



## Does My Business Need a Server?

### *White Paper*

Document Control	
Document	PLR03_WP-SRVR_DM01_13-01
Date Created	10/25/2002 12:25 PM
Version	1.00
Author	David Merry
Approved by	Gary Axten MCSE

**Table of Contents**

Does My Business Need a Server?..... 1  
    White Paper ..... 1  
        Document..... 1  
    Introduction ..... 3  
        Management Summary ..... 3  
Does an organization need a server or not?..... 3  
    How does a server help?..... 3  
    What are the benefits? ..... 4  
    What are the drawbacks?..... 4  
    Costs ..... 4  
    Technical ..... 5  
    General..... 5  
Appendix B..... 6  
    Glossary of Terms - Explanation of Services and Acronyms ..... 6  
        ADSL..... 6  
        DNS ..... 6  
        Firewall (stateful inspection) ..... 6  
        IMAP ..... 7  
        POP ..... 7  
        PoP ..... 7  
        SDSL..... 7  
        SMTP ..... 7  
        SMTP Feed..... 7  
        SNMP..... 7

**Commercial – In Confidence;**

**This document is released to individuals or organisations on a confidential basis.**

**It may not be passed to third parties without the written permission of the management of Polar Computer Communications Ltd.**

**The contents of the document may not be discussed in any way, with third parties without the written permission of the management of Polar Computer Communications Ltd.**

**© 2002 - This document is copyright Polar Computer Communications Ltd.**

**All Rights Reserved.**

**All trademarks are acknowledged.**

## ***Introduction***

### ***Management Summary***

This document is aimed at business managers that feel that their current stand-alone PC infrastructure may not be sufficient to meet the needs of their business or require additional information to make an informed choice to upgrade their infrastructure or not.

The document is intended to be vendor independent and looks to identify key features, as opposed to explain the differences between various server types and server services.

### ***Does an organization need a server or not?***

In a network, there are two basic methods of sharing data.

- Peer to peer networking.
- Client-server networking<sup>1</sup>.

In general the smaller a company is the more likely they are to use a Peer to Peer network and the larger a company is, the more likely Client-Server architecture will be employed.

The reason for this is that with Peer to Peer networking, it is very simple to allow others to share information on the hard-drive or use a printer that is attached to one's PC. The problem however is that the operating system of the PC does not have additional modules of software to control who is accessing what and tracking that information.

When there are only two users in an office, if someone accidentally deletes a file, it should be relatively easy to identify who did it.

When there are between five and ten users in an office, there may be the temptation for a user not to admit to a mistake that may mean someone else has to do more work to resolve the issue.

In most business scenarios, having between 5 and 10 PC users is the point at which a server would be appropriate. This may be lower where several users use a laptop as the data needs to reside on a central repository when a user is out of the office with a laptop.

### ***How does a server help?***

A server implements a number of functions that ensure ***data is protected and changes are audited***;

- Server software and architecture is typically more robust, leading to fewer failures.
- Users are required to properly identify themselves to the server before data can be accessed. Most Peer implementations do not authenticate users very well, if at all.
- Users can have different privileges assigned – for example; all may create documents, but only the office manager may delete documents.
- Data is all held on one device therefore;
  - ✓ It is simple to back data up and restore if required.
  - ✓ There is a reduced cost for providing fault tolerance.

---

<sup>1</sup> In very large organizations variations on the theme of client-server exists such as thin-client, host-based, and distributed computing environments. For the purposes of this document, it is assumed that these environments are not within scope, however close enough to client-server architecture to be considered under the client-server banner.

## polar computer communications ltd

- ✓ Only one device needs very strong physical security.
- ✓ Auditing whom accessed what, is possible when is centralized.
- ✓ Templates are held centrally, so everyone uses the same version.

A server also provides a central point of administration to ensure that;

- Software licensing can be monitored.
- Anti-virus software can be properly updated.
- Programmes, such as diaries can be shared.
- New users are added and leaving staff removed in one location.
- Security policy is enforced (e.g. password changes occur regularly).

### ***What are the benefits?***

The most important benefit (by far) is that the data is being centralized and protected.

- In many cases, where the data contains information of a personal nature – there is a legal requirement to ensure that the data is protected. This is achieved by using user IDs and passwords properly.
- The data can be easily backed up from a central point.
- The data should be better organized to permit users to find data easily – this should translate to more efficiency.

### ***What are the drawbacks?***

In general the server becomes the heart of the IT service therefore it is important to ensure that the server is adequately protected against;

- Power Failure (a UPS [uninterruptible power supply] is normally installed)
- Ingress of dirt, water whatever can cause a failure.
- Theft of the server.
- Physical hardware failure (a support contract is normally taken out).

