ZYBERT Computing Ltd.
Innovation Centre
Longbridge Technology Park
1 Devon Way
Birmingham B31 2TS
Tel: +44 (0)121 222 5457
http://www.zybert.co.uk

# Z1 GEM Reviewer's Guide

Richard Zybert, Zybert Computing Ltd
3rd November 2014

Z1 GEM is the latest implementation of the Z1 Microframe server designed by Zybert Computing Ltd as a self-contained network and security appliance for small businesses. Z1 GEM is based on a mini-ITX motherboard, SATA disks and is designed to serve a small (about 20 workstations) group of users in an average office environment.

The system uses Linux kernel and Open Source tools in addition to data security system called TripleA™ developed by Zybert Computing specifically for the Z1 series. Use of Open Source software not only does away with license issues and costs but provides a solid development and production platform, high security, stability and performance.

TripleA™ stands for 'Advanced Automatic Archiving' and encompasses a range of technologies assembled and configured in order to provide a safe, 'near zero maintenance' system to handle data for a small (micro) business, a small group etc.

## 1 Introduction

The general design of the system stemmed from a market research performed by Zybert Computing where a number of micro businesses were approached with questions concerning their IT priorities. The set of answers revealed that micro businesses had a very well defined set of requirements, in many cases very different (and not necessarily lower) from larger organizations. The different set of priorities is a result of a different business structure in terms of business model, staff and business practices. One of the issues mentioned most was the lack of dedicated, experienced IT personnel and difficulties in managing the network systems that resulted from this. It appears that most of the other problems were simply the result of this simple fact. In particular most small businesses were worried about possible data loss due to lack of well defined and consistent backup and archive strategies.

Therefore the design of the system dedicated for micro-businesses had to start from the basic premise that the system must be able to work with almost no intervention. However – this should not preclude the system offering high class, sophisticated services. The system has been designed to provide all essential networking, security, file sharing and email handling services, to provide high level of data safety suitable for the size of the business we were targeting.

TripleA™ system covers the following areas:

- Fully automatic disk-to-disk backup system of all system, configuration and user data files.
- Archive system that provides a daily versioning structure, preserving previous versions of all changed files.
- Email archiving to 'Write Once' structures.
- Fully automatic checks and monitoring of the system functionality and health.
- Multiple levels of recovery – from previous copies of data files, to fully operational, bootable copies of the system disks.
- Exceptional level of support – including remote monitoring and interventions.

All these functions are achieved without any need of local administrator to intervene – the functionality is present on power up and requires no set-up or configuration. For advanced applications the system is fully configurable and many of the functions may be extended or modified.

- Research shows that about 70% of the data losses are caused by human or software error. This ranges from a user simply deleting a file by mistake to a program corrupting its database. In most situations the user quickly notices a problem. TripleA™ provides immediate access to the last backed-up version of the file. There is no 'recovery process' – the files are accessible and can be copied into place immediately.
- Sometimes the damage to the files is not visible immediately, the backup disk may be affected before it is realized that the files are corrupted or missing. The archive system allows immediate access to previous versions of all files. Fast, index based search allows the user to find all versions of needed files and the selected versions can be simply copied into place.
- Remaining 30% of data loss, according to statistics is a result of hardware failure or physical damage to the storage equipment.

ZYBERT Computing Ltd.
Innovation Centre
Longbridge Technology Park
1 Devon Way
Birmingham B31 2TS
Tel: +44 (0)121 222 5457
http://www.zybert.co.uk

## 2 Technical Specifications

| **Hardware** | |
|---|---|
| **CPU** | 4GHz Quad Core 64 bit Intel i7 CPU |
| **Memory** | DDR3 16GB/1600MHz |
| **Networking** | Two 1000Mb/s interfaces |
| **USB** | Six USB2 sockets |
| **Disks** | Two SATA, 7200rpm disks (up to 2000GB each) in hot swap enclosures. One off-site disk in protective carrier. |
| **Power** | Internal 200VA PSU |
| **Cooling** | Total of 5 cooling fans |
| **Hardware monitoring** | Disk temperature and fan status monitored independently on each disk. System temperature and fan status monitored by firmware. |
| **Size** | W:225mm H:225mm D:310mm |

