**Bill Buckles - Project 2013**

Michael Spence

2013-07-04

**Audience:**

This document is written for the use of the Project Manager, network engineer, and support staff. This document will be referenced for explanatory purposes to the Bill Buckles Group, including personnel there such as the Financial Controller, Dealer Principal and IT Support Staff.

**Preamble:**

This document will detail the Deliverables for the Bill Buckle Project.

This document will explain the implementation of these Deliverables.

**Topics of Discussion:**

1. Initial configuration

2. Deliverables

a. Physically Neat and Workable Network

b. Good Network Infrastructure

i. Logical and Documented Switching Layout

ii. Verified Telstra Router Configuration

c. Managed ESX Server

d. Active Directory

i. Group Policy Control

ii. User Management

e. File Servers

i. File Collaboration and Sharing

ii. Folder Redirection

f. Internet Connectivity

g. Remote Access

i. New Terminal Server

ii. Secured Gatekeeper

3. Implementation

a. Network Improvement

i. Patch Panel Re-configuration

ii. Switch Replacements

iii. IP Address Cleansing

b. Server Refresh

i. ESX Configuration

ii. Server Builds

c. User and PC Migration

i. User Creation

ii. Domain Migration

**Topics in Detail:**

**1. Initial configuration**

At present the state of the IT infrastructure at Bill Buckles can only be classified as poor. Many of the pieces for creating a workable network and application set exist within the systems that are present, but lack of personnel with competent IT skills has resulted in mismatched and mis-configured systems. This has created an environment which is unstable. Systems regularly fail, and restoration times are high due to the time required to unravel the knot of system configurations which exist.

This is physically evidenced by the method in which computer have been patched into the network at the communications cabinets. At these points a tangle of cables exist, where no one wire is easily distinguishable from the other, in either purpose or destination. This creates a huge burden on even the easiest IT task of adding computers to the network.

Further evidence is shown in the use of equipment which is unmanageable due to cheap equipment or unmanageable due to lack of documentation. There exist switches at bill buckles which cannot be controlled, leaving network traffic to chance - this could obviously pose a threat to data integrity and reliability. Further to this the connection from HQ to VW/Subaru is given by equipment which has no documentation to speak of. Without this information, it is impossible to know or understand what this equipment is doing or how it is passing network traffic from one side to the other - this is imperative if anyone is to have confidence in the network systems.

Building upon the network are the applications which are provided to the users. Presently only the most rudimentary file sharing exists between users, although recent initiatives have started to give users a more structured sharing capability. It is the author's opinion that Units (or any ERP provider) and their systems should be stand alone and should not interfere with the daily running and internal collaboration of a dealership. For this reason, the Units systems at Bill Buckles provide services similar to the required services, but potentially configured in such a way to be detrimental to the actual requirements. These systems are also essentially the sole responsibility of Units themselves and therefore should be left to their care.

For this reason, the following items are what are considered to be the required items for a stable system.

**2. Deliverables**

The planned items which APEagers Qld IT will be making available to Bill Buckles will include the following. These items do not include the entire set of available items which have been developed for the Qld and NT dealership, but budgetary roadblocks prohibit creating further responsibility for the QLD IT staff.

**2.a. Physically Neat and Workable Network**

First and foremost within any IT system must be a simple and effective method for supplying "network" to "network connected" devices. Maintaining a physically neat and workable patching system is imperative for this daily task.

A network patching system should be easily traceable; meaning that any wall socket which is connected can be easily located on a switch port. Also the cabling used should indicate the purpose for why the port is patched; it is common to colour code patching to signify purpose.

For this reason, IT staff from QLD will visit HQ and Service and neaten the patching at these two sites. If necessary, switches will be moved to provide better access for patching purposes. Colour coded cables will be used to signify purpose. The following colour key will be adhered to at all times.

