

Specification

Table of Contents - Specification

1.	PROJECT SCOPE	3
1.1	PROCUREMENT	3
1.2	DESIGN SERVICES	3
1.4	CUTOVER SERVICES	4
1.5	DOCUMENTATION AND HANDOVER	4
1.6	FIREWALL REQUIREMENTS	5

1. PROJECT SCOPE

1.1 Procurement

Procure Equipment Based on Specification Requirements

- Quote on system that meets the requirements section
- Include maintenance NBD replacement on products
- Include subscriptions if required

1.2 Design Services

DMZ redesign to reduce dual tier firewall to single tier. This will include:

- New public IP address range, validation or redesign of DMZ/Firewall Interface IP Range, ruleset validation/changes, VLAN design if required
- Design should take into account secondary internet pipe that will be implemented in the future as a redundant internet link (with separate external IP range)
- Design netflow for flow export to firewall analytical system
- Design reporting outputs based on best practice
- Archiving of firewall data to remote source
- Design maintenance plan and log archiving schedule

1.3 Implementation

- Rack and Stack Firewalls (Active at St Kilda Town Hall, Passive at South Melbourne Town Hall)
- Configure firewall interfaces
- Create firewall rulesets, routes, NATs & perform basic traffic tests
- Configure Active/Passive Firewall
- Test failover & Failback
- Attach virtual DMZ to environment and perform basic testing
- Enable netflow on core routers (5) and configure flows to export to Firewall Analysis tool
- Enable firewall analysis tool and configure to report exceptions, changes in traffic behaviour through firewall
- Enable monitoring of Firewall through network management tool (Argent)
- Enable Reporting service based on industry standards including monthly configuration change reports, highest denied traffic inbound/outbound
- Enable data archiving off-box for long term retention of logs

- Enable maintenance plan and log archiving schedule

1.4 Cutover Services

- Perform routing/VLAN/switching changes if required
- Switch physical interfaces of current switches / servers to new firewall
- Assist in performing connectivity tests for inbound and outbound services
- Establish VPN connections
- Move Ironport C650 web proxy into DMZ segment from LAN
- Assist in migration of Public DNS/MX records to new IP range
- Cutover to occur no later than December 12, 2009

1.5 Documentation and Handover

Documentation to be provided in MS Word and any Diagrams are to be provided in Visio format

Documentation to include any configurable items including and not limited to:

- Interface IP address and trunking
- Rules
- NAT/PAT settings
- User accounts
- Authentication settings (LDAP/AD etc)
- IPS configuration details
- VON connection details
- SNMP security changes (public/private strings etc)

Handover to include basic functionality handover of Firewall, Reporter and Traffic Analyser such as rule creation, how to perform upgrades/maintenance, reporting configuration, traffic analysis changes, highlight known operability pitfalls

1.6 Firewall Requirements

1.6.1 System Architecture & Implementation requirements:

Type	Architecture & Implementation Requirement	Compliant	Reference Document
Software	The firewall shall be a dedicated standalone appliance		
NAT	Supports Network Address Translation		
NAT	Supports dynamic NAT N:M with unused IP numbers utilization		
NAT	Supports unlimited number of NAT table entries		
NAT	Supports dynamic and NAT		
NAT	Supports static NAT		
NAT	Supports NAT configured on a per-interface basis		
PAT	Supports Port Address Translation		
Network	Supports unlimited mapped IPs per interface		
Network	Supports unlimited virtual IPs per interface		
Network	Supports unlimited dynamic IPs per interface		
Network	Supports WAN encapsulation		
Interfaces	Supports VLANs		
Interfaces	Supports minimum of 8 Gigabit interfaces		
Routing	Supports virtualization (virtual firewall)		
Routing	Supports transparent mode firewall		
Routing	Supports OSPF, RIP, and BGP routing protocols		
Routing	Supports Multicast routing		
Integration	Supports IPv6		
Integration	Supports LDAP integration		
Integration	Supports VoIP communications and protocols (H323 & SIP)		
Integration	Follows open standards		
Hardware	Appliances are rack-mountable in 19" rack with rails & cable management		

1.6.2 System Certifications:

Type	Product Certification & Standards	Compliant	Reference Document
Standards	FCC class compliant		
Standards	CE Class compliant		
Standards	C-Tick compliant		
Standards	VCCI Class compliant		
Safety	UL safety standard compliant		
Awards	Recipient of Best-of-breed / Commercial / Neutral Awards		
Awards	Recipient of Government Awards		
Certification	Meets Common Criteria EAL-4+ application protection		
Certification	FIPS 140-2, level 2 certified		
Certification	ICSA Labs IPsec VPN certified		
Customers	Published customer case studies		

1.6.3 System Security:

Type	Security Requirements	Compliance	Reference Document
Authentication	Requires users to identify & authenticate when signing onto firewall		
Authentication	Console access provides strong authentication capabilities		
Authentication	Console Authentication Methods: Password LDAP (Lightweight Directory Access Protocol) Active Directory RADIUS Single Sign On (SSO)		
Authentication	MAC & IP controlled authentication enforceable		
Certificates	Supports Automated Certificate Enrolment (SCEP)		
Certificates	Supports Online Certificate Status Protocol (OCSP)		
UTM	Capable of reputation-based defences		
UTM	Ensures packets are in compliance with RFC standards		
UTM	Provides Unified Threat Management capabilities on-box (Antivirus, Antispyware, Anti-Malware, SPAM filtering)		
UTM	Capable of URL Filtering (on-box)		
Anti-Tamper	Packaging sealed with custom tape		
Anti-Tamper	Uses tamper seals to indicate authenticity		
Anti-Tamper	Hardware can restrict remote access via access lists		
Anti-Tamper	Access list creation based on IP and MAC addresses		
Anti-Tamper	Hardware protects against password overrides		
Anti-Tamper	Hardware uses secure connections for remote access		
Anti-Tamper	FIPS certified for physical protection of keys, configuration, and software		
Protection	Provides TCP rate limiting		
Protection	Protects against SYN attack, IP spoofing, and port scanning		
Protection	Provides source route blocking		
Protection	Provides IP spoof protection		
Protection	Provides panic-Mode capabilities (such as during DoS, out of memory, etc)		
Protection	Supports configurable session timeouts		
Protection	Protects against DoS attacks		
Protection	Encrypted traffic inspection (Deep Packet Inspection)		
Protection	Packet Filter		
Protection	Stateful Packet Inspection		
Protection - Proxy	Provides protection for HTTP(S) traffic		
Protection - Proxy	Provides protection for FTP traffic		
Protection - Proxy	Provides protection for Sendmail		
Protection - Proxy	Provides protection for SIP		

Protection - Proxy	Provides protection for SMTP traffic		
Protection - Proxy	Provides application proxy services for FTP, HTTP/s, SMTP, Telnet, MS-SQL, Oracle, Citrix, SIP, SSH, Instant Messaging, Peer-to-Peer, H.323		
Protection - Proxy	Provides a Dual / Split DNS proxy		
IPS	Employs anomaly detection		
IPS	Provides customizable IPS signatures		
IPS	Capable of Intrusion Prevention (on-box)		
IPS	Provides Signature-based IPS		
IPS	Provides preconfigured signature groups		
IPS	Automatic IPS signature updates		
IPS	Multiple IPS Notifications can be sent to defined destination via SMTP,SNMP or to remote monitoring solution		
VPN	Supports 3DES AES-256 and below		
VPN	SHA-1 and MD5 authentication		
VPN	Deffie-Hellman 1,2 & 5		
VPN	IKEv1 and IKEv2		
VPN	Diffie-Hellmann groups 1, 2, and 5		
VPN	Policy-restricted tunnels		