| **Software** | |
|---|---|
| **Operating System** | Linux 2.6 |
| **File Sharing** | CIFS, NFS, WEBDAV, SCP |
| **Configuration** | WEB Interface |
| **WEB Server** | Apache 2.2 with SSL,PHP4,Python,CGI,WEBDAV,Virtual Hosts |
| **Virtualization** | KVM-qemu |

| **Networking** | |
|---|---|
| **General** | Two-way router with firewall and NAT |
| **WAN Configuration** | DHCP client or manual |
| **LAN Configuration** | Manual |
| **Firewall** | Stateful Packet Inspection, fully configurable |
| **NAT** | Configurable network address translation and port redirection |
| **DHCP** | Client on WAN, Server on LAN |
| **DNS** | Master DNS server |

ZYBERT Computing Ltd.
Innovation Centre
Longbridge Technology Park
1 Devon Way
Birmingham B31 2TS
Tel: +44 (0)121 222 5457
http://www.zybert.co.uk

| **Email** | |
|---|---|
| **SMTP** | SMTP server with virtual hosts, mail filters, SSL/TLS security, authentication |
| **POP3 Server** | SSL security enabled |
| **POP3 Client** | Downloads email from external mailboxes. Configurable mail filtering before download. Handles 'multi-drop' mailboxes. SSL enabled. |
| **IMAP** | IMAP4 server with SSL/TLS |
| **WEBMAIL** | IMAP and SMTP based. |
| **Antivirus** | Filtering all emails before delivery, regular disk scans, virus database automatically updated. |
| **Anti-SPAM** | Filtering all incoming mail, tagging or stopping emails when SPAM is detected. Can be customised for individual users. |
| **Email delivery** | Automatic delivery to local mailboxes, mail aliases and lists, configurable delivery filters, shared mail folders. Server side filter rules. |
| **Email archiving** | Automatic archiving of all emails in WORM structures, immediate access to full archive with IMAP clients including secure WEBMAIL. |

| **Security** | |
|---|---|
| **Firewall** | Stateful Packet Inspection, fully configurable |
| **Secure Shell** | SSH server providing SSH1,SSH2, SCP and SFTP protocols. Public/Private key authentication. |
| **Secure HTTP** | SSL enabled WEB server |
| **Email security** | SMTP, POP3 and IMAP over SSL |
| **SSH tunneling** | SSH tunnels allow secure/encrypted remote access to any port/host on LAN based on Public/Private key authentication. |
| **File access** | Shared and private file shares, Role Based Access Control. |

| **Backup and Archival** | |
|---|---|
| **Control** | TripleA™ system |
| **File Backup** | Daily automatic disk-to-disk synchronization. Includes system and configuration making backup disk bootable copy of the main disk. |
| **Email** | Archives all incoming and outgoing mail in non-rewriteable files. |
| **Archival** | Files modified or deleted since last backup are archived with full version control. File retention policy may be applied for different types of files. |
| **Off site disk** | Backup disk is hot-swappable. A spare disk is provided to allow the backup disk to be moved off premises. The off-site disk is a fully working system disk and can be used in an off-the-shelf replacement server. |
| **Recovery** | Each of the three disks contains the full copy of the system, data and configuration. The system can be rebooted from any of the disks. If the server is not available, the spare disk will boot in the replacement server. |

| **Databases** | |
|---|---|
| **MySQL Server** | |
| **PostgreSQL Server** | |
| **Groupware Tools** | |
| **CRM** | SugarCRM, eGroupware |
| **General Groupware** | eGroupware |
| **File Sharing** | Samba3, Pydio |
| **Calendar/Contacts sharing** | CalDAV, CardDAV via eGroupware |
| **Document Management** | Subversion via WEBDAV |