COLOUR PURPOSE

Blue PC or Printer ONLY

White Telephone (IP or PSTN)

Green Servers

Red Uplink (Switch to Switch or WAP to switch)

Yellow Edge (Router to Device [Switch or FW])

Allowances will be made, when connecting distances further than inside the patch system, if cables of the correct length cannot be found. In these cases, blue cables with coloured electrical tape may be used to identify cable purpose.

**2.b. Good Network Infrastructure**

The phone system at all Bill buckles sites exists on the same physical network as the PCs and printers. Due to this it is good practice to separate these systems with VLANs. At present this has been done, but only so far. It is also not clear what configuration Telstra has made to the onsite routers. Without this information it cannot be certain that routing for particular purposes will work as expected.

**2.b.i. Logical and Documented Switching Layout**

At present the switching configuration is haphazard and inconsistent with standard configuration methods. Essentially, it is the author's opinion that servers and services should be grouped on the core switch so that the can be easily identified and located close to each other. Branching switches should also be connected to the core switch, providing the closest proximity to services to all devices and users of the entire network.

For this reason, switches may require access to both the data and voice networks. It follows that this must be clearly documented so that patching is still simple.

With this in mind, the core switch will attach to each local (i.e. in immediate proximity) switch using the highest speed connector available. For switches which are in an alternate location, it may not be possible to connect all local switches to the core switch, in this case one switch will act as the "core" switch for this branch of the network. The effort will be made to make the user or devices as close to the WAN router as possible; in this case distance is measured by the number of switches between the user and the router.

Finally, documentation will be provided detailing the connectivity of devices. The documentation will supply visual representations of the switch as to which ports are available for data or voice usage. The configuration of each switch will be recorded for both backup and reference purposes.

**2.b.ii. Verified Router Configurations**

Bill Buckles has a complex network due to its number of brands, unique telephone system and connectivity to the APEagers WAN via a Telstra VPN. This connectivity is provided by both the APEagers managed Firewall at Bill Buckles HQ and also the Telstra WAN Routers.

By default the Telstra routers send traffic to HQ. This is not true of some services, most notably the telephone system. Each LG IPECS telephone system is independent and provides phones primarily for the site at which it is located via ISDN on ramps. To enable phone redirection and transferral, the phone conversation must be routed across the WAN via the Telstra routers, to each of the servers. This configuration mirrors the data network in some respects, but must be taken into consideration when looking at the layout of the network.

With the addition of onsite firewalls to connect the local site networks to the internet, a more complex routing topology has been introduced. With this routing resiliency can be introduced to the network, however care must be taken to enable clients to be correctly configured at all times. These configuration methods will be documented and available for appropriate staff.

**2.c. Managed ESX Server**

The server infrastructure being provided by the APEagers IT department will be housed within one single server. This server will be running VMWare's ESXi 5.1 and hosting virtual machines to act as servers for various application purposes. The server provided will be accessible via a Remote Management Module, providing access for administrators direct to the console of the server. Access will also be granted to the ESX subsystem for integration into the APEagers Virtual Centre standard configuration.

The purposes of Virtual Machines, as noted at the time of this document, are:

Primary Firewall and Router

Domain Controller(s)

Terminal Server

File Server

Administration Login Server

Remote Gatekeeper

Further addition to the list of applications being hosted on this system will be possible. Resource allocation at this time is expected to be considerably less than maximum capacity.

The ESX system will also be supported by a backup method which will duplicate each virtual machine to disk, once daily.

**2.d. Active Directory**

A primary goal of this project is to enable file sharing between employees. Within a Windows computer network, this is most easily achieved through the deployment of Active Directory to all computers and users. Once this deployment is achieved, using Microsoft techniques, configuration of users can be performed en masse quite readily.

The QLD APEagers IT team have had extensive working knowledge of a Windows 2000/2003 based Active Directory system. This system has limitations which the team is readily aware of. It is the intention of this project to deploy an Active Directory system which is modern and capable of supporting a Windows network, well into the future. This deployment will require further skilling of the team members from QLD whom will be involved in the deployment of this AD system.

