virus protection
- Internal network is 100% hardware redundant
- Physical security including biometric identity verification, zoned access and 24/7 monitoring
- Complete data centre systems redundancy including zoned cooling, power and fire suppression and early-warning systems.

We have engineered our data centre like no other with every facet of our network scalable to gigabit speeds with no single point of failure. We have an almost unlimited amount of bandwidth available to us since our data centre lies on a fibre-network within GO's network.



## 3.0 Network

Our network provision is via Malta's largest telecommunications operator: GO (formerly known as 'Maltacom'). GO's Gigabit network consists of high-end service provider equipment. Through this network, GO offers Ethernet over Fibre services to its customers. The network is made up of core networking elements as illustrated below. The switching fabric consists of various Cisco Catalyst switches for termination of Ethernet over fibre services. Routing is done through two Cisco fully redundant routers, running an MPLS backbone. GO's network is also connected to the core, through separate Catalyst switches.

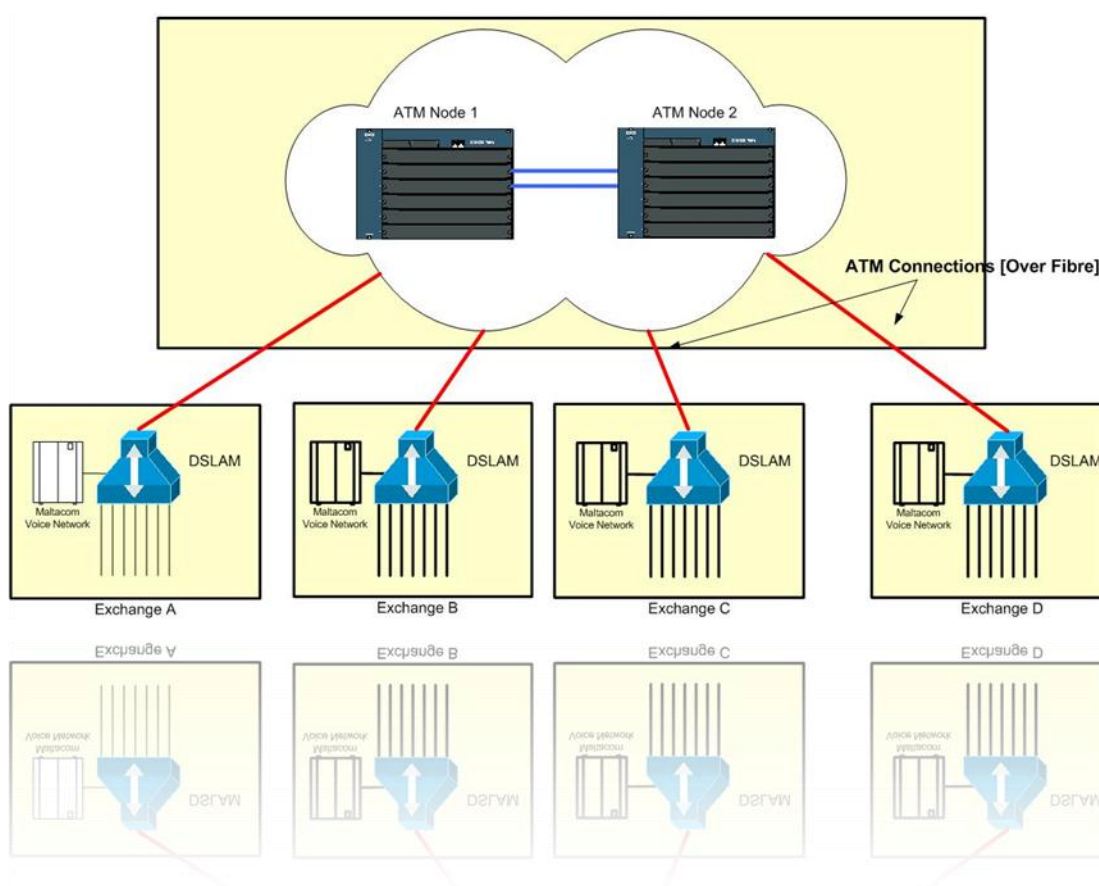
Services for different customers are segregated through the use of VLANs and IP MPLS. This ensures that the offered service is secure and that customer data is switched only over the allocated links. The underlying technology is Multiprotocol Label Switching [MPLS], which provides great flexibility in the provision of service for large provider networks. Moreover the technology further enhances the security already inherent to ADSL and fibre networks.

