# Detailed Design / ITRON Headend

## Detailed Design

**Date:** 17/03/2023

**Version:** 0.1

**Author:** Adeel Ahmed

# 1 Document Control

## 1.1 Version History

This table shows a record of significant changes to the document.

| Version | Date | Who | Description of Change |
|---|---|---|---|
| 0.1 | | Adeel Ahmed | Initial Draft |
| | | | |
| 1.0 | | | Released Design |
| | | | |

## 1.2 Reviwer of the document is recorded below.

| Reviewer Names | Roles | Organization |
|---|---|---|
| Kevin Wong | Senior ICT Engineer | WEL Network |
| Andrew Mackintosh | Senior ICT Engineer | WEL Network |
| Paul Seddon | Solution Architect | WEL Network |
| Ian Hayton | Head of Strategy & Architecture | WEL Network |
| Kevin Chen | Senior ICT Consultant | ITRON |
| | | |
| | | |
| | | |
| | | |

## 1.3 Distribution Lists

| Copy No | Names | Roles | Organization |
|---|---|---|---|
| 1 | Ray Hardy | | |
| 2 | Paul Seddon | | |
| 3 | Jeffrey Hooper | | |
| 4 | Saran Bibhakar | | |
| 5 | Andrew Bruce | | |
| 6 | Hatzis Mel | | |
| 7 | | | |

| | | | |
|---|---|---|---|
| 8 | | | |
| 9 | | | |

## 1.4 Related Documents

| Item No | Document Descriptions | Document Name |
|---|---|---|
| 1 | ITRON Environment Design | Environment Design - WEL Networks - version-0.10 |
| 2 | ITRON Workshop PPT | WEL Networks Licensed Transition Network Workshop |
| 3 | Oracle ODA online information | https://docs.oracle.com/en/engineered-systems/oracle-database-appliance/19.18/cmtxp/readying-oda.html#GUID-04E47DE5-057A-4BC6-89A8-974F5DA8DBE0 |
| 4 | ODA Datasheet | ODA-X9-2-HA-Datasheet |
| 5 | Keysafe HSM | https://statics.teams.cdn.office.net/evergreen-assets/safelinks/1/atp-safelinks.html |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |

# 2 Table of Contents

# 3 Introduction

## 3.1 Purpose

WEL Networks is an electricity distributor in New Zealand covering the city of HAMILTON and surrounds (south of AUCKLAND). WEL Networks have a current customer base of 70,000 meters and they are planning to increase this base to 100,000 electric meters.

WEL Networks have historically utilized the ITRON Managed Service model to support and maintain their AMI Metering Solution. A decision has been made to move away from a Managed Service engagement in favor of an on premise (Licensed Customer) Solution.

This document aims to describe the design and implementation of the WEL Networks Advanced Metering Infrastructure (AMI) system for supporting a deployment of up to 100,000 electricity meters.

The solution architecture for the WEL Networks On-Premises Migration project head-end system which will serve as the primary control system for the WEL Networks Advanced Metering Infrastructure (AMI) network.

## 3.2 Scope

**In Scope**

This document defines the solution architecture for the WEL Networks On-Premises Migration project head-end system.

- Infrastructure Services including DNS, NTP.
- Network Infrastructure and Firewall.
- Security and Remote Access.

**Out of Scope**

## 3.3 Design Decisions

| | | | |
|---|---|---|---|
| **Subject Area** | SVI on the firewall of App/Oracle/DB/HSM servers | **Topic** | Layer-3 |
| **Architectural Decision** | DEV environment is considered as less likely to be replicated as PROD/DR. | **ID** | 01 |
| **Summary** | SVI of all services will reside on WEL CORP switches | | |

| | | | |
|---|---|---|---|
| **Subject Area** | Bandwidth required between core switches and Cooperate firewalls | **Topic** | Interface total BW |
| **Architectural Decision** | There will be 5 apps servers, 1 DB server and one HSM, bandwidth required likely be less than 1G | **ID** | 02 |
| **Summary** | Existing link between core switches and CORP firewall will not congest | | |