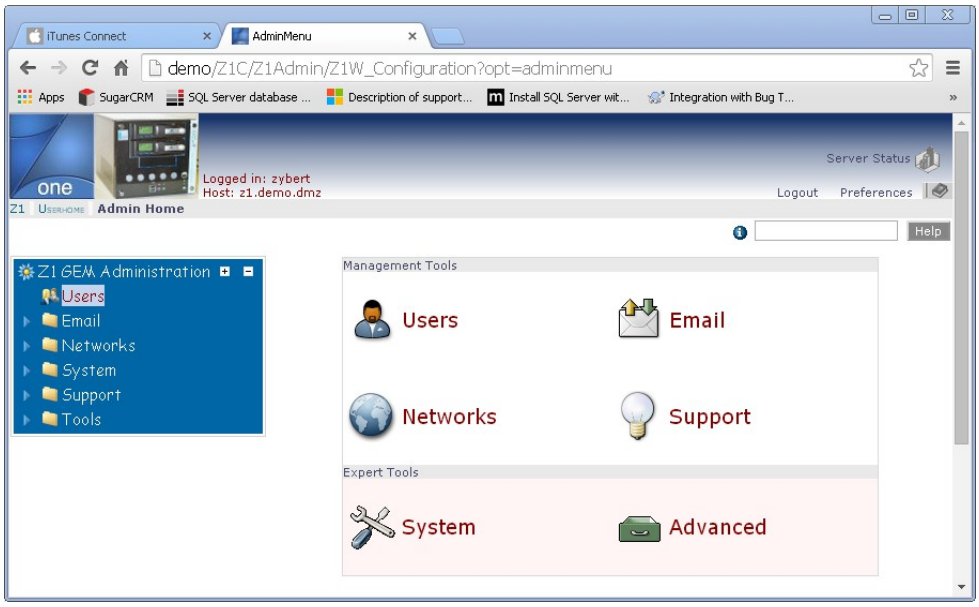
| **Compatibility** | |
|---|---|
| **File Sharing** | CIFS, NFS, WEBDAV, Compatible clients: Windows 98/NT/2000/XP/Win7/Win8, MAC OSX, UNIX, Linux, Android, IOS |
| **Configuration** | IE, Mozilla Firefox, Chrome |
| **WEB Server** | HTTP, HTTPS/SSL, WEBDAV, SVN |
| **Email** | SMTP - SSL/TLS security and authentication<br>IMAP4 - SSL/TLS security and authentication<br>POP3 - SSL/TLS security and authentication |
| **Time server** | NTP |
| **File access** | SCP, SFTP, FTP |
| **Shell access** | SSH1, SSH2, Telnet |
| **Name Server** | DNS Master |
| **Workstation configuration** | DHCP |

ZYBERT Computing Ltd.
Innovation Centre
Longbridge Technology Park
1 Devon Way
Birmingham B31 2TS
Tel: +44 (0)121 222 5457
http://www.zybert.co.uk

# 3 Administration and Monitoring

Z1 administration is reduced to absolute minimum, although *advanced* options allow the expert user to gain a full control over the system.

All administration is performed via WEB interface and can be performed from any WEB browser on the LAN. (Access to administration functions from WAN is enabled, usually using SSH tunnels).




The main administrative functions involve adding/removing/modifying users, setting email aliases and filtering, control of firewall and configuration of user remote access.

Administrators can also create network 'Shares' and control access to them. Each share is owned by a group. Users can be made members of a group by the administrator – this gives them access to files stored by the group. Each group may have a shared mailbox, shared calendar and shared Subversion repository

# 4 Backup

Disk-to-Disk backup has been chosen as a preferred option for the following reasons:

- To minimise human intervention. All used disks are the same size, which guarantees that the full copy of the source disk can be stored on a single backup disk.
- To allow immediate access to backup files – via file sharing on a read-only mounted disk
- To achieve maximum speed.
- Backup disks can be used immediately to boot and run the system.
- Disk synchronising system allows the end-user to migrate easily to larger disks when the system requires it, it is also easy to add more disks to the scheme for security or long term storage.

The system is delivered equipped with two internal hard disks (up to 2000GB) in removable enclosures and a third identical disk with a strong carrying case.

The journalling file system is used on all disk to minimize risk of data corruption in cases of sudden power cut-off etc.