The connections between the various switches and the two core routers are fibre connections provided at Gigabit speeds. Enough capacity is available to ensure that each customer is guaranteed the bandwidth purchased. Upgrading of these links can easily be achieved if necessary through the use of technologies such as EtherChannel.

### Our ATM Network

The ATM backbone provides fibre-based connectivity to end-customers based on ATM technology, utilizing a fully resilient platform. All DSLAMs, which provide ADSL connectivity and are located within the GO exchanges, are connected to this resilient switch technology.

The ADSL service is provided over a dedicated copper link to the exchange. Data and voice traffic are carried over the same line up till the concentrator in the nearest exchange. The concentrator or DSLAM [Digital Subscriber Line Access Multiplexer] aggregates multiple ADSL lines onto an ATM fibre link. It also separates the data traffic from the voice traffic. Data traffic is sent towards GO's ATM network whereas voice traffic is routed to GO's network.



## Network Security

Network security is inherently built in our product portfolio. Fibre based services are carried over a fibre based network all the way from the remote sites to the central Head Office. This guarantees excellent reliability and technical performance. These services have a reduced chance of failure due to the fact that the underlying fibre infrastructure is a robust medium. Fibre is an inherently secure and reliable medium for data transmission. In addition to this, the cabling involved is primarily underground, hence protecting the cable from environmental interference and damage.

Moreover since data over fibre is transmitted in the form of light waveforms, it is not prone to interference. It is also not possible to tap into the fibre and eavesdrop on user data. Thus the technology is inherently much more secure than copper or coax based solutions.

ADSL based services are provided over dedicated telephone lines which are installed between the customer premises and the nearest point of presence usually situated in the nearest exchange. This dedicated feature of the ADSL service immediately implies that others do not share the connection between the remote sites and the central site. Moreover, this enables GO to guarantee the data rates that one opts for and dedicate the bandwidth to the particular ADSL line.

## Network Scalability

Since flexibility is inherently built into the network design, the rollout of services to a new site is achievable with very short lead times due to the extensive presence of the Fibre/Copper infrastructure virtually anywhere in Malta and Gozo. No changes need to be done to the existing infrastructure in order to accommodate any new connections.

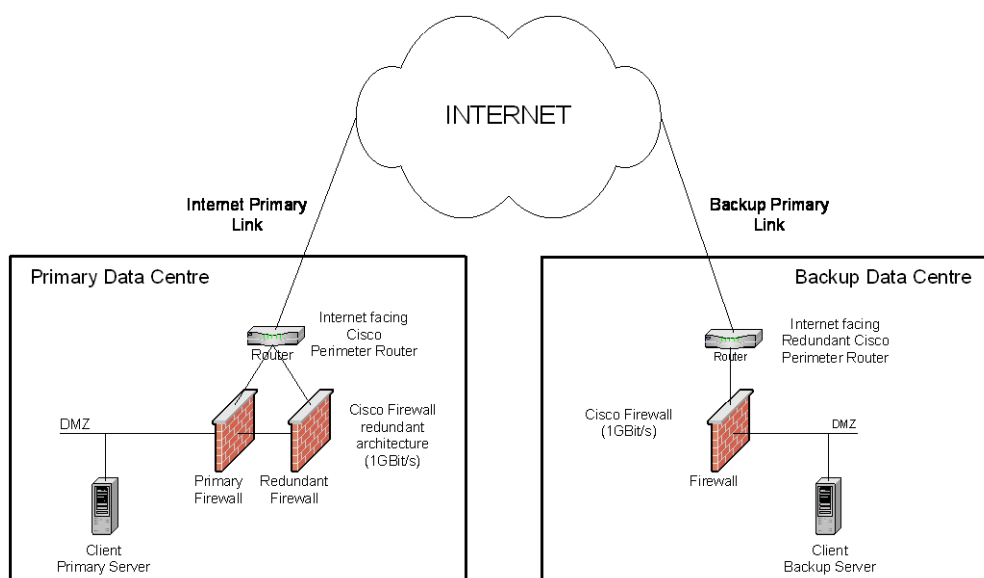
## Data centre and internet connectivity