| | | | |
|---|---|---|---|
| **Subject Area** | Oracle ODA connectivity requirement | **Topic** | ODA appliance |
| **Architectural Decision** | DEV-TEST V8300 tunnel router will be running on ODA therefore need to understand the network ports required to be connected | **ID** | 03 |
| **Summary** | One port for iLO and other for data connected directly to core switch. | | |

| | | | |
|---|---|---|---|
| **Subject Area** | HSMs must reside within an isolated VLAN protected by a firewall and be physically separated from the AMI application servers | **Topic** | Isolated VLAN |
| **Architectural Decision** | DEV will not be replicated with PROD/DR | **ID** | 04 |
| **Summary** | Isolated VLANs not protected via firewall | | |

# 4 High Level Overview

WEL Networks intends to have the same application layout on the DEV environment to align with PREPROD and PROD environments application layout. Thus, by leveraging on this AMI deployment, the number of VMs in DEV has been doubled up from 5 VMs to 10 VMs. This will be making the deployment activities easier as having the same number of VMs across all the environments.

## 4.1 Environments

WEL network will have four different environments to deliver the smart meter services. The four environments will be hosts in 2 Data Centres as following

- Production, Preprod and Development: Maui Street Data Centre
- Disaster Recovery: Avalon Drive Data Centre

### 4.1.1 Test/DEV

Used to test application functionality and integration prior to installation in the production environment. The development environment will be sized to support up to 1,000 network endpoints and will be physically hosted in WEL Networks Maui Street Data Centre.

Spark APN will be same as that of PROD and PRE_PROD environments.

ODA will be used to spin up v8300 as Tunnel Router in the DEV and PRE_PROD environments instead of physical 8300 Cisco at this stage due to delivery dates of the equipments/devices.

Once the devices are reached at Auckland, v8300 will be replaced with physical router as tunnel router.

V8300 router will be spinned in ODA who OVF file which will be downloaded from Cisco website. One virtual Cisco C8000v tunnel router will be deployed for terminating PREPROD and DEV AP's 6in4 tunnels in PROD datacentre.

### 4.1.2 Pre-PROD/UAT

Pre-Production Environment (PREPROD) – The PREPROD is used to perform scale and performance testing, user acceptance testing and end-to-end integration testing prior to any changes being applied to the production environment. The environment will be sized to support up to 200K simulated AMI meters and installed on dedicated hardware in WEL Networks Maui Street.

PREPROD and DEV environments, WEL Networks will deploy one Oracle Database Appliances (ODA) X9-2L with the following specification:

- One 2U X9-2L server per system
- Two x Intel® Xeon® S4314 2.4 GHz, 16 cores, 135 watts, 24 MB L3 cache
- One 512 GB (16 x 32 GB) of Memory for ODA X9-2L
- Two internal 240 GB M.2 SSDs (mirrored) per server for Operating System and Oracle Grid Infrastructure (GI) Software
- 13.6 TB of RAW Storage (2 x 6.8 TB NVMe) 6.2 TB mirrored
- Oracle Dual Port 25 Gb Ethernet Adapter

### 4.1.3 Production

Production – Supports the AMI deployment in the WEL Networks electricity network. This environment is sized to support up to 100K electric meters, 100K water meters and associated network equipment (APs, Relays, Micro APs) and is physically hosted at WEL Networks Data Centre in Maui Street.

### 4.1.4 Disaster Recovery

Disaster Recovery (DR) – Replicates the production environment and is designed to operate as the production environment in the event of a planned or unplanned outage at the Maui Street. The DR environment is physically hosted in the Avalon Drive located in WEL Networks HQ.

Production and DR environments, WEL Networks will deploy two Oracle Database Appliances (ODA) X9-2-HA with the following specifications:

- Two 2U X9-2L servers and one 4U DE3-24C storage shelf per system
- Two x Intel® Xeon® Silver 4314 2.4 GHz 16 cores (135 watts, XCC, 24 MB L3 cache)
- Two x 512 GB (16 x 32 GB) of Memory
- Two internal 240 GB M.2 SSDs (mirrored) per server for Operating System and Oracle Grid Infrastructure (GI) Software
- 46 TB of RAW Storage (6 x 7.68 TB SSD) 17.8 TB mirrored
- Oracle Dual Port 25 Gb Ethernet Adapter

## 4.2 Current/Existing Network

Current network connectivity and information has been captured here with the IP addresses provided by ITRON in the workshop.