**2.d.i. Group Policy Control**

Group Policies allow an administrator to quickly control and adapt a user or many users operating environment. The QLD APEagers IT team has operated GPO's for many uses and their implementation is extremely streamlined and essentially error free. As part of this project, it is intended that many of the QLD GPO's will be copied verbatim into the new Bill Buckles Active Directory Domain.

The purposes for Group Policies which will be transposed are:

My Documents/Desktop Redirection

Shared Drives Mapping

Proxy Configuration

Windows Update Configuration

Default Computer Configuration

Password Enforcement

Computer Investigation

Further development of GPOs will be done as the need arises.

**2.d.ii. User Management**

The creation and management of users will be the responsibility of the onsite Bill Buckles IT staff member. However, the domain will be provisioned to allow access from the APEagers IT Helpdesk for this purpose also, in the case of "emergency". At all times, the Bill Buckles domain Enterprise Administrators will have access to create, modify and manage users as well as revoke users' rights and securities.

**2.e. File Servers**

Initially, only one file server will be provisioned at Bill Buckles. This server will be housed at the Head Office as a virtual machine. The purpose of this machine will be (and will only be) file serving to the users of the network. File sharing will cover two basic purposes.

**2.e.i. File Collaboration and Sharing**

To enable intra- and inter-department collaboration, a simple an effective method has been used throughout APEagers Qld for some time. This method utilizes the built in file sharing technology of the Windows platform, layered with the security model enabled by the introduction of Active Directory. However, without the appropriate preparation of the shares and a strict enforcement of how access is granted to shares, the future administration of these structures becomes problematic. For this reason the following trends will be followed.

A simple and secure file structure will be shared between all users at Bill Buckles. This system will have subfolders secured by security groups. It is the engineer's intention that single, one-off security for users shall not be applied to folders or shares. For each subfolder a distinct AD Security Group shall be created and applied to the folder for "read and write" purposes. Subfolders that do not have their own AD security group shall inherit their permission/security model from their parent.

Because faults (due to mis-configuration or other) can occur at any level in a multi-user share, Domain Administrators must be given access to all levels of the file share. The root share will have Domain Admins as having full ownership rights of this folder and this will be propagated throughout the lower folders.

If users insist that files must be restricted from all other users' access, they will be able to remove inheritance from files they own. These users run the risk of causing file sharing issues between themselves and other users and when problems arise must relinquish control to Domain Admins when the time arises for them to fix these issues.

**2.e.ii. Folder Redirection**

As a backup method, APEagers Qld IT has deployed Folder Redirection for many years. This invaluable tool, replicates the user's Desktop and MyDocuments to a file share on the network, meaning there is a local copy on the computer and also on the network. This network copy can then easily be backed up and stored for later use.

With the advent of Windows Server 2008 R2 the feature set of Folder Redirection has greatly increased and it is the engineer's intention to employ some of the additional techniques which would limit some of the information stored on the network. For example, it has been noted that sync'd iPhones and iPads store their music libraries in users' MyDocument. Copying this music from one media type to another, is a grey area in terms of legal copyrights, and it is the engineer's intention to not include this feature in Folder Redirection.

**2.f. Internet Connectivity**

Internet connectivity is quickly becoming the most required resource for many departments within the dealerships. A marked increase in internet traffic has been noted over the past few years, especially in the areas of service and parts. For this reason the internet connectivity for users is a large concern.

Presently at all site locations at Bill Buckles AAPT internet connections have been installed. These internet connections are present to relieve the pressure internet activity has put on the Telstra WAN links, which should now be primarily used for internal business purposes only. Also at head office there still resides a Telstra internet connection.

It is the intention of this project to streamline the use of the internet at the head-office such that both internet connections are used concurrently, with either providing a backup for the other failing. Also since the WAN will still exist, if an internet connection at a site fails, the WAN can be used to provide internet redundancy through the use of proxies at alternate sites.