Our data centre's are directly connected to the GO fibre network. Multiple fiber connections are available at each of the company's data centres so as to provide the capacity as well as the level of resiliency required. Different fibre routes are utilised in order to provide alternate path routing in the case of fibre cut-outs.

Access to the above mentioned Gigabit network is *sine qua non*. We run two data centers which host a variety of application servers and which provide connectivity from the GO network to the internet. Both data centers have routable IP networks that co-exist on the Gigabit network and as such both networks may host independent servers at the same time.

A "floating network" design has been implemented to satisfy the requirements for these data centers to have network redundancy, i.e. for the same IP address to move from one data center to another in a seamless fashion, given that the same IP address may only appear at one data center at any point in time.

This floating network model is the recommended procedure to achieve server redundancy. The main network components are the CISCO Catalyst 6509 (as a main Layer 2 switch and Layer 3 router), the CISCO 3725 (as a Layer 3 router) and the CISCO PIX 535 firewall. The above components together comprise the key security devices protecting the data center from the internet.



## The Perimeter Router

The CISCO perimeter router is used to connect the data center infrastructure to the internet. Full redundancy is available between the two data centers, since perimeter routers are installed in both the primary and backup data centers. The routers run Border Gateway Protocol (BGP) to ensure proper and fast routing. The routers are capable of enforcing traffic policies, and are used to help secure the perimeter network as well as add an additional layer of security. These routers are also used to guarantee any QoS policies our clients may wish to enforce.

## The Firewall

Apart from the perimeter router, a CISCO PIX firewall is used to implement and maintain the required security policies within the data centre. With its 1Gbit backplane, the PIX is capable of delivering high security to fast performing corporate networks. The PIX firewall provides full firewall protection and conceals the internal network from any external networks as well as to the Internet from within existing private networks.



The CISCO PIX provides stateful filtering, a secure method of analyzing data packets. It also provides sequence number randomization so that it makes the process of guessing TCP sequence numbers extremely difficult, in the case of spoofing attacks. The PIX also makes use of a secure, real-time embedded operating system, which has been extensively tested for any operating system flaws. The internal operating system is specifically designed for secure high-performance protection. It intercepts new session setup requests for common TCP/IP Internet services (e.g. HTTP, FTP, TELNET etc.)

The PIX adaptive security algorithm (ASA) and cut-through proxy allows the PIX to deliver outstanding performance for more than 256,000 simultaneous connections. The CISCO PIX also enhances the security of the data center by supporting important features such as:

- Intrusion Protection Guards Against Popular Internet Threats
- Fail-Over to Guarantee Maximum Business Uptime

The Cisco PIX also provides stateful failover capabilities that ensure resilient network protection for enterprise network environments. Employing a cost-effective, active-standby, highly available architecture, the Cisco PIX is configured as a failover pair. Connection state synchronization takes place over a high-speed 1Gbit LAN connection, providing another layer of protection through the ability to geographically separate the failover pair. In the event of a system or network failure, network sessions are automatically transitioned between the firewall pair, with complete transparency to users.