One of the internal hard disks is used as a *Master* disk where all system and user data are stored. The second disk is designated as a *Backup* disk and is normally not used (although it is continuously accessible in *Read-Only* mode).

Once every 24 hours (usually at night) a daily backup is scheduled by the system. The backup system synchronises the *Backup Disk* to be identical to the *Master Disk*. During this process all files that are about to be deleted or modified on the *Backup Disk* are archived first. The archive resides on the *Master Disk* and is copied to the *Backup Disk* as all other files.

After this process is finished, the two disks are identical and each is bootable and fully functional. A hardware crash or corruption of the main disk requires a reboot from the *Backup Disk* in order to return the system to full functionality (although changes to files made since the last daily backup may be lost – depending on the damage sustained by the main disk).

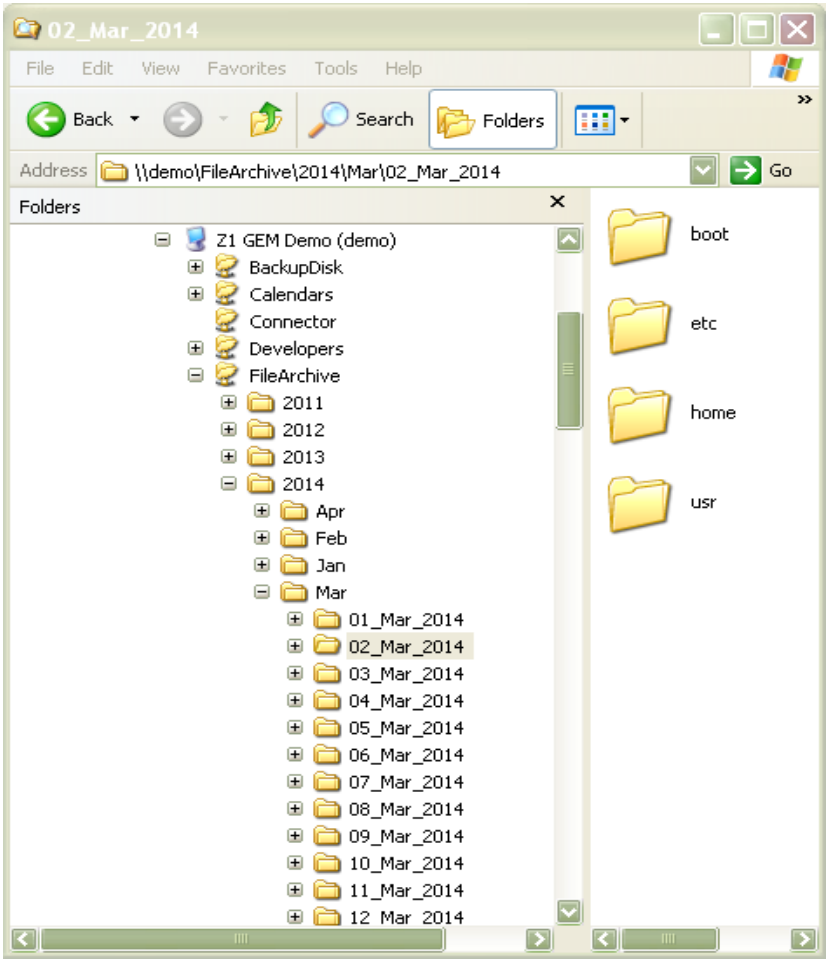
All files from the last backup time are 'frozen' on the *Backup Disk* and are accessible *read-only* without any special arrangements. Any damaged or deleted file on the main disk can be immediately replaced by the 'last-night' version from the *Backup Disk*.

The backup disk can be removed from the system at any time (except during backup) and replaced by the third disk. The disk should be then taken off the premises. The disk will boot and work without any additional action in any Z1 Server model.

Each daily backup run performs basic checks of the backup disk. A short report is then emailed to a nominated account (usually a 'system admin' or a support person). If necessary error information in the report can be easily detected, for instance by the email client or by a special script.