It may also be necessary to have an employee trained to carry out basic tasks.

### ***Costs***

A server implementation (hardware and software) can cost from as little as £2000, however this kind of figure does not include the important aspects of a storage rack, UPS and software to automate back-ups and other software, such as a local e-mail system.

For a competent server, server software, rack, UPS and basic software the budget is likely to be between £3000 and £5000 for 5-10 users. Note this does not include any PCs or PC software.

***It is worthy of note that a correctly designed system should last 2-5 years, therefore may businesses feel it is appropriate to lease the components to maximize the capital investment.***

## ***Caveats and Disclaimers***

### ***Technical***

This information is provided in good faith, as-is for informational purposes only and is accurate to the best of our belief.

Polar Computer Communications accept no responsibility or liability whatever for any inaccuracies in this text.

Polar Computer Communications accept no responsibility or liability whatever for any consequential losses as a result of using (or not using) the information contained in this document.

It is the responsibility of the reader to satisfy themselves as to the accuracy of this information prior to acting upon it.

### ***General***

Please note: This information and all services and products are provided in accordance with our Standard Terms and Conditions of business which can be found at;  
<http://www.polar-cc.co.uk/text/stc.html>

## Appendix B

### Glossary of Terms - Explanation of Services and Acronyms

#### ADSL

Short for *Asymmetric Digital Subscriber Line*, a local loop technology that allows more data to be sent over existing copper telephone lines. ADSL supports speeds of from 1.5 to 9 Mb/s when receiving data (known as the *downstream* rate) and from 16 to 640 Kb/s when sending data (known as the *upstream* rate). ADSL requires a special ADSL modem.

ADSL is growing in popularity as more areas around the world gain access, however the deployment model of many ISPs does not permit enough upstream bandwidth (from the PoP to the Internet) to cope with the large number of user demands placed upon the system. In particular, most ISPs do not offer any upstream bandwidth QoS (Quality of Service) measures to ensure a minimum bandwidth is available to each user.

#### DNS

Short for *Domain Name System (or Service)*, an Internet service that translates domain names into IP addresses.

Because domain names are alphabetical, they are easier to remember. The Internet however, is really based on IP addresses.

Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name *www.anydomain.com* might translate to *193.92.262.4*.

The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

DNS is particularly important in the provision of SMTP mail services. The SMTP gateway (or mail server) uses the "MX record" to convert an email address (*anyone@anydomain.com*) to the mail server's IP address for delivery of e-mail.

Denial of Service attacks are commonplace to DNS servers that are not adequately protected. In a recent event, [www.microsoft.com](http://www.microsoft.com) was 'taken down' for several days due to the failure of the DNS systems, partially caused by hackers. Due to the fact that changes in the DNS configurations of companies must be propagated to all ISPs, any rectification of a failure can cause several days to resolve.

#### Firewall (stateful inspection)

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

- **Packet filter:** Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

## polar computer communications ltd

- **Application gateway:** Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.
- **Stateful inspection gateway:** Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- **Proxy server:** Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, firewalls may use two or more of these techniques in conjunction with each other.

### IMAP

Short for *Internet Message Access Protocol*, a protocol for retrieving e-mail messages. The latest version, *IMAP4*, is similar to POP3 but supports some additional features. For example, with IMAP4, you can search through your e-mail messages for keywords while the messages are still on mail server. You can then choose which messages to download to your machine. Like POP, IMAP uses SMTP for communication between the e-mail client and server.

### POP

Short for *Post Office Protocol*. The de-facto standard protocol for e-mail clients to communicate with the e-mail server. See also IMAP.

### PoP

Short for *Point of Presence*, a location from where services can be delivered. Internet Service Providers (ISPs) generally provide many POPs so that users can make a local call to gain Internet access.

### SDSL

Short for *Symmetric Digital Subscriber Line*, a local loop technology that allows more data to be sent over existing copper telephone lines. SDSL supports symmetrical speeds of up to 2.3 Mbps. SDSL requires a special SDSL modem.

SDSL is growing in popularity as more areas around the world gain access. It uses a variety of modulation techniques and is rate adaptable dependant on the quality of the copper wire that is being used.

### SMTP

Short for *Simple Mail Transfer Protocol*, a protocol for sending e-mail messages between servers. Most email systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your email application.

### SMTP Feed

An Internet service may block the SMTP service from entering a client site. To permit SMTP to pass (an SMTP feed) the client may incur an additional charge. PCC normally includes SMTP feed with managed Internet bundles.

### SNMP

*Simple Network Management Protocol* is a protocol and framework for obtaining operational statistics and status of a network device (e.g. server, router etc.). SNMP is a very powerful tool and can be used to create a denial of service attack or a security violation by reading information about devices that can be valuable to attackers.