**2.g. Remote Access**

While there is not generally a large push for Bill Buckles users to have access from home, there are at least some key individuals who require this feature. Also during times of emergency, locations with failed WAN links may be able to access remote features using their internet link.

**2.g.i. New Terminal Server**

It has been proposed that a new terminal server be built to replace the current system. This terminal server should have appropriate applications installed on it such that users can perform everyday tasks as if they were on their computer. This could include applications such as Word or Excel, web browsers or Toyota applications. Due to the storage requirements of some applications, such as Outlook for example, some applications cannot be included. It is the author's opinion that most applications have a browser counterpart (for example OWA for Outlook) or they will not be missed for short periods of time.

This server will be secured by Active Directory and users will be required to login using these credentials only. Further to this, a security group will be configured, which will allow or deny the access of a user to this remote terminal server. Since this server will be web-facing, it is prone to abuse by hackers and must be as well secured as possible. Users in the allow security group, will be forced to have more secure passwords.

**2.g.ii. Secured Gatekeeper**

As a second layer of security for accessing the remote systems, APEagers Qld IT has employed the use of a Secured Gatekeeper. This method uses security certificates to validate users as well as the username/password method.

An added feature of this system is the ability to access more than one system, for example a user's PC, via the gateway. This can then be secured for only this user to access their machine.

It is the intention of this project to roll out this feature once all other deliverables are in place.

**3. Implementation**

The following steps document the methods administrators will take to implement the above outlined objectives and deliverables.

**3.a. Network Improvement**

First and foremost in the network improvement is the documentation surrounding how devices are interconnected throughout the sites. This documentation will be prepared prior to implementation and during reconfiguration all attempts will be made to make reality this engineered works. Changes/alterations at the time of implementation will be noted and final documentation will be created and stored for future reference.

**3.a.i. Patch Panel Re-configuration**

Within patch panel areas, cable tidies will be used to ensure that patching is no longer a burdensome task. For each 2RU of patches a 1RU cable tidy shall be used between them, in a P-T-P arrangement. From initial documentation it appears there is a present lack of cable tidies, for this reason further supplies have been sent.

Depending on the bulk of cables returning to switches 2RU cable tidies (which are to be recovered from the VW patch area) will be used below switches to again tidy the patch area.

All Ethernet cables identified as being used for telephony will be colour coded to white. It is preferred that white cables shall leave via a cable tidy towards the right.

All Ethernet cables identified as being used for data will be colour coded to blue. It is preferred that blue cables shall leave via a cable tidy towards the left.

Switches will be considered in the following way. The switch closest to the Telstra WAN router will be called CORE. From the CORE switch all other switches will branch, they are to be considered ACCESS with roles of DATA, VOIP or DATA&VOIP (aka COMBO). If a switch at a campus cannot be directly connected to the CORE switch, due to proximity etc, the switch immediately prior to it must be considered to be a DISTRObution switch. For documentation purposes, branches with DISTRO switches are labeled with additional letters to denote their location.

All Ethernet cables identified as connecting two switches will colour coded to red. Connect the ACCESS or DISTRO switch to the highest numbered port on the CORE or DISTRO switch. All switches should be connected at the highest speed rated ports available.

All Ethernet cables identified as connecting a switch to a router will be colour coded to yellow. Connect the router to the last non-special port on the switch, which is typically port 48 or port 24 on HP switches.

All Ethernet cables identified as connecting a server to a switch will be colour coded to green. Connect servers to the CORE switch only and patch to the highest numbered ports first, leaving space for switch and router patches.

It is preferred that red, yellow and green cables shall eave via a cable tidy towards the right.

At present colour coding is not present at Bill Buckles and due to this stock of coloured cables has been ordered to fulfill this implementation.

**3.a.ii. Switch Replacements**

In each patch panel, it is the engineers intention that only manageable equipment (such as switches) be used. Switches shall be configured on-site with appropriate security measures and IP addressing to enable access to administrators while reducing the impact of users' tampering.