# 5 Archive

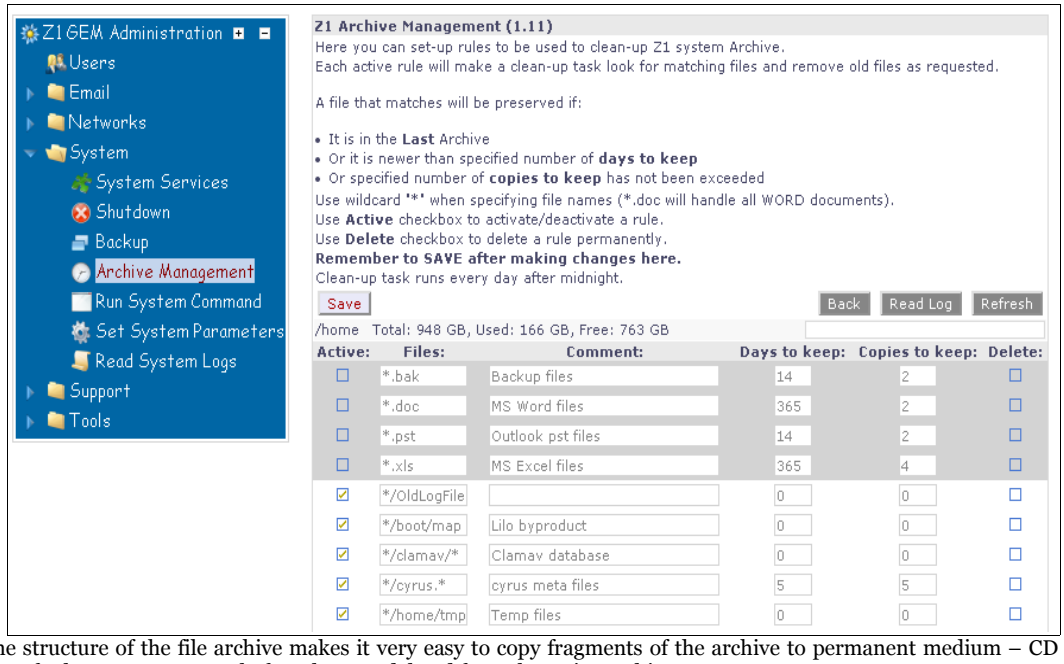
Each file that is about to be deleted or modified on the *Backup Disk* during the daily backup run is archived first. The archive structure provides the complete folder tree for each day. Additionally the month/year structure is constructed for easy access.




The archive is indexed every night to provide fast search capability. The user can easily display a list of versions on an archived file, select the require version and copy it from archive to their working space.

In order to control the disk space requirements a special tool is provided to set-up retention policy for archived files.

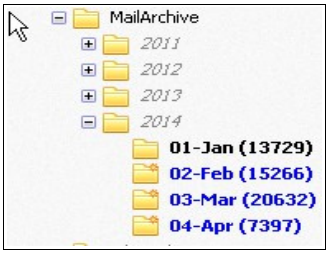
ZYBERT Computing Ltd.
Innovation Centre
Longbridge Technology Park
1 Devon Way
Birmingham B31 2TS
Tel: +44 (0)121 222 5457
http://www.zybert.co.uk




The structure of the file archive makes it very easy to copy fragments of the archive to permanent medium – CD or DVD for long term storage, before they are deleted from the active archive.

A combination of Archive system with the disk-to-disk backup allows the state of the archive to be 'frozen' on a backup disk that is then permanently removed from the system for long term storage. The archived (as well as other files) can be then deleted from the running system and can be easily restored from the 'archive' disk. The 'archive' disk may be inserted into 'backup disk' slot or it can be used in an optional USB2 based external enclosure.

## 6 *Email Archive*




All email (incoming,outgoing and internal) is archived by the system.

The mail messages are stored in standard mail folders, allowing authorized access with most of email clients and systems.

All archived emails are stored in monthly folders and are immediately available. Authorized persons have immediate read-only access to the archive (segmented into *year/month* structure) – using IMAP protocol with any email client (or built-in secure WEBMAIL system). Secure remote access to IMAP is also provided.

The mail archives – like all other files are backed up overnight and are write-protected on the backup disk. Just like File Archive, email archives can be easily copied to a permanent storage media.