- 203.109.245.134 = Public IP address from Vodafone for termination of IPsec tunnel.
- 74.121.20.22 = ITRON public IP address for IPsec tunnel.
- 74.121.18.0 = ITRON IP public IP range
- 172.20.116.0/22 = AP via SCADA
- 172.20.119.0/24 = AP via PAPN

## 4.3 Target State of TEST environment

Conceptually, the virtualized server environment has several external IPv4 and IPv6 interfaces. The IPv4 interfaces are used for core administrative services such as NTP, DNS and SSH and for access into and out of the application domain which relies in part on HTTPS, SNMP, SMTP, FTP, JMS, and SCP. The IPv6 interfaces are used for access to the AMI network which relies on an encrypted IPv6-over-IPv4 tunnel for access to the Access Points over either the cellular or WEL Networks Ethernet network.

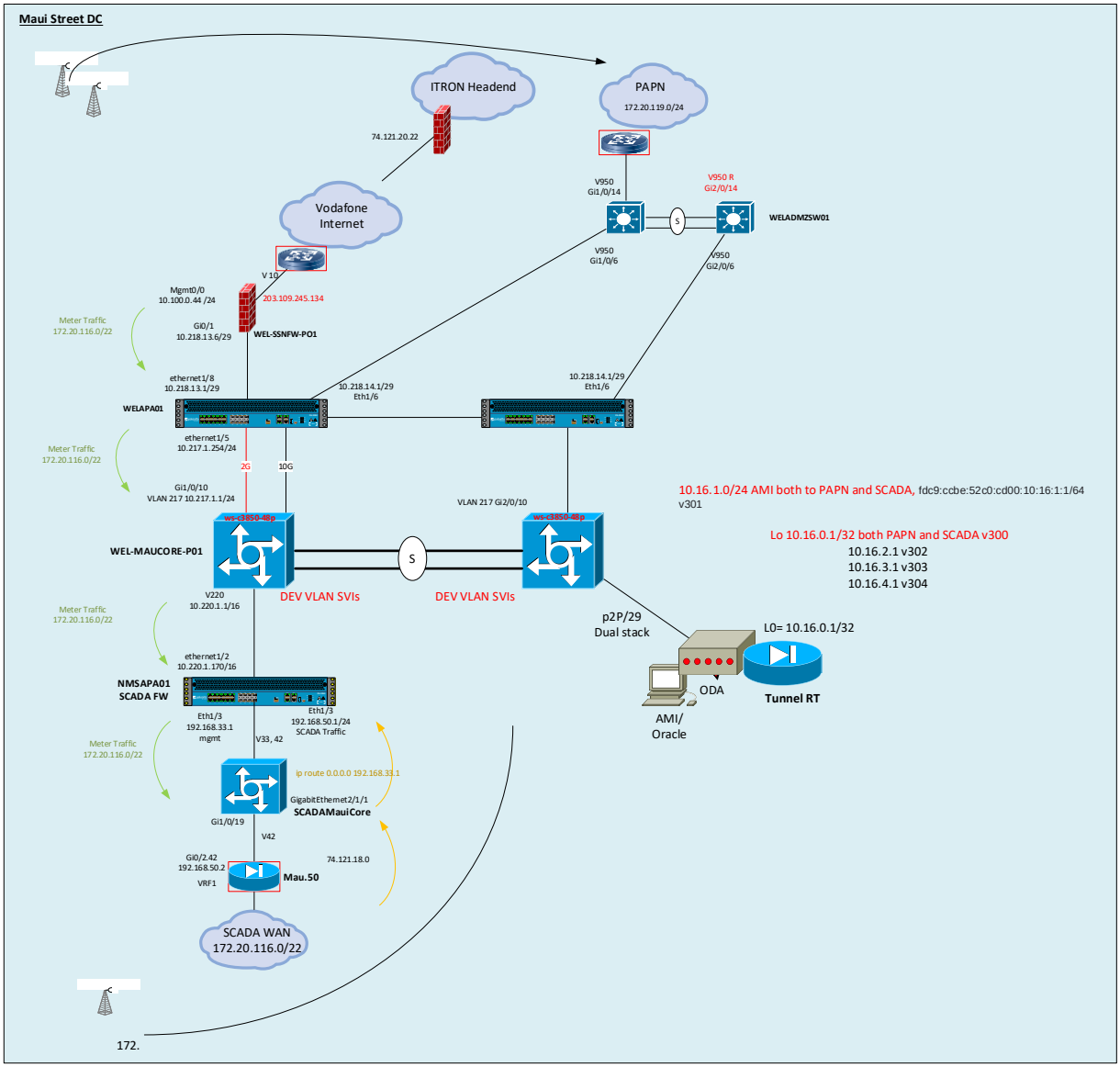


Figure 1: Target Network Topology

## 4.4 AP/Meter Traffic Flow

AP communicates with headend servers with IPv6 and IPv4.

- Each AP builds a 6-in-4 tunnel with IPSEC protection to tunnel router.
- IPv6 traffic is over the established 6-in-4 tunnels.
- IPv4 is used for AP remote management and troubleshooting purpose

Meter communicates with headend servers via IPv6 network only.

- Meter has no IPv4 address.

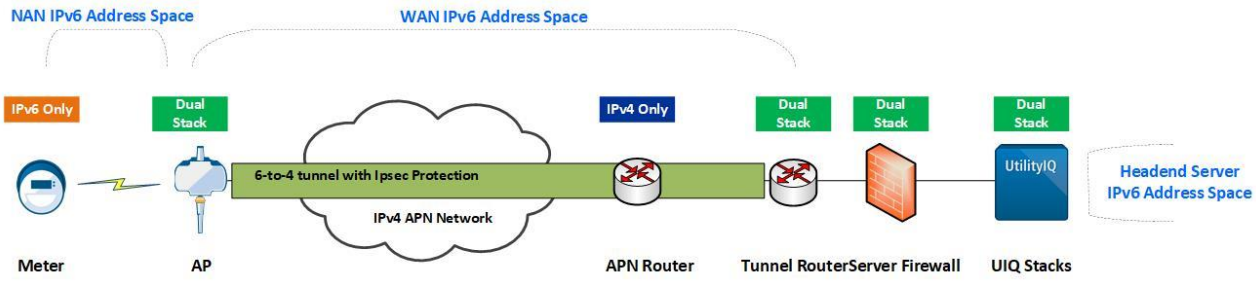


Figure 2: AP/Meter Traffic Flow Diagram

## 4.5 Admin Link

Admin link is the existing IPsec VPN connection between WEL Network's PROD data centree and Itron's LAS datacentre. This admin link needs reconfiguration for admin access by Itron support staff, allowing remote support, deployment services, system health monitoring and data analysis to facilitate WEL Network's business drivers.

This admin link is IPv4 traffic only.

### 4.5.1 Current Admin Link Setup

- FH: Allow WEL to access UIQ in Itron Datacenter. (NAT)
- BH: Route WEL APN network into Itron Datacenter

### 4.5.2 Admin Link during Project Implementation

- FH: Allow WEL to access UIQ in Itron Datacenter
- BH: Route WEL APN network into Itron Datacenter
- Replication: Allow data replication from SaaS to Licensed servers. (NAT if required)
- Admin: Allow Itron project team remotely connect to Licensed networks for implementation. (NAT if required)

### 4.5.3 Admin Link after Project Completion

- Admin: Allow Itron project team remotely connect to Licensed networks for troubleshooting. (NAT if required)
- Admin: Allow Itron Lorenzo remotely collect and analysis the data for operation optimization. (NAT if required)

## 4.6 Oracle Database Appliance ODA

Oracle Database Appliance X9-2-HA is an Oracle Engineered System that saves time and money by simplifying deployment, management, and support of high availability database solutions. Optimized for the world's most popular database— Oracle Database—it integrates software, compute, storage, and network resources to deliver high availability database services for a wide range of custom and packaged online transaction processing (OLTP), in-memory database, and data warehousing applications.