1.6.4 System Administration, Monitoring & Availability:

Type	Administration, Monitoring & Availability Requirement	Compliance	Referenc Document
Administration	Provide ability to monitor multiple firewalls		
Administration	Provides a GUI for configuration / management		
Administration	Employs SSH remote administration		
Administration	Provides local console administration		
Administration	Supports full command-line interface for editing rules, routing, and NAT		
Administration	Provides a searchable configuration archive		
Administration	Provides the ability to manage differing software versions		
Policy	Provides a policy version control capability		
Policy	Ability to performs multi-appliance policy changes, configuration changes, and management		
Policy	Provides time-based policies		
Policy	Supports ability to view rule utilization statistics		
Policy	Supports time synchronization		
Policy	Provides a one-look rule view / simplified rule creation		
Access	Controls allocation and revocation of access and network access privileges		
Access	Controls access to audit tools / network management tools		
Access	Validates user's identify via password management, etc		
Backup/Restore	Provides a configuration backup & restore capability		
Network Mgmt	Provides a Ethereal/Wireshark or tcpdump capability		
Network Mgmt	Integrates with network management tools		
Network Mgmt	Compatible with SNMP v2 or later		
Network Mgmt	Supports syslog		
Network Mgmt	Defined MIBs available for monitoring solution		
Network Mgmt	Out of Band Management option available		
Updates	Provides firewall software updates/enhancements		
Updates	List all Critical Security updates required in the past 3 years		
Updates	Provides an easy rollback mechanism for failed updates		
Capacity	Supports a minimum of 100,000 concurrent connections		
Capacity	Supports a minimum of 100,000 NAT table entries		
Capacity	Provides stateful inspection throughput of 1 Gbps or higher		
Capacity	Supports a minimum of 100,000 ACLs		
Latency	Provides latency statistics		
Redundancy	Provides redundant power supplies		
Redundancy	Provides redundant hard drives		
Performance	List Maximum site-to-site and remote access VPN user sessions		
Performance	IPSec VPN performance at 240Mb/sec or greater		
Performance	Supports multiple concurrent sessions		
Performance	Packet filtering throughput 1.8Gb/sec or greater		
Performance	Application filter throughput 1.4Gb/sec or greater		
Performance	Stateful throughput 1.8Gb/sec or greater		

Traffic Mgmt	Ability to process traffic at varying packet sizes.		
Traffic Mgmt	Provides traffic prioritization to ensure business critical applications are available		
Traffic Mgmt	Controls bandwidth at policy level, interface level, or both		
Traffic Mgmt	Supports jumbo frames		
Traffic Mgmt	Sets priority field in the Type of Service (TOS) byte to reflect traffic priority		
Load Balancing	Load balancing capabilities available		
High Availability	Supports active-standby high availability		
High Availability	Disk failure immune		
High Availability	Provides redundant power supplies		
High Availability	Synchronizes the configuration from active to standby machine		
High Availability	Synchronizes data from active to standby machine		
High Availability	Active/Standby monitoring & failover available across WAN segment (Remote IP monitoring)		

1.6.5 Firewall Reporting & Traffic Analysis:

Type	Firewall Reporting Requirement	Compliance	Reference Document
Log	Supports syslog UDP logging support		
Log	Supports syslog TCP logging or logging to a file support		
Log	Supports begin of session logging		
Log	Supports end of session logging		
Log	Supports before NAT and after NAT IP addresses logging		
Log	Supports source and destination interface logging		
Log	Supports number of bytes transferred by session logging		
Log	Supports session duration time logging		
Log	Supports session termination reason logging		
Rule Usage	Logs or audits based upon usage of rules		
Audit	Do your audit logs record exceptions and other security related events		
Audit	Monitors system audit logs		
Audit	Provides detailed log reports		
Audit	Supports near real-time alerts on violations and intrusions		
Audit	Displays firewall latency statistics		
Auditing	Forensic Quality data tracking (attack type, source, destination, port, protocol, severity, rule, etc)		
Reporting	Inbuilt reporting which meets Sarbanes-Oxley & PCIDSS requirements		
Reporting	Ability to create custom reports per user		
Reporting	Report configuration change detail to prove that corporate networks are configured to specified requirements		
Reporting	Ability to Classify events based on each policy		
Reporting	Report on security issues and trends over time		
Reporting	Report on protocol usage by device, user, and department		
Reporting	Personalize/Customizable Dashboard Experience		
Distribution	Email reports ad-hoc or automatically to multiple recipients on a regular distribution list		
Distribution	Report outputs include: HTML, PDF, Excel, and Text		
Distribution	Ability to correlate events from multiple firewall appliances		
Analysis	Automatically identify and display changes in firewall behavior that may require attention		
Analysis	Analyse and report on firewall behavior in its full context: who (users and source locations), what (services and applications), and where (destination location) across the network based		

	on the flow information it receives from routers and switches (Netflow)		
Analysis	Report details of the activities users, services, and assets perform in real time through the firewall interfaces		
Analysis	Extract and Correlate Asset security information from McAfee ePO console		
Analysis	Integration with Active Directory for identity acquisition and role assignment.		
Analysis	Indicates why the firewall is dropping traffic: violates rule, contains malware, bad reputation etc		
Analysis	Drills down on what changed to violate firewall rule: locations of user, location of application, granular profile of application/service, or firewall rule change		

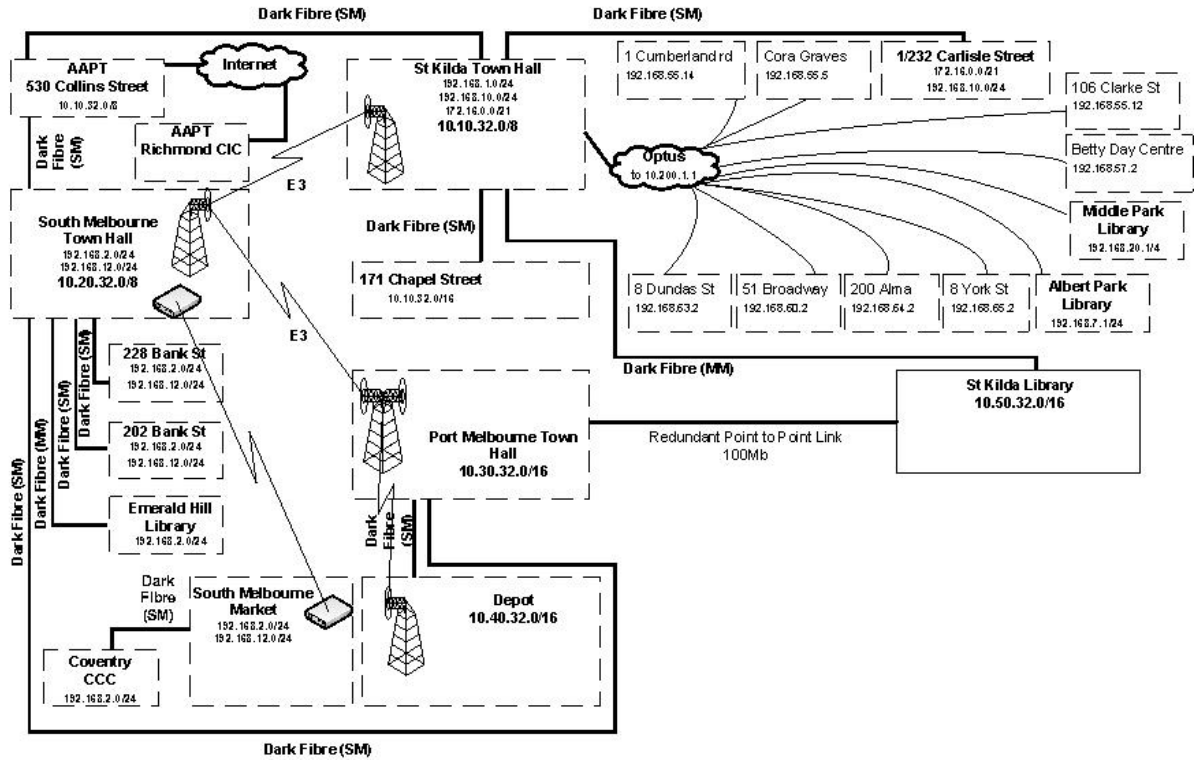
1.1.1.1

- 1.
- 2.
- 3.
- 4.
- 5.

