![Northumbria University Newcastle logo]

KF5004

——

Company Brief

——

The Implementation of a DNS infrastructure (BIND9) and Web Server
Farm facilities (Apache, PHP, NFS, and MySQL)

——

Dr. M. Fatih Tuysuz

September 2023

Contents

1   Introduction

A company requires a large-scale implementation of a DNS architecture with a **load balanced** web server farm and an intranet to fulfil its web infrastructure needs. The company also wishes to manage aspects of its computer assets and staff requirements through the DNS implementation. Below is a description of the company needs.

2   Overview

The company requires two domains and one subdomain to fulfil its internal and external needs.

unn.co.uk

tech.co.uk

staff.unn.co.uk

The three zones fulfil different requirements based on how devices are addressed.

The company has a single gateway machine connecting the company to the internet and has 15 static IP addresses supplied by their ISP. These addresses allow the company to map machines directly to the internet from their internal network such as their company internet web server farm (details to follow). This external mapping is outside of the brief and is supplied for information only.

The company's gateway IP Address is: 192.168.100.254

2.1   Domain - Purpose

2.1.1   unn

This domain is managed by the technicians. The domain is used to direct traffic to the company's externally facing web service and internally for the company's internal network. The zone is also used for mapping of the main servers such as NFS and the central MySQL server.

2.1.2   tech

This zone is managed by the technicians and is used by the technical staff so they can remotely access machines via a fixed asset number that the machines are given (The asset number remains with a machine while it is in use by the company). This zone should only be accessible from the technicians machines that are in the range 192.168.170.0/24 and 192.168.180.0/24 and 192.168.190.0/24

2.1.3   staff.unn

The zone is managed by the **personnel department** who have their own administrator who runs the zone in cooperation with the IT department. This zone is used to manage the movements of staff within the organisation and their locally shared resources. i.e. it is used to point to the machine they are using. Once a person is allocated a FQDN in the staff.unn zone it remains with them as long they work at the company. As staff move to new equipment (PC's) the IT department inform personnel department who will change the DNS entry.

3   Operational Implementation

3.1   Transaction Logging

The company carries out 6-weekly audits of DNS requests that are made against the DNS service. This is to allow an analysis of websites that staff are visiting. This data is used to develop firewall policies (beyond the scope of this brief). You should therefore ensure logging can be enabled and disabled on the DNS service by commenting a configuration.

3.2   Client DNS configuration

All client machines should be configured to use the two secondary DNS servers. The primary server should be protected from client queries except for the secondary servers. The primary server should be excluded from any NS queries of the domain.

All domains should be able to disclose the *available* DNS architecture.
i.e. nslookup -type=ns unn.co.uk

4   Mode of Operation - Zones

4.1   Company zone - (unn)

Almost all the FQDN's in the unn domain need to be set up so that the details will be changed at least every 6 hours for PC's and caching servers and the secondary servers should be updated every 4 hours. If there is a failure of the primary DNS server, the domain should stay active for one week.

The unn zone is used to map the individual's personal web space that is stored on a single web server which is only used to support the staff's static shared website areas. This server should be accessable via http://intranet.unn.co.uk/ <username>. This site is only visible inside the company network.

All staff, when they join the company, are allocated a personal account on the personal web server machine. The server is a small HP Rack Mount server running Ubuntu LTS Server. All staff must have access to an FTP facility to upload files to their storage space. The personal areas are for static websites only and should not support any server-side scripting. Although it should be possible to enable scripting in personal area if necessary. There is one exception to this: The chief executive (account name ceo) has insisted that their personal web space should support scripting.

> **NOTE:** You should implement an upload access facility (FTP) and install a sample static website for a few user accounts. You will need to research installing vsftpd server and the command adduser to do this.

The intranet server, in addition to the personal webspace, also supports the company intranet site. The intranet site is accessed via the URL http://intranet.unn.co.uk The intranet site must support dynamic scripting and requires it own locally installed database (MySQL) that should only be accessible from the server.

> **NOTE:** A sample page will be required to demonstrate the configuration of all the accounts on the server i.e. intranet (dynamic), static users and the CEO's dynamic account).

The intranet MySQL database is to be managed via PHPMyAdmin (this should be demonstrated and include the creation of a secure database). The database service (on the intranet server) should be configured to only allow access from the localhost connection (Security!).

An additional database server (MySQL) is required with 7 Databases to be set up for different projects of which one is used for the external facing internet site (1 for internet + 6 for other future systems). There should be separate username/password for each of the MySQL databases in addition to the administrator account. The database service must therefore be accessible from other machines on the network to allow the web server farm to connect.

> **NOTE:** The internet site may require additional servers to provide faster access to database queries (research database performance in a load balanced environment), you do not need to implement this but you should understand the concept.

The company also uses this zone to map the externally facing internet service (3 IP addresses from the 15 provided by the ISP), to the internally hosted web server farm. The external IP addresses are forwarded to the internal IP addresses. The internal DNS mappings are controlled by the company and must be mapped in a round robin mode. Both the **internal** and **external** access should be provided through the URL http://www.unn.co.uk (Only the internal DNS service needs to be configured).

The internal mapping of the internet service is very stable and tends not to move so can be set to have a 'long' lifetime (TTL).

Thee company website is a web server farm. It should consist of 3 web servers that are load-balanced via DNS round-robin to provide *some* fault tolerance. The servers should share static content (uploaded documents and static images) via an NFS server that is secured (rDNS) and backed up to another machine in a fault tolerant manner via block replication (Do not build it is not required initially). The web servers should host their own copy of any PHP based applications locally.

> **NOTE:** You do not have to implement the NFS data block replication but you should configure a FQDN for it as an example.

The internet web servers should be accessible on an individual basis as well as via the load-balanced URL. The servers should be mapped via both the tech and for web access via the unn zone.

The content server used for the internet site should be accessible via the domain names nfs.tech.co.uk and nfs.unn.co.uk. The replication server should be accessible via nfs2.tech.co.uk and nfs2.unn.co.uk.

The NFS server should provide a security policy to only allow the web servers to access the content store via an rDNS lookup.

There is also a mail server entry required in the unn domain to map to a hosted mail service at mail.microsoftonline.com.

4.2   **Admin** zone - **(**tech**)**

The admin (tech) zone is used by the technical staff to manage the infrastructure of the organisation. All equipment that the company places on the network is added to this domain so that it can be uniquely access by the technical staff who manage the equipment.

The domain has regularly additions made to it, but the mappings of devices to their allocated addresses are rarely changed. Howeber. the company does not want want any mappings cached on the network.

The domain name allocated is the asset number given by the finance department and the zone name. Asset numbers start with an A and are followed by an 8 digit number.

e.g.   A12345678.tech.co.uk

Machines that are to run a network service are assigned an alias to make their name easier to remember. This name used to access the service (database, mail etc.). When equipment is updated or replaced by a new asset the asset number-based domain name will change but the service access name will be the same.

4.3   **Staff** sub-domain zone - **(**staff.unn**)**

The staff.unn zone is used to map staff in the company to desktop machines. All the machines use sharing of some sort for the staff to make documents available usually via universal naming convention (UNC) or uniform resource locator (URL). Therefore, each member of staff is allocated a domain name based on their name (e.g. William Smith will be given ws, so their full domain name will be ws.staff.unn.co.uk). If more than one member of staff has the same initials a number will be appended to the name e.g. ws1.

All staff movements, should there be any, take place monthly and the domain zone distribution needs to cater for this.

END