### 4.6.1 Specification of ODA in Test/DEV

PREPROD and DEV environments, WEL Networks will deploy one Oracle Database Appliances (ODA) X9-2L with the following specification:

- One 2U X9-2L server per system
- Two x Intel® Xeon® S4314 2.4 GHz, 16 cores, 135 watts, 24 MB L3 cache
- One 512 GB (16 x 32 GB) of Memory for ODA X9-2L
- Two internal 240 GB M.2 SSDs (mirrored) per server for Operating System and Oracle Grid Infrastructure (GI) Software
- 13.6 TB of RAW Storage (2 x 6.8 TB NVMe) 6.2 TB mirrored
- Oracle Dual Port 25 Gb Ethernet Adapter.

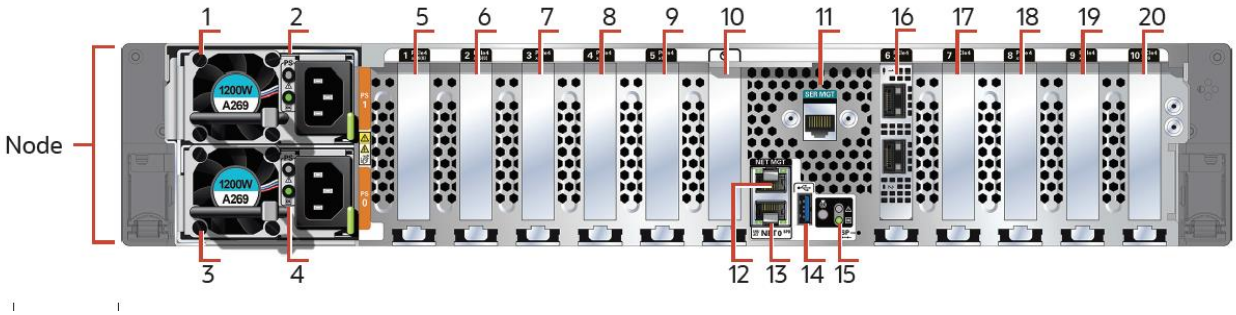


Figure 3: ODA X9-2L

### 4.6.2 ODA Network Ports and Description

| Networking Ports | Description |
|---|---|
| 11 | SER MGT port: RJ-45 serial port used to connect to the Oracle ILOM service processor |
| 12 | NET MGT port: 10/100/1000Base-T network interface port with RJ-45 connector used to connect to the Oracle ILOM service processor |
| 13 | 100/1000Base-T network interface port with RJ-45 connector: NET 0 |

ODA Appliance Management IPv4 = 10.220.2.X (ILO)

## 4.7 HSM (Keysafe)

Keysafe HSMs can be implemented as part of a broader set of security initiatives to achieve compliance with the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) plan. For NERC CIP compliance, the HSMs must reside within an isolated VLAN protected by a firewall and be physically separated from the AMI application servers.

Due to the critical nature of the HSM's role in allowing applications to perform operations on the network (e.g., meter reads, remote connects/disconnects, meter reprogramming, firmware upgrades,

etc.), there are obvious benefits of not introducing additional network constraints and intermediary hardware which could fail and result in a system wide disruption by preventing applications from accessing the HSMs. Given this, it is better if the HSMs are installed within the same VLAN as the application servers (which also obviates the need for more complex firewall rules), however, a separate firewall protected VLAN can be used if the firewall is designed with redundancy and performs to an acceptable level.

Note that there are two RJ45 ports available for connecting a HSM to the network. These will both be set up in a teaming (NIC Bonding) configuration for connecting the HSM to the network

### 4.7.1 HSM Specifications

- 1U 19" Form Factor LAN Device
- Redundant field-replaceable power supply: 2 x 100 ~ 240 V AC, 50 ~ 60 Hertz, 300 W
- Power consumption: typically 45 W / 66 VA, max. 50W / 70VA
- Heat dissipation: max. 171 BTU/hr
- 2 RJ45 1 Gb/s network interfaces
- Operating temperature: +10° C to +40° C (+50° F to +104° F)
- Storage temperature: -10° C to +55° C (+14° F to +131° F)
- Relative humidity: 10% to 95%, non-condensing
- MTBF 100,000 hours at 25°C / 77°F, GB Ambient, GC - Ground Benign, Controlled