1.2 3a. Current Architecture

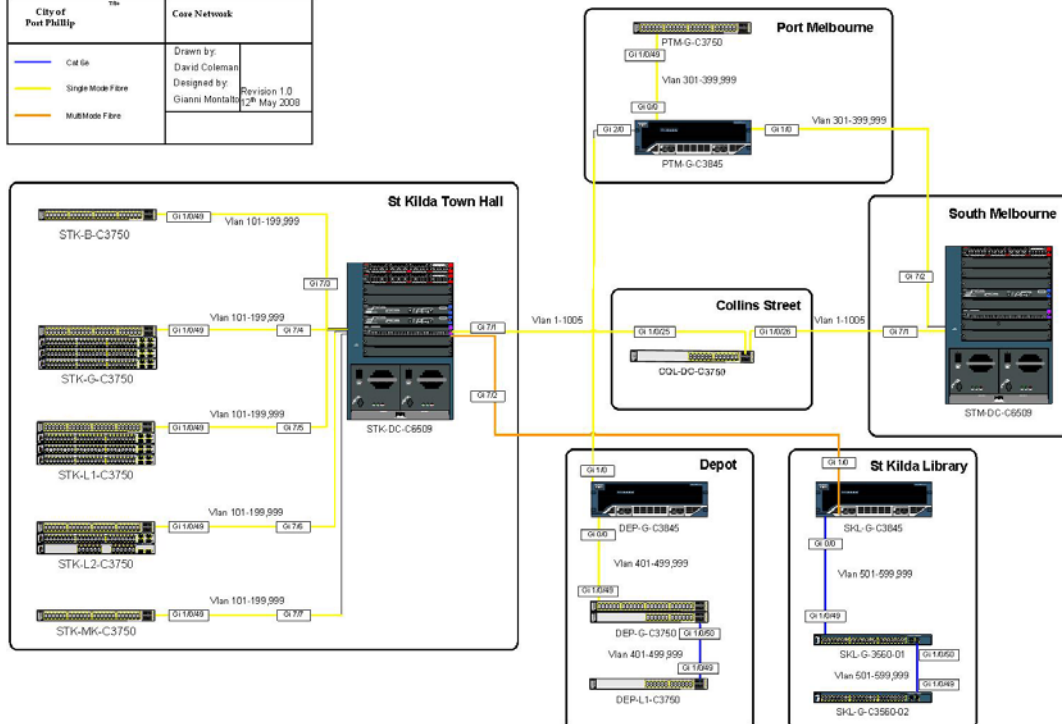
1 Network Design

City of Port Phillip Wide Area Network



Please note that the Dark Fibre connections are single core connections and no additional fibre pairs can be deployed.

City of Port Phillip	Core Network
<ul style="list-style-type: none"> Blue line: Cat 6e Yellow line: Single Mode Fibre Orange line: Multimode Fibre 	Drawn by: David Coleman Designed by: Gianni Montalbano Revision 1.0 May 2009



All routing/switching environments are Cisco with the core switch at St Kilda & South Melbourne being a Cisco 6509E running a Sup720b-3b (12.2SHX) controller. St Kilda Library, Port Melbourne & Depot routers are Cisco 3845's
Edge switches are either Cisco 2811's in remote sites, 3560's in smaller sites or Cisco 3750's in larger sites.

The environment is fully routed using EIGRP with all unknown routes being directed to the inside interface of the firewall

The Main data centre is currently located in St Kilda Town Hall. The location of the proposed DR Centre is the South Melbourne Town Hall. By the time of implementation it is envisaged that the two Town Halls will be connected by a 10Gb Link.

1.1 St Kilda Router Config

```
upgrade fpd auto
version 12.2
service nagle
no service pad
service telnet-zeroidle
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service counters max age 5
!
hostname STK-DC-C6509
!
boot-start-marker
boot-end-marker
!
logging buffered 16384 debugging
enable secret 5 $1$VSn/$tQuX4ly3ihx5ILtemC88V.
!
username Xxxxxxxx password 7 061107710D5D1D115703
no aaa new-model
clock timezone AEST 10
clock summer-time AEDT date Oct 5 2008 2:00 Apr 5 2009 3:00
call-home
  alert-group configuration
  alert-group diagnostic
  alert-group environment
  alert-group inventory
  alert-group syslog
profile "CiscoTAC-1"
  no active
  no destination transport-method http
  destination transport-method email
  destination address email callhome@cisco.com
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

```
subscribe-to-alert-group diagnostic severity minor
subscribe-to-alert-group environment severity minor
subscribe-to-alert-group syslog severity major pattern ".*"
subscribe-to-alert-group configuration periodic monthly 4 17:02
subscribe-to-alert-group inventory periodic monthly 4 16:47
ip subnet-zero
!
!
!
ip domain-name portphillip.vic.gov.au
ip name-server 172.16.4.47
ip name-server 192.168.2.151
udld enable

vtp domain COPP
vtp mode transparent
mls netflow interface
no mls flow ip
mls qos map cos-dscp 0 8 16 24 32 46 48 56
no mls qos rewrite ip dscp
mls qos
mls cef error action reset
!
object-group ip address iscsimgtaddr
host 10.10.40.11
host 10.10.40.10
host 10.10.60.10
host 10.10.60.11
host 10.10.36.63
host 10.10.36.15
host 10.10.36.16
host 172.16.4.24
host 10.10.40.19
host 10.10.40.12
host 10.10.36.120
host 10.10.37.11
host 10.10.37.12
!
object-group ip port iscsimgtports
eq 80
eq 22
eq 443
range 1433 1434
!
!
redundancy
keepalive-enable
mode sso
main-cpu
auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 101-199,910-911 priority 8192
diagnostic cns publish cisco.cns.device.diag_results
```

```
diagnostic cns subscribe cisco.cns.device.diag_commands
!  
vlan internal allocation policy ascending  
vlan access-log ratelimit 2000  
!  
vlan 10  
  name Legacy_Vlan_10  
!  
vlan 99  
  name fw-outside  
!  
vlan 101  
  name STK-MGMT-101  
!  
vlan 102  
  name STK-SVR-102  
!  
vlan 103  
  name STK-DATA-103  
!  
vlan 104  
  name STK-VOICE-104  
!  
vlan 105  
  name STK-WIFI-105  
!  
vlan 106  
  name STK-PUBLIC-106  
!  
vlan 107  
  name STK-NAC-107  
!  
vlan 109  
  name STK-iSCSI  
!  
vlan 110  
  name STK-WIFIMGMT-110  
!  
vlan 198  
  name STK-WAN-198  
!  
vlan 201  
  name STH-MGMT-201  
!  
vlan 254  
  name Temp_Vlan_254  
!  
vlan 301  
!  
vlan 401  
  name Temporary_Library_Fibre_link  
!  
vlan 666  
  name STK-FW-OUTSIDE-666  
!
```

```

vlan 910
 name STK-LEGACY-DATA-910
!
vlan 911
 name STK-LEGACY-DATA-911
!
vlan 999
 name NATIVE-VLAN-999
!
class-map match-any 512K-3phones-remote-sites
 match access-group name police-to-512K-3phones-remote-sites
class-map match-any 2MB-2phones-remote-sites
 match access-group name police-to-2MB-2phones-remote-sites
class-map match-any 2MB-4phones-remote-sites
 match access-group name police-to-2MB-4phones-remote-sites
class-map match-any 512K-1phone-remote-sites
 match access-group name police-to-512K-1phone-remote-sites
class-map match-any 10MB-4phones-remote-sites
 match access-group name police-to-10MB-4phones-remote-sites
class-map match-any 10MB-8phones-remote-sites
 match access-group name police-to-10MB-8phones-remote-sites
class-map match-all voice
 match ip dscp ef
!
!
policy-map ericsson-remote-sites
 class 10MB-8phones-remote-sites
  police 8500000 conform-action transmit exceed-action drop
 class 10MB-4phones-remote-sites
  police 9000000 conform-action transmit exceed-action drop
 class 2MB-4phones-remote-sites
  police 1000000 conform-action transmit exceed-action drop
 class 2MB-2phones-remote-sites
  police 1200000 conform-action transmit exceed-action drop
 class 512K-3phones-remote-sites
  police 220000 conform-action transmit exceed-action drop
 class 512K-1phone-remote-sites
  police 350000 conform-action transmit exceed-action drop
!
interface GigabitEthernet7/1
 description Cisco Wireless LAN Controller
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 105,110
 switchport mode trunk
 channel-group 11 mode on
!
interface GigabitEthernet7/2
 description Cisco Wireless LAN Controller
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 105,110
 switchport mode trunk
 channel-group 11 mode on
!

```