ZYBERT Computing Ltd.
Innovation Centre
Longbridge Technology Park
1 Devon Way
Birmingham B31 2TS
Tel: +44 (0)121 222 5457
http://www.zybert.co.uk

# 7 System monitoring

Reliability is an essential component of the design in order to ensure low maintenance.

A range of automatic monitoring tasks are included, for instance:

- Hardware monitoring:
  - SMART disk monitor – checks health of the hard disk drives using internal disk firmware.
  - Temperature and fan status monitor – checks CPU temperature and status of system fans using built in motherboard control system.
- Software subsystem monitoring and control.

  All subsystems that provide services for users are continuously monitored by the system. If necessary action is taken to reset or restart subsystems that fail the monitor test. This monitoring includes all networking services.

  This monitoring system is easily configurable, new monitors may be added to the system by administrator.
- Functional checks

  Regular tasks performed by the system (like backup) perform their own hardware and software checks and report if necessary. In particular backup system performs file system check of the backup disk.
- Remote monitoring

  As a part of basic support contract a regular health check may be performed remotely by automatic tools. The resulting report is checked for early indications of possible problems (in particular the checks look at history of disk space usage for indications that the system may run out of disk space soon).

# 8 Recovery

Ability to recover is the essence of any backup or archiving system. TripleA™ includes multiple recovery levels providing appropriate systems for different situations.

TripleA™ provides immediate access to the last backed-up version of the file. There is no 'recovery process' – the files are accessible and can be copied into place immediately.

The archive system allows immediate access to previous versions of all files. Fast, index based search allows the user to find all versions of needed files and the selected versions can be simply copied into place.

All three (or more) disks maintained by TripleA™ system are bootable and fully operational. The system will start with any of them. A hard crash of the main system disk simply means that the system needs to be rebooted from the second or third disk. The state of the system and data will correspond to the last backup time (corrected by possible later 'snapshots').

As at least one of the disks is kept off site at all times – it provides means of quick recovery in more dramatic situations. If the whole server is lost (by flood, fire, theft or planes hitting buildings) – the off-site disk will boot the system in a new off-the-shelf server.

The recovery is full (to the state of the system at the time of last backup) and immediate. (The whole process takes less than 2 minutes).

In order for the *Recovery Plan* to be meaningful a mechanism to test the plan is required. TripleA™ maintained disk can be tested by booting the system from it. This can be done with the main disk removed from the server to guarantee that the system can be returned to the current state. Testing recovery requires as much time as is needed for the user applications to check their files. The consistency of the system files is checked during the booting process and takes less than 2 minutes.

# 9 Support

TripleA™ is dedicated to a provision of high level of data protection with virtually no need for administration and maintenance.

In order to handle unexpected issues ZYBERT Computing provides exceptionally high level of support. This level of support has been made possible because of a large number of tools and utilities specifically designed for support personnel. The automatic monitors and general reliability of the system also improves support efficiency, allowing us to provide more support within the limit of the support contract budget.

# 10 Advanced file handling

In addition to all basic subsystems protecting data, Z1 provides advanced file handling functionality for version control, security and remote access.

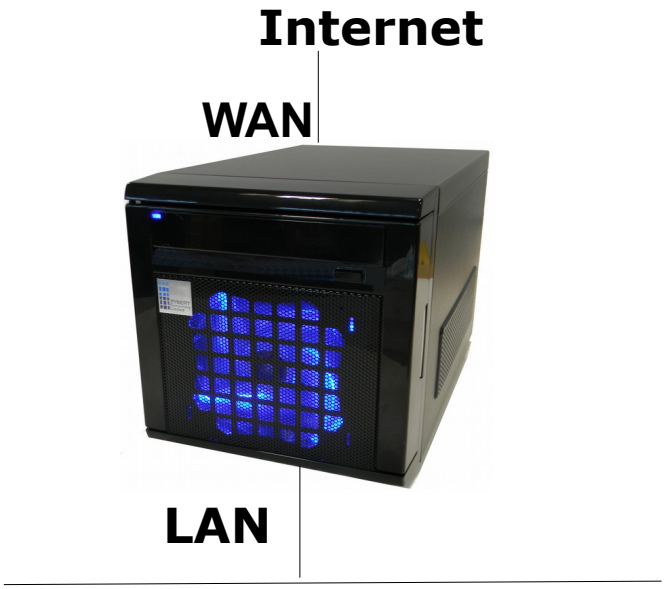
- WEBDAV file sharing system is available for remote, secure access (using Apache SSL)