Switches will be configured with the S4/S3 security model:

Access password = <clueless>

Enable password = <is a!>

As a rule, switches will be given a single data type role only and then be clearly labeled for that role, either DATA or VOIP. If necessary, such as in small installations, a switch may be given a dual role, in which case, data ports will be provisioned on the left and VOIP ports provisioned on the right; this fits with the cabling methodology described above.

**3.a.iii. IP Address Cleansing**

At each site, regarding the data network, it is the engineer's intention that a strict IP addressing scheme be used. The provisioning of this scheme is still up for debate, but the following should provide a skeleton framework, with which to work with.

START END PURPOSE

0 0 Unusable

1 15 Servers

16 47 Static IP Address PCs

48 148 DHCP'd IP Address PCs/Notebooks/Tablets

149 149 Reserved for Admin

150 180 Static IP Address Printers

181 199 (No Purpose)

200 244 Static IP Address Switches

245 252 Misc Networking Devices

253 253 Site Firewall

254 254 Site Telstra WAN

255 255 Unusable

With an appropriate numbering scheme in place, each individual device will be altered to fit within these planned usage areas.

**3.b. Server Refresh**

The APEagers server which is on-site at head office at Bill Buckles will be replaced. The replacement server will be more capable and will be covered by warranty for the next four years.

Access to this server will be possible through the Remote Management Module. This system should be considered an S1 system.

Name bbu-rmm.apeagers.com.au

IP Address 172.17.150.2/24

IP Gateway 172.17.150.254

User issadmin

Password <easy>

Through this interface the operating system can be reinstalled. Presently this server has ESXi 5.1 installed.

Included in the Server are six (6) 250GB SSDs. With one drive marked as a Hot Spare the other five (5) drives have been placed in a Raid-5 configuration creating a virtual drive of 890GB.

**3.b.i. ESX Configuration**

The ESX system is managed through the VMKernel Port. This system should be considered an S1 system.

Name bro-esx1.apeagers.com.au

IP Address 172.17.150.1/24 (temporarily .8/24)

IP Gateway 172.17.150.254

User root

Password <easy>

The system is already connected to the qld-vc51.apeagers.com.au vCentre 5.1 installation.

Internally the ESX system will have three virtual networks and one Management Network:

VLAN1 VM Network

VLAN5 DMZ Network

VLAN666 WWW Network

These networks will be hosted on two virtual switches, and will access the real network via three (3) NICs:

vSwitch0 VLAN1, VLAN5, Management Network vmNic0

vSwitch1 VLAN666 vmNic1, vmNic2

It is intended that Nic0 is patched directly into the LAN network on the CORE switch.

It is intended that Nic1 and Nic2 are patched directly into the internet links from Telstra and AAPT directly.

NTP Time configuration is configured to gain time from 10.1.1.43 (a.k.a. qld-dc1.apeagers.com.au).

**3.b.ii. Server Builds**

The following servers will be built as virtual machines on the ESX system:

BBU-PF1 Firewall and Router

BBU-DC1 Primary Domain Controller

BBU-DC2 Secondary Domain Controller

BBU-FS1 File Server

BBU-TS1 Terminal Server

BBU-ISSADM Administration Machine

BBU-GK1 Secure Gatekeeper

The following summarises the builds for each of the above:

The Firewall and Router system is an S1 system.

Name bbu-pf1.apeagers.com.au

IP Address0 203.43.230.186/30

IP Address1 172.17.150.250/24

IP Address2 10.40.1.34/27

IP Gateway 203.43.230.185

User issadmin

Password <easy>

Configure /etc/pf.conf

/etc/squid/squid.conf

/etc/rc.local

The Primary Domain Controller is an S2 system.

Name bbu-dc1.buckles.local

IP Address 172.17.150.3/24

IP Gateway 172.17.150.254

Configure dcpromo - all primary roles

The Secondary Domain Controller is an S2 system.