```
interface GigabitEthernet7/3
description STK-B-C3750 1/0/49
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 101-199,999
switchport mode trunk
mls qos trust cos
!
interface GigabitEthernet7/4
description STK-G-C3750 1/0/49
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 101-199,999
switchport mode trunk
mls qos trust cos
!
interface GigabitEthernet7/5
description STK-L1-C3750 1/0/49
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 101-199,999
switchport mode trunk
mls qos trust cos
!
interface GigabitEthernet7/6
description STK-L2-C3750 1/0/49
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 101-199,999
switchport mode trunk
mls qos trust cos
!
interface GigabitEthernet7/7
description STK-MK-C3750 1/0/49
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 1,101-199,999
switchport mode trunk
mls qos trust cos
!
interface GigabitEthernet7/8
description Stk-Chamber-C3560PoE
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 1,101-199,999
switchport mode trunk
mls qos trust cos
!
interface GigabitEthernet7/9
```

```
no ip address
shutdown
!
interface GigabitEthernet7/10
description STKPABX-L1-C3560
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 1,101-199,201,999
switchport mode trunk
mls qos trust cos
!
interface GigabitEthernet7/11
no ip address
shutdown
!
interface GigabitEthernet7/12
description 232Carlisle-L1-C3750
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 1,101-199,999
switchport mode trunk
mls qos trust cos
!
interface GigabitEthernet7/13
no ip address
shutdown
!
interface GigabitEthernet7/14
description STK-MK-C3750 Spare
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 1,101-199,999
switchport mode trunk
mls qos trust cos
!
interface GigabitEthernet7/15
no ip address
shutdown
!
interface GigabitEthernet7/16
no ip address
shutdown
!
interface GigabitEthernet7/17
no ip address
shutdown
!
interface GigabitEthernet7/18
no ip address
shutdown
!
interface GigabitEthernet7/19
```

```
description STKLIB-G-C3845 1/0
ip address 192.168.254.1 255.255.255.252
no ip redirects
no ip proxy-arp
mls qos trust dscp
!
interface GigabitEthernet7/20
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 1,101-199,999
switchport mode trunk
mls qos trust cos
!
interface GigabitEthernet7/21
description .
switchport
switchport mode access
mls qos trust cos
!
interface GigabitEthernet7/22
description stkilda-sw04 0/1
switchport
switchport mode access
mls qos trust cos
!
interface GigabitEthernet7/23
description .
switchport
switchport mode access
switchport nonegotiate
mls qos trust cos
!
interface GigabitEthernet7/24
description 530Collins
switchport
switchport trunk encapsulation dot1q
switchport mode trunk
mls qos trust cos
!
interface Vlan1
ip address 172.16.0.254 255.255.248.0 secondary
ip address 192.168.10.2 255.255.255.0 secondary
ip address 192.168.1.1 255.255.255.0
ip helper-address 172.16.4.47
no ip redirects
ip directed-broadcast
no ip proxy-arp
!
interface Vlan99
no ip address
!
interface Vlan101
description STK Management VLAN
ip address 10.10.32.1 255.255.252.0
```

```
!  
interface Vlan102  
description STK Server VLAN  
ip address 10.10.36.1 255.255.252.0  
ip helper-address 172.16.4.47  
!  
interface Vlan103  
description STK Data VLAN  
ip address 10.10.40.1 255.255.252.0  
ip helper-address 172.16.4.47  
ip helper-address 172.16.4.28  
!  
interface Vlan104  
description STK Voice VLAN  
ip address 10.10.44.1 255.255.252.0  
ip helper-address 172.16.4.47  
!  
interface Vlan105  
description STK Wireless VLAN  
ip address 10.10.48.1 255.255.252.0  
ip helper-address 172.16.4.47  
!  
interface Vlan106  
description STK Public VLAN  
ip address 10.10.52.1 255.255.252.0  
!  
interface Vlan107  
description STK NAC VLAN  
ip address 10.10.56.1 255.255.252.0  
!  
interface Vlan108  
description COPP VPN  
ip address 10.10.60.1 255.255.252.0  
!  
interface Vlan109  
description STK-iSCSI  
ip address 10.10.64.1 255.255.255.0  
!  
interface Vlan110  
description Wireless Network Management VLAN  
ip address 10.10.68.1 255.255.252.0  
ip helper-address 172.16.4.47  
!  
interface Vlan198  
description STK WAN VLAN  
ip address 10.10.248.1 255.255.252.0  
!  
interface Vlan254  
ip address 192.168.254.253 255.255.255.252  
!  
interface Vlan666  
description STK Firewall Inside VLAN  
ip address 10.10.252.1 255.255.252.0  
!  
router eigrp 100
```

```
network 10.0.0.0
network 172.16.0.0
network 192.168.0.0
network 192.168.1.0
network 192.168.254.0
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.3
!
no ip http server
no ip http secure-server
!
ip access-list extended ISCSI
permit icmp host 10.10.64.1 10.10.64.0 0.0.0.255
permit icmp addrgroup iscsimgtaddrs 10.10.64.0 0.0.0.255
permit tcp addrgroup iscsimgtaddrs host 10.10.64.11 portgroup iscsimgtports
permit tcp addrgroup iscsimgtaddrs host 10.10.64.12 portgroup iscsimgtports
ip access-list extended police-to-10MB-4phones-remote-sites
permit ip any 10.170.40.0 0.0.0.255
permit ip any 10.180.40.0 0.0.0.255
ip access-list extended police-to-10MB-8phones-remote-sites
permit ip any 10.140.40.0 0.0.0.255
permit ip any 10.70.40.0 0.0.0.255
ip access-list extended police-to-2MB-2phones-remote-sites
permit ip any 10.80.40.0 0.0.0.255
permit ip any 10.110.40.0 0.0.0.255
ip access-list extended police-to-2MB-4phones-remote-sites
permit ip any 10.190.40.0 0.0.0.255
ip access-list extended police-to-512K-1phone-remote-sites
permit ip any 10.90.40.0 0.0.0.255
ip access-list extended police-to-512K-3phones-remote-sites
permit ip any 10.100.40.0 0.0.0.255
permit ip any 10.130.40.0 0.0.0.255
permit ip any 10.120.40.0 0.0.0.255
!
logging 10.10.36.63
access-list 20 permit 128.250.5.101
access-list 49 permit 10.10.37.47
access-list 49 permit 10.10.37.46
access-list 49 permit 10.10.36.63
access-list 49 deny any
access-list dynamic-extended
snmp-server community public RO 49
snmp-server community COPP RW 49
snmp-server packetsize 4096
snmp-server location STK Data Centre
snmp-server contact Helpdesk 03 9209 6595
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps config
snmp-server enable traps syslog
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps envmon fan shutdown supply temperature
```

```
snmp-server host 10.10.36.63 COPP config syslog envmon
snmp-server host 10.10.37.46 COPP config syslog envmon
snmp-server host 10.10.37.47 COPP config syslog envmon
```

```
!
```

```
control-plane
```

```
!
```

```
dial-peer cor custom
```

```
!
```

```
banner motd
```

```
***** Authorised use only *****
```

```
**** City of Port Phillip ****
```

```
*****
```

```
*
```

```
*
```

```
* WARNING: Under Australian law, it is a criminal offence to:
```

```
*
```

```
* i. Obtain access to data without authority *
```

```
* (Penalty 2 years imprisonment) *
```

```
* ii. Damage, delete, alter or insert data without authority *
```

```
* (Penalty 10 years imprisonment) *
```

```
*
```

```
*
```

```
*****
```

```
ntp logging
```

```
ntp source Vlan101
```

```
ntp update-calendar
```

```
ntp server 10.20.32.1
```

```
ntp server 128.250.36.2 prefer
```

```
!
```

```
end
```

1.2 South Melbourne Router Config

```
!  
!  
upgrade fpd auto  
version 12.2  
service nagle  
no service pad  
service telnet-zeroidle  
service tcp-keepalives-in  
service tcp-keepalives-out  
service timestamps debug datetime localtime show-timezone  
service timestamps log datetime localtime show-timezone  
service password-encryption  
service counters max age 5  
!  
hostname STH-DC-C6509  
!  
boot-start-marker  
boot-end-marker  
!  
logging buffered 16384 debugging  
enable secret 5 $1$HvZB$x43hPcRRyOI9q4/0t4g7K0  
!  
username Xxxxxxxx password 7 061107710D5D1D115703  
no aaa new-model  
clock timezone AEST 10  
clock summer-time AEDT date Oct 5 2008 2:00 Apr 5 2009 3:00  
call-home  
  alert-group configuration  
  alert-group diagnostic  
  alert-group environment  
  alert-group inventory  
  alert-group syslog  
profile "CiscoTAC-1"  
  no active  
  no destination transport-method http  
  destination transport-method email  
  destination address email callhome@cisco.com  
  destination address http  
https://tools.cisco.com/its/service/oddce/services/DDCEService  
  subscribe-to-alert-group diagnostic severity minor  
  subscribe-to-alert-group environment severity minor  
  subscribe-to-alert-group syslog severity major pattern ".*"  
  subscribe-to-alert-group configuration periodic monthly 11 16:09  
  subscribe-to-alert-group inventory periodic monthly 11 15:54  
ip subnet-zero  
!  
!  
!  
ip domain-name portphillip.vic.gov.au  
ip name-server 172.16.4.47  
ip name-server 192.168.2.151  
uddl enable
```