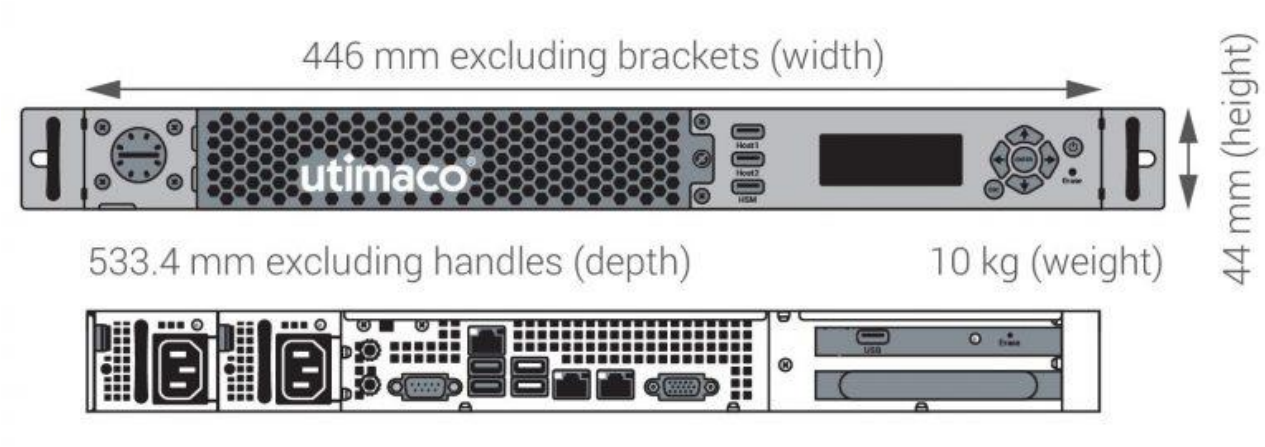


Figure 4: HSM Keysafe

### 4.7.2 Network Ports of HSM

There are two RJ45 ports available for connecting a HSM to the network. These will both be set up in a teaming (NIC Bonding) configuration for connecting the HSM to the network.

# 5 Detailed Design

This will include detail outline of WEL Network and integration with the existing infrastructure for DEV/TEST environment.

## 5.1 IP Addresses/VLAN allocation for DEV/TEST environment

The IPv4 addresses assigned to the AMI application servers in the WEL Networks on-premise environment will be allocated by WEL Networks. However, for IPv6, the same IPv6 address space used currently in the Itron SaaS deployment - including NAN / WAN prefixes and IPv6 addresses assigned to application servers – will be utilized.

| VLAN Number | Services | Subnet/IP address | Gateway IP address |
|---|---|---|---|
| Loopback50 | Anycast Gateway of Tunnel Router | 10.16.0.1/32 | NA |
| MGMT | Tunnel router MGMT IP | 10.100.0.X | |
| 300 | P2P Tunnel Transit | 10.16.0.248/29<br>fdc9:ccbe:00cc:ccdd::/64 | .249/29 on switch<br>fdc9:ccbe:00cc:ccdd:10:16:0:249/64 on switch |
| 301 | App servers. AMI servers IPv4 | 10.16.1.0/24 | 10.16.1.1 |
| | App servers. AMI servers IPv6 | fdc9:ccbe:52c0:cd00::/64 | fdc9:ccbe:52c0:cd00:10.16.1.1/64 |
| 302 | Oracle/DB | 10.16.2.0/24 | 10.16.2.1 |
| 303 | HSM | 10.16.3.0/24 | 10.16.3.1 |
| 304 | ODA | 10.16.4.0/24 | 10.16.4.1 |

Table 1: DEV/TEST VLANs Details

## 5.2 IPv4/IPv6 Address Allocation

IPv6 addresses are assigned to every device in the mesh network as well as to the AMI application servers in the back-office.

IPv6 addresses are 128-bit addresses that consist of a 64-bit network prefix. Within the AMI network, each