## Network Architecture Design

The network architecture of our data center is flexible because it uses VLAN technologies to isolate servers and control communication traffic. A number of VLANs are setup to isolate and provide different network sub-nets required for the internet setup within the data center. These VLAN sub-nets are used to host the data centre's and the client systems and consequently to connect such systems to the internet, through the CISCO PIX.

Of particular relevance to are the following VLAN zones:

- The internet zone
- The management zone
- The anti-virus zone
- The backup zone
- The DMZ

Each zone can host a number of multi-homed web applications / servers that users can query directly from the Internet through the internet perimeter router and firewall. The VLAN architecture allows traffic flow to be managed efficiently by creating a series of protected security devices to which rules and policies can be applied by the PIX.

The management VLAN hosts a number of network and server management systems including HP Openview, Cisco Works and the Cisco ACS authentication server.

## Network Availability

Network availability is achieved by providing redundancy at every level and by using automatic failover:

- The VLAN switch is a fully redundant CISCO switch
- The CISCO PIX is setup in a fail-over fashion, such that if the primary firewall fails, a backup firewall takes over maintaining all client connections active
- Should a customer opt to make use of our secondary / backup site, then as soon as the internet connection to our primary data center fails, all internet traffic is automatically re-routed to our secondary / backup data center.

## Network Security

The core of the security architecture is the Cisco PIX firewall, with its 1Gbps back plane, hot standby and ASA algorithm. These elements allow the network to achieve high levels of availability and resiliency.

In addition to the above ICON provides for higher levels of security with the introduction of an Intrusion Detection Module installed in our switches. This IDS module is designed specifically to provide security and flexibility to monitor traffic flowing through the Cisco Catalyst series switches throughout the network. The IDS module can help identify denial of service attacks including the distributed denial of service attacks (DDoS). Apart from the high level of security achieved through this IDS module, the switch offers 100% redundancy with dual supervisory engines and redundant power supplies.

# 4.0 Infrastructure Specifications

## Fire Detection and Protection

- Very Early Smoke Detection Apparatus (VESDA) with sampling taken from equipment area, raised flooring void, false ceiling void and air conditioning return ducts
- Smoke and fire detectors installed in equipment area, raised floor void and false ceiling void
- Argonite flooding system
- CO2 manual fire extinguishers

## Air Conditioning System

- Close Circuit Units in an N + 1 hot redundancy configuration with temperature and humidity control
- Cold air distribution trough raised floor plenum (all cables are plenum grade)
- Filtered fresh air blower will provide positive pressure inside equipment room
- Upon fire detection, air conditioning units will shut down and fire dampers in fresh air ducts will be activate. Argonite flooding will then be activated in equipment area, raised floor and false ceiling voids with a minimum holding time of 30 minutes

## Access Control

- Both the main and back-up data centres are provided with a network-dedicated area and server dedicated area. Access to both areas is individually controlled
- Biometric access control to the individual areas
- CCTV with continuous recording on all doorways to equipment rooms
- All access doors status will be connected and monitored through an on site system and an off site central system
- Security guard on site on a 24/7 basis



### Intrusion Detection

- Intrusion detection infrared and microwave towers are installed along the perimeter around the main building
- CCTV with zone event triggering installed around the perimeter

### Power Supply

- Dual redundant distribution system (Dual power bus bars at main data centre)
- Scalable Modular UPS system in an N + 1 hot redundant system
- Standby by generator to supply UPS, Air Conditioning Units and lighting
- 1 hour UPS battery back-up to provide smooth shutdown in case of generator failure
- On site sub-station
- Planned 2nd standby generator
- The system is designed with a dual distribution system, in order to be eventually fully upgraded to a fully hot redundant Power Supply Chain, i.e. dual generators, dual modular N+1 UPS systems and a possible a second sub-station. All servers are equipped with a fully redundant (N+N) power supply system.