```
vtp domain COPP
vtp mode transparent
mls netflow interface
no mls flow ip
mls qos map cos-dscp 0 10 18 24 34 46 48 56
mls qos
mls cef error action reset
!
!
redundancy
keepalive-enable
mode sso
main-cpu
  auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1,200-299,920 priority 8192
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 10
  name LEGACY_VLAN_10
!
vlan 101
  name LEGACY-VLAN-101
!
vlan 200
  name STH-MGMT-200
!
vlan 201
  name LEGACY-VLAN-201
!
vlan 202
  name STH-SVR-202
!
vlan 203
  name STH-DATA-203
!
vlan 204
  name STH-VOICE-204
!
vlan 205
  name STH-WIFI-205
!
vlan 206
  name STH-PUBLIC-206
!
vlan 207
  name STH-NAC-207
!
```

```
vlan 253
 name Temp_Link_7204
!
vlan 254
 name Temp_Vlan_254
!
vlan 298
 name STH-WAN-298
!
vlan 555
 name LEGACY-VLAN-555
!
vlan 920
 name LEGACY_VLAN_920
!
vlan 999
 name NATIVE-VLAN-999
!
interface GigabitEthernet7/1
 description link to 530 Collins
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mls qos trust cos
!
interface GigabitEthernet7/2
 description Trunk link to Port Melbourne Town Hall
 ip address 192.168.254.5 255.255.255.252
 no ip redirects
 no ip proxy-arp
 mls qos trust dscp
!
interface GigabitEthernet7/3
 description link to 228 Bank Street
 switchport
 switchport access vlan 201
 switchport mode access
!
interface GigabitEthernet7/4
 description STH-L1-C3750E Ground floor
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
!
interface GigabitEthernet7/5
 description sthmelb-r01
 switchport
 switchport trunk encapsulation isl
 switchport mode trunk
!
interface GigabitEthernet7/6
 no ip address
 shutdown
!
```

```
interface GigabitEthernet7/7
no ip address
shutdown
!
interface GigabitEthernet7/8
no ip address
shutdown
!
interface GigabitEthernet7/9
no ip address
shutdown
!
interface GigabitEthernet7/10
no ip address
shutdown
!
interface GigabitEthernet7/11
no ip address
shutdown
!
interface GigabitEthernet7/12
no ip address
shutdown
!
interface GigabitEthernet7/13
no ip address
shutdown
!
interface GigabitEthernet7/14
no ip address
shutdown
!
interface GigabitEthernet7/15
no ip address
shutdown
!
interface GigabitEthernet7/16
no ip address
shutdown
!
interface GigabitEthernet7/17
no ip address
shutdown
!
interface GigabitEthernet7/18
no ip address
shutdown
!
interface GigabitEthernet7/19
no ip address
shutdown
!
interface GigabitEthernet7/20
no ip address
shutdown
```

```
!  
interface GigabitEthernet7/21  
no ip address  
shutdown  
!  
interface GigabitEthernet7/22  
no ip address  
shutdown  
!  
interface GigabitEthernet7/23  
no ip address  
shutdown  
!  
interface GigabitEthernet7/24  
no ip address  
shutdown  
!  
interface Vlan1  
no ip address  
shutdown  
!  
interface Vlan10  
description Link to sthmelb-r01  
ip address 192.168.68.101 255.255.255.0  
shutdown  
!  
interface Vlan200  
description STH-MGMT-200  
ip address 10.20.32.1 255.255.252.0  
!  
interface Vlan201  
description 172.16.4.28 is Zenworks BOOTP server and 172.16.4.47 is Windows  
DHCP server  
ip address 192.168.12.1 255.255.255.0 secondary  
ip address 192.168.204.1 255.255.255.0 secondary  
ip address 192.168.2.1 255.255.255.0  
ip helper-address 172.16.4.47  
ip helper-address 172.16.4.28  
no ip redirects  
ip directed-broadcast  
no ip proxy-arp  
!  
interface Vlan202  
description STH-SVR-202  
ip address 10.20.36.1 255.255.252.0  
ip helper-address 172.16.4.47  
!  
interface Vlan203  
description STH-DATA-203  
ip address 10.20.40.1 255.255.252.0  
ip helper-address 172.16.4.47  
ip helper-address 172.16.4.28  
ip directed-broadcast  
!  
interface Vlan204
```

```
description STH-Voice-204
ip address 10.20.44.1 255.255.252.0
ip helper-address 172.16.4.47
!
interface Vlan205
description STH-WIFI-205
ip address 10.20.48.1 255.255.252.0
ip helper-address 172.16.4.47
shutdown
!
interface Vlan206
description STH-Public-206
ip address 10.20.52.1 255.255.252.0
ip helper-address 172.16.4.47
shutdown
!
interface Vlan207
description STH-NAC-207
ip address 10.20.56.1 255.255.252.0
ip helper-address 172.16.4.47
shutdown
!
interface Vlan253
ip address 192.168.253.253 255.255.255.252
!
interface Vlan254
ip address 192.168.254.254 255.255.255.252
!
interface Vlan298
description STH-WAN-298
ip address 10.20.248.1 255.255.252.0
ip helper-address 172.16.4.47
!
router eigrp 100
network 10.0.0.0
network 192.168.2.0
network 192.168.12.0
network 192.168.68.0
network 192.168.253.0
network 192.168.254.0
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.254.253
!
no ip http server
no ip http secure-server
!
logging 10.10.36.63
access-list 49 permit 10.10.37.47
access-list 49 permit 10.10.37.46
access-list 49 permit 10.10.36.63
access-list 49 deny any
snmp-server community public RO 49
snmp-server community COPP RW 49
```

```

snmp-server packetsize 4096
snmp-server location STH Data Centre
snmp-server contact Helpdesk 03 9209 6595
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps config
snmp-server enable traps syslog
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps envmon fan shutdown supply temperature
snmp-server host 10.10.36.63 COPP config syslog envmon
snmp-server host 10.10.37.46 COPP config syslog envmon
snmp-server host 10.10.37.47 COPP config syslog envmon
!
control-plane
!
dial-peer cor custom
!
banner motd
        ***** Authorised use only *****

        **** City of Port Phillip ****

*****
*
*
* WARNING: Under Australian law, it is a criminal offence to:
* i. Obtain access to data without authority
* (Penalty 2 years imprisonment)
* ii. Damage, delete, alter or insert data without authority
* (Penalty 10 years imprisonment)
*
*****

!
transport input telnet ssh
!
ntp logging
ntp source Vlan200
ntp update-calendar
ntp server 10.10.32.1
ntp server 128.250.36.2 prefer
!
end

```

1.3 Port Melbourne Router Config