Name bbu-dc2.buckles.local

IP Address 172.17.150.4/24

IP Gateway 172.17.150.254

Configure dcpromo - secondary for DC1

wsus - gpo for computers

The File Server is an S3 system.

Name bbu-fs1.buckles.local

IP Address 172.17.150.5/24

IP Gateway 172.17.150.254

User issadmin

Password <is a!>

Configure share folders - bbu.data and bbu.users

sec groups - data shares and folder redirection

folder red - gpo for users

The Terminal Server is an S4 system.

Name bbu-ts1.buckles.local

IP Address 172.17.150.6/24

IP Gateway 172.17.150.250

User issadmin

Password <clueless>

Configure remote desktop - sec group

remote access - gpo for computer

user profiles - gpo for terminal servers

The Administration Server is an S3 system.

Name bbu-issadmin.buckles.local

IP Address 172.17.150.7/24

IP Gateway 172.17.150.254

User issadmin

Password <is a!>

Configure ? vSphere

? Browsers

The Secure Gatekeeper is an S2 system.

Name bbu-gk.buckles.local

IP Address 172.17.150.9/24

IP Gateway 172.17.150.250

User issadmin

Password <yay!>

Configure rpc over https - certification

sec groups - computer and user

**3.c. User and PC Migration**

**3.c.i. User Creation**

The migration of users to the new domain can occur well before users are configured on computers. With this in mind, it is necessary that a list of the users is compiled along with user roles and location. Assumptions regarding users will be made based on their role within the dealership and their working location. Initial security configurations will revolve around this information.

The following roles are assumed to exist within the dealership:

Receptionist

Sales person

Sales manager

Finance manager

Service advisor

Service manager

Workshop foreman

Parts advisor

Parts manager

Administration

Financial controller

Dealer principal

It is understood that there are five (5) sites within the Bill Buckles dealership:

BRO Brookvale Toyota, VW, Subaru, Land Rover, Jaguar

aka HeadOffice

HRB Harbour Rd Service Centre

OPB Old Pittwater Parts Centre

MON Monavale Service Centre

PRB Pittwater Rd Pre Delivery

Users will be created according to the list provided. Each user will be given this initial configuration:

Username <firstname>.<lastname>

Password Pa$$w0rd

Users will then be added to security groups according to role

Sales Group Receptionist, Sales person, Sales manager,

Financial controller, Dealer principal

Service Group Receptionist, Service advisor, Service manager, Workshop foreman, Financial Controller,

Dealer Principal

Parts Group Receptionist, Parts advisor, Parts manager,

Financial controller, Dealer principal

Admin Group Administration, Financial controller, Dealer principal

Manager Group Sales manager, Service manager, Parts manager,

Financial controller, Dealer principal

Also users will belong to a location group appropriate to their working location

HeadOffice Group

Harbour Rd Group

Old Pittwater Group

Monavale Group

Pittwater Rd Group

**3.c.ii. Domain Migration**

At the time of deployment, computers will be moved across to the newly appointed domain. It is the author's opinion that the preceding network infrastructure work should be completed in at least the area of deployment, prior to rolling out Active directory to computers.

During each computer migration, the following tasks will be performed to retain a user's usability experience:

Copied to New User Profile

- Desktop

- My Documents

- Favourites/bookmarks

Outlook Email re-configured (if present)

Default Printer Set

Some Desktop short cuts may be moved to the "All Users" profile. For example the Remote Desktop to the Units Terminal server.

Each computer will also have its remoting capabilities verified and its anti-virus software updated.

Each computer will also have its administrator password changed. Computers are considered to be S5 security items.

Username Administrator

Password <woody!>

The following items will be lost to a user's profile after the transition:

Internet Browser History including

- Cached sites

- Site Passwords

- Cookies etc

Desktop Background Configuration

Email Signatures

Due to the limited time available to the technical people who will be onsite for this task, addressing other issues not relating to this migration will not be able to be undertaken. Users will be prompted to bring these issues to the attention of the Helpdesk.