- SVN file versioning system is installed. The files are stored in a database with full version history – the remote access is provided with Apache WEBDAB SVN module allowing complete folder trees to be 'checked out' to client machines and changes to be checked in. The system allows for different types of authentication and SSL security. Windows and MAC integration is provided by TortoiseSVN – open source, freely downloadable package.
- SCP and SFTP protocols allow secure, encrypted, public/private key based access to server files. Windows and MAC integration is provided by open source packages.
- The system has a provision for full audit of all file operations. This can be activated on a share by share basis as needed.
- Access control is implemented on several levels to allow great flexibility.
    - File permissions set by client programs are respected
    - Each share has an independent control of access.
    - Several pre-configured shares with different level of user access allow the system to be used without additional set-up. This provides for private and public shares with different level of access, shares with limited *write* access and general *read* access etc.
    - Role Based Access Control allows shares to be owned by groups. Users can be easily added or removed from specific groups thus controlling their access to shares.
    - Group shares may include sharing of email folders
    - WEBDAV and SVN systems allow additional levels of user authentication

## *11 Networking options*

Z1 is equipped with two network interfaces labeled LAN and WAN.

The most common configuration is to place Z1 between Internet access device (like ADSL router) by connecting WAN interface to the router and LAN interface to the local network. In this set-up Z1 may obtain its own WAN configuration from the router (as a DHCP client) – if available. Usually Z1 will act as a DHCP server for the LAN network. This configuration is active on a power up and may be modified later – usually with the initial set-up. Z1 provides Name Server DNS in a master configuration. In addition to the normal name resolution it provides aliases for itself and all LAN.



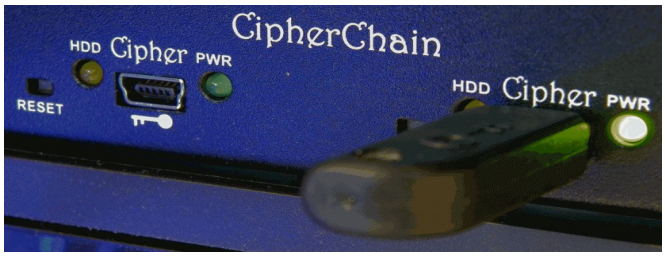
ZYBERT Computing Ltd.
Innovation Centre
Longbridge Technology Park
1 Devon Way
Birmingham B31 2TS
Tel: +44 (0)121 222 5457
http://www.zybert.co.uk

Z1 can also be connected as a 'client' on the LAN network. This is the choice Z1 is added to an existing network and it is not required to provide Internet routing. Z1 may obtain DHCP information from the existing DHCP server and will construct its own LAN, separated from the main network. This configuration may be useful to create self-sufficient sub-groups or department, giving them access to the main network and allowing them full control over their own LAN.


## 12 Security

Strong emphasis has been placed on data security in the system. Automatic backup, file and email archiving, powerful firewall and Role Based Access Control are all designed to protect data stored on the system.

Additional functionality is present in Z1 GEM/S version of the product. GEM/S version is equipped with hardware disk encryption module using external hardware keys and AES256 encryption to protect all the disks in the system. This makes all disks unreadable without the key containing AES256 encryption key.




The keys have to be inserted when the system powers up – the cryptographic key is read from the mini-USB key and stored in volatile memory. The keys are then removed and stored away from the server. When the backup disk is removed it is fully encrypted and cannot be accessed without the valid cryptographic key. If the whole system is stolen from the site, it cannot be booted and the disks are not readable without the keys. The encryption is transparent to the users while the system is running. All disks use the same encryption key and hot-swap of the backup disks does not require encryption key to be inserted.