```
version 12.4
service nagle
no service pad
service telnet-zeroidle
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname PML-G-C3845
!
boot-start-marker
boot system flash:c3845-ipbasek9-mz.124-17.bin
boot-end-marker
!
logging buffered 16384 debugging
logging rate-limit console all 15
enable secret 5 $1$JPV2$F9gCLk2Jybf5U7bYSeG/0
!
no aaa new-model
clock timezone AEST 10
clock summer-time AEDT recurring last Sun Aug 2:00 last Sun Mar 3:00
no ip source-route
ip cef
!
no ip bootp server
no ip domain lookup
ip domain name portphillip.vic.gov.au
ip name-server 172.16.4.47
ip name-server 192.168.2.151

username xxxxxxxx password 7 061107710D5D1D115703
ip ssh version 2

interface GigabitEthernet0/0
no ip address
no ip redirects
no ip proxy-arp
duplex auto
speed auto
media-type sfp
!
interface GigabitEthernet0/0.301
description PML Management VLAN
encapsulation dot1Q 301
ip address 10.30.32.1 255.255.252.0
ip helper-address 172.16.4.47
!
interface GigabitEthernet0/0.302
description PML Server VLAN
encapsulation dot1Q 302
ip address 10.30.36.1 255.255.252.0
```

```
ip helper-address 172.16.4.47
!
interface GigabitEthernet0/0.303
description PML Data VLAN
encapsulation dot1Q 303
ip address 10.30.40.1 255.255.252.0
ip helper-address 172.16.4.47
ip helper-address 172.16.4.28
ip directed-broadcast
!
interface GigabitEthernet0/0.304
description PML Voice VLAN
encapsulation dot1Q 304
ip address 10.30.44.1 255.255.252.0
ip helper-address 172.16.4.47
!
interface GigabitEthernet0/0.305
description PML Wireless VLAN
encapsulation dot1Q 305
ip address 10.30.48.1 255.255.252.0
ip helper-address 172.16.4.47
!
interface GigabitEthernet0/0.306
description PML Public VLAN
encapsulation dot1Q 306
ip address 10.30.52.1 255.255.252.0
ip helper-address 172.16.4.47
!
interface GigabitEthernet0/0.307
description PML NAc VLAN
encapsulation dot1Q 307
ip address 10.30.56.1 255.255.252.0
ip helper-address 172.16.4.47
!
interface GigabitEthernet0/0.999
description Native VLAN
encapsulation dot1Q 999
ip helper-address 172.16.4.47
!
interface GigabitEthernet0/1
description Backup Ethernet Link to STKLIB-G-C3845 0/1
bandwidth 100
ip address 192.168.254.13 255.255.255.252
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet1/0
description WAN link to STH-DC-6509
ip address 192.168.254.6 255.255.255.252
ip helper-address 172.16.4.47
negotiation auto
!
interface GigabitEthernet2/0
description WAN link to DEPOT
```

```

ip address 192.168.254.9 255.255.255.252
ip helper-address 172.16.4.47
negotiation auto
!
router eigrp 100
network 10.0.0.0
network 192.168.254.0
no auto-summary
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
logging history informational
logging facility local5
logging 10.10.36.63
access-list 49 permit 10.10.37.46
access-list 49 permit 10.10.36.63
access-list 49 deny any
snmp-server community public RO 49
snmp-server community COPP RW 49
snmp-server packet-size 4096
snmp-server location STK Data Centre
snmp-server contact Helpdesk 03 9209 6595
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps envmon fan shutdown supply temperature
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps syslog
snmp-server host 10.10.36.63 COPP envmon config syslog
snmp-server host 10.10.37.46 COPP envmon config syslog
!
control-plane
banner motd
        ***** Authorised use only *****
        ***** City of Port Phillip *****

*****
*
*
* WARNING: Under Australian law, it is a criminal offence to:
* i. Obtain access to data without authority
* (Penalty 2 years imprisonment)
* ii. Damage, delete, alter or insert data without authority
* (Penalty 10 years imprisonment)
*
*****

banner prompt-timeout
FAIL : Only Authorised Users may log into this system!!!!
transport input telnet ssh
scheduler allocate 20000 1000
ntp server 172.16.0.11
end

```

1.4 Depot Router Config

```
! No configuration change since last restart
version 12.4
service nagle
no service pad
service telnet-zeroidle
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname DEP-G-C3845
!
boot-start-marker
boot system flash:c3845-ipbasek9-mz.124-17.bin
boot-end-marker
!
logging buffered 16384 debugging
logging rate-limit console all 15
no logging console
enable secret 5 $1$sac9$uWqVlyXL1.7iF9hCPQNx6/
!
no aaa new-model
clock timezone AEST 10
clock summer-time AEDT recurring last Sun Aug 2:00 last Sun Mar 3:00
no ip source-route
ip cef
!
ip dhcp use vrf connected
!
no ip bootp server
ip domain name portphillip.vic.gov.au
ip name-server 172.16.4.47
ip name-server 192.168.2.151
!
username xxxxxxxx password 7 061107710D5D1D115703
!
interface GigabitEthernet0/0
description WAN link to Port Melbourne
ip address 192.168.254.10 255.255.255.252
no ip redirects
no ip proxy-arp
duplex auto
speed auto
media-type sfp
!
interface GigabitEthernet0/1
no ip address
shutdown
```

```
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet1/0
no ip address
no ip redirects
no ip proxy-arp
negotiation auto
!
interface GigabitEthernet1/0.401
description DEP Management VLAN
encapsulation dot1Q 401
ip address 10.40.32.1 255.255.252.0
ip helper-address 172.16.4.47
!
interface GigabitEthernet1/0.402
description DEP Server VLAN
encapsulation dot1Q 402
ip address 10.40.36.1 255.255.252.0
ip helper-address 172.16.4.47
!
interface GigabitEthernet1/0.403
description DEP Data VLAN
encapsulation dot1Q 403
ip address 10.40.40.1 255.255.252.0
ip helper-address 172.16.4.47
ip helper-address 172.16.4.28
ip directed-broadcast
!
interface GigabitEthernet1/0.404
description DEP Voice VLAN
encapsulation dot1Q 404
ip address 10.40.44.1 255.255.252.0
ip helper-address 172.16.4.47
!
interface GigabitEthernet1/0.405
description DEP Wireless VLAN
encapsulation dot1Q 405
ip address 10.40.48.1 255.255.252.0
!
interface GigabitEthernet1/0.406
description DEP Public VLAN
encapsulation dot1Q 406
ip address 10.40.52.1 255.255.252.0
!
interface GigabitEthernet1/0.407
description DEP NAc VLAN
encapsulation dot1Q 407
ip address 10.40.56.1 255.255.252.0
!
interface GigabitEthernet1/0.940
description DEP Legacy VLAN
encapsulation dot1Q 940
ip address 192.168.14.1 255.255.255.0 secondary
```

```

ip address 192.168.4.1 255.255.255.0
ip helper-address 172.16.4.47
ip helper-address 172.16.4.28
!
interface GigabitEthernet1/0.999
description Native VLAN
encapsulation dot1Q 999
!
router eigrp 100
network 10.0.0.0
network 192.168.254.0
no auto-summary
!
no ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
logging history informational
logging facility local5
logging 10.10.36.63
access-list 49 permit 10.10.37.46
access-list 49 permit 10.10.36.63
access-list 49 deny any
snmp-server community public RO 49
snmp-server community COPP RW 49
snmp-server packetsize 4096
snmp-server location Depot Data Centre
snmp-server contact Helpdesk 03 9209 6595
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps envmon fan shutdown supply temperature
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps syslog
snmp-server host 10.10.36.63 COPP envmon config syslog
snmp-server host 10.10.37.46 COPP envmon config syslog
!
control-plane
banner motd
        ***** Authorised use only *****
        ***** City of Port Phillip *****

*****
*
*
* WARNING: Under Australian law, it is a criminal offence to:
*
* i. Obtain access to data without authority
* (Penalty 2 years imprisonment)
*
* ii. Damage, delete, alter or insert data without authority
* (Penalty 10 years imprisonment)
*
*
*****

banner prompt-timeout
FAIL : Only Authorised Users may log into this system!!!!

```

```
scheduler allocate 20000 1000
ntp server 172.16.0.11
!
end
```

1.5 Library Router Config

```
! No configuration change since last restart
version 12.4
service nagle
no service pad
service telnet-zeroidle
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname STKLIB-G-C3845
!
boot-start-marker
boot system flash:c3845-ipbasek9-mz.124-17.bin
boot-end-marker
!
logging buffered 16384 debugging
logging rate-limit console all 15
enable secret 5 $1$Pjx$ix2yUvaVOJXY4mivNavmj1
!
no aaa new-model
clock timezone AEST 10
clock summer-time AEDT recurring last Sun Aug 2:00 last Sun Mar 3:00
no ip source-route
ip cef
!
no ip bootp server
no ip domain lookup
ip domain name portphillip.vic.gov.au
ip name-server 172.16.4.47
ip name-server 192.168.2.151
!
username xxxxxx password 7 061107710D5D1D115703
!
ip ssh version 2
!
interface GigabitEthernet0/0
description LAN network
no ip address
no ip redirects
no ip proxy-arp
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/0.501
description STKLIB Management VLAN
encapsulation dot1Q 501
ip address 10.50.32.1 255.255.252.0
ip helper-address 172.16.4.47
!
interface GigabitEthernet0/0.502
```

```
description STKLIB Server VLAN
encapsulation dot1Q 502
ip address 10.50.36.1 255.255.252.0
ip helper-address 172.16.4.47
!
interface GigabitEthernet0/0.503
description STKLIB Data VLAN
encapsulation dot1Q 503
ip address 10.50.40.1 255.255.252.0
ip helper-address 172.16.4.47
ip helper-address 172.16.4.28
ip directed-broadcast
!
interface GigabitEthernet0/0.504
description STKLIB Voice VLAN
encapsulation dot1Q 504
ip address 10.50.44.1 255.255.252.0
ip helper-address 172.16.4.47
!
interface GigabitEthernet0/0.505
description STKLIB Wireless VLAN
encapsulation dot1Q 505
ip address 10.50.48.1 255.255.252.0
ip helper-address 172.16.4.47
!
interface GigabitEthernet0/0.506
description STKLIB Public VLAN
encapsulation dot1Q 506
ip address 10.50.52.1 255.255.252.0
ip helper-address 172.16.4.47
!
interface GigabitEthernet0/0.507
description STKLIB NAC VLAN
encapsulation dot1Q 507
ip address 10.50.56.1 255.255.252.0
ip helper-address 172.16.4.47
!
interface GigabitEthernet0/0.950
description STKLIB Legacy VLAN
encapsulation dot1Q 950
ip address 192.168.201.1 255.255.255.0 secondary
ip address 192.168.5.1 255.255.255.0
ip helper-address 172.16.4.47
!
interface GigabitEthernet0/0.999
description Native VLAN
encapsulation dot1Q 999
!
interface GigabitEthernet0/1
description Backup Ethernet Link to PML-G-C3845 0/1
bandwidth 100
ip address 192.168.254.14 255.255.255.252
duplex auto
speed auto
media-type rj45
```

```

!
interface GigabitEthernet1/0
description WAN link to St Kilda Town Hall
ip address 192.168.254.2 255.255.255.252
no ip redirects
no ip proxy-arp
negotiation auto
!
router eigrp 100
network 10.0.0.0
network 192.168.254.0
no auto-summary
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.254.1
no ip http server
no ip http secure-server
!
logging history informational
logging facility local5
logging 10.10.36.63
access-list 49 permit 10.10.37.46
access-list 49 permit 10.10.36.63
access-list 49 deny any
snmp-server community public RO 49
snmp-server community COPP RW 49
snmp-server packetsize 4096
snmp-server location STK Library
snmp-server contact Helpdesk 03 9209 6595
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps envmon fan shutdown supply temperature
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps syslog
snmp-server host 10.10.36.63 COPP envmon config syslog
snmp-server host 10.10.37.46 COPP envmon config syslog
!
control-plane
banner motd
        ***** Authorised use only *****
        ***** City of Port Phillip *****
*****
*
*
* WARNING: Under Australian law, it is a criminal offence to:
* i. Obtain access to data without authority
* (Penalty 2 years imprisonment)
* ii. Damage, delete, alter or insert data without authority
* (Penalty 10 years imprisonment)
*
*****
banner prompt-timeout
FAIL : Only Authorised Users may log into this system!!!!
transport input telnet ssh

```

```

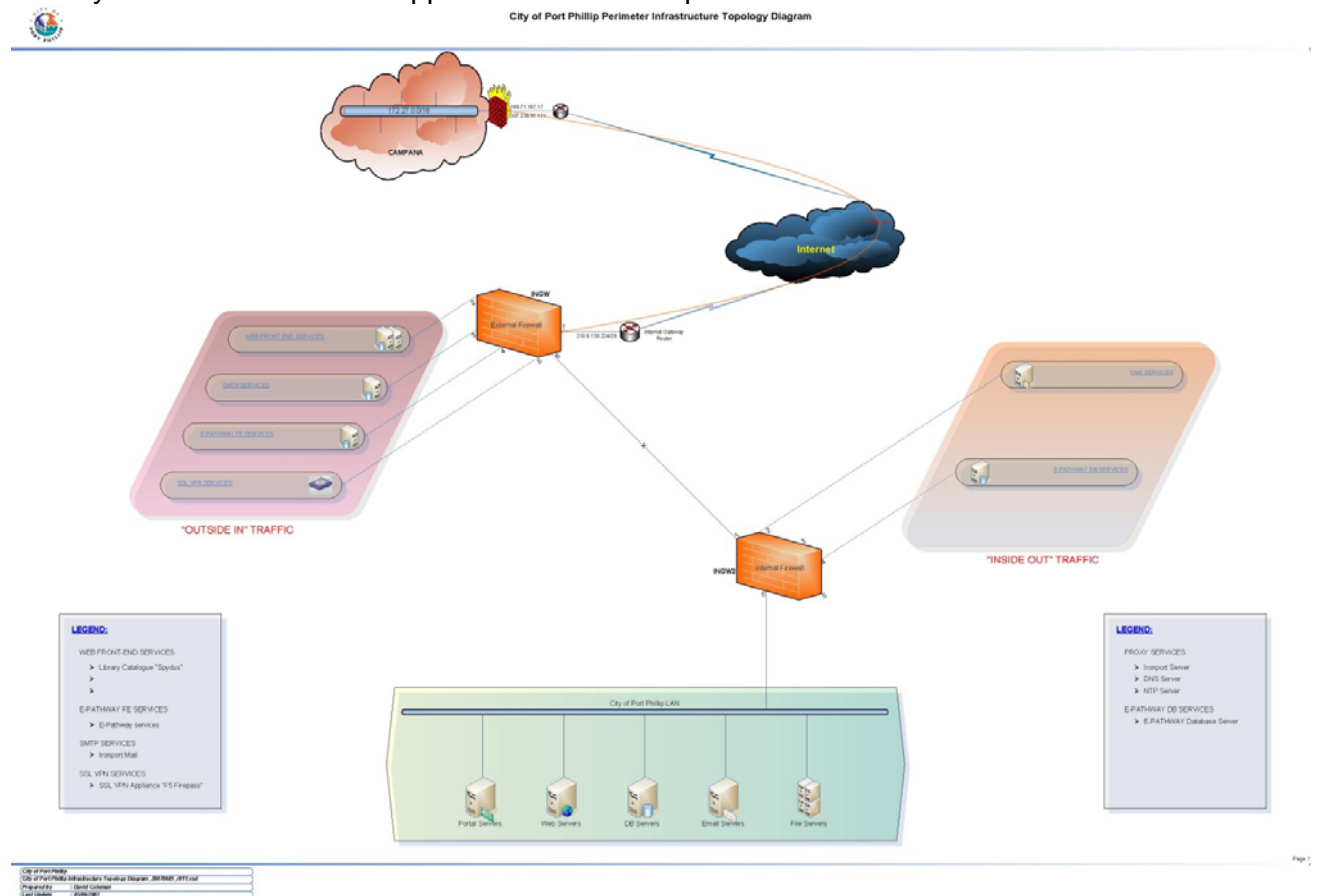
scheduler allocate 20000 1000
ntp server 172.16.0.11
end

```

2 DMZ

The perimeter network/DMZ has been designed in a 2-tier approach with a firewall as a termination for inbound traffic and a firewall as a termination point for outbound traffic. The firewalls are Symantec SG5620 appliances.

There are ~116 rules on each firewall, generally most rule sets are replicated on both firewalls to allow certain outbound traffic through both firewalls. There are a handful of NAT's in place and some port redirections
 3 VPN tunnels exist
 A Deny All unless authorised approach has been implemented.



2.1 Internet Link

The City of Port Phillip has a single internet link which handles all internet traffic and serves the Public IP address ranges. The link is a 100Mb full duplex link. The link utilisation has never peaked above 30% however it is expected to grow, but not exceed 100mb

The router handling internet traffic handles 2 public IP Address ranges:
 210.9.130.224/29
 203.63.91.64/29

2.2 Server Deployment

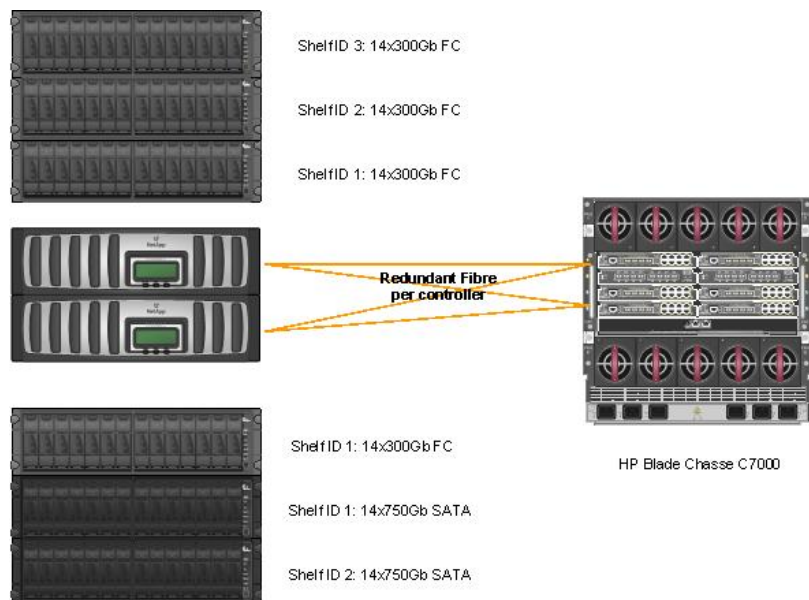
The City of Port Phillip as an environmentally conscious organisation has heavily virtualised the majority of its servers using VMWare ESX v3.5 directly connected to an active/active set of NetApp FAS3020 Filers (SAN/NAS) via a redundant Cisco 9124e Fabric Switch housed in an HP C7000 blade enclosure. The consolidation ratio is presently >10:1, with 6 ESX Hosts presently deployed.

The ESX host hardware is listed below:

Name	Model	CPU	RAM	Mezanin
Stkesx3	HP BL460	2x Quad Core @ 2.33Ghz	16Gb	HBA, 4 Port NIC
Stkesx4	HP BL460	2x Quad Core @ 2.33Ghz	16Gb	HBA, 4 Port NIC
Stkesx5	HP BL460	2x Quad Core @ 2.33Ghz	16Gb	HBA, 4 Port NIC
Stkesx6	HP BL460	2x Quad Core @ 2.33Ghz	16Gb	HBA, 4 Port NIC
Stkesx7	HP BL460	2x Quad Core @ 2.33Ghz	32Gb	HBA, 4 Port NIC
Stkesx8	HP BL460	2x Quad Core @ 2.33Ghz	32Gb	HBA, 4 Port NIC

The virtual machine storage is spread over 2 filers:

Filer	Disk Size	Disk Type	Lun	Partition Format
StkFiler1	500Gb	Fibre Channel	Vm01	VMFS
StkFiler1	500Gb	Fibre Channel	Vm02	VMFS
StkFiler2	500Gb	Fibre Channel	Vm03	VMFS
StkFiler2	500Gb	Fibre Channel	Vm04	VMFS
StkFiler2	500Gb	Fibre Channel	Vm05	VMFS
StkFiler1	500Gb	SATA	Vmtst01	VMFS
StkFiler1	500Gb	SATA	Dmz_vmfs	VMFS



2.3 Exchange 2007

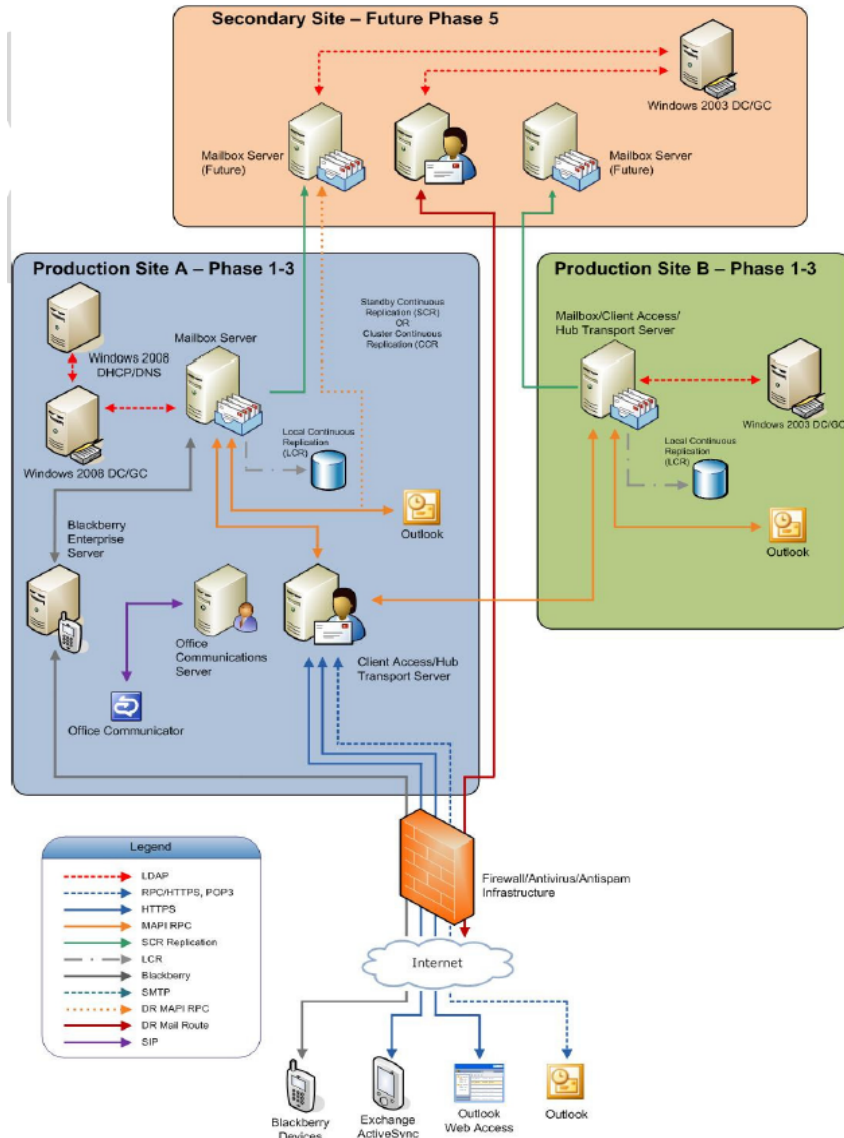
Storage for St Kilda's Primary Exchange 2007 server (Production Site A) including databases and logs is provided by City of Port Phillip's SAN in the following LUN configuration.

Description	Lun Name	Vol Size (Gb)	Distribution
Storage Group 1	EXC001	120	User Mailboxes
Storage Group 2	EXC002	25	User Mailboxes 2
Storage Group 3	EXC003	25	Councillors & Executives
Storage Group 4	EXC004	25	IT Mailbox
Storage Group 5	EXC005	5	Public Folders
Logs	Exclogs001	50	Logs

There are currently no advanced backup/replication options being exercised at the moment. The intent is to deploy SCR for both site A and site B to the South Melbourne DR Site.

The Depot Exchange server (Production Site B) contains local attached storage only.

Presently there are no Hub Transport servers deployed into the DMZ as OWA access is served through our SSL-VPN however in the next upgrade of Exchange we expect to redesign the environment to have a hub transport server in the DMZ serving OWA. We may also include a OCS2007 server for federated chat.



2.4 PABX

The City of Port Phillip runs an Ericsson MD110 PABX system with a mixture of Analogue, Digital & IP extensions. Each major site has a LIM connected back to the GroupSwitch over Ethernet using a HL950 converter.

The MD110 is running revision BC13. Each VOIP connection is running H323 with G711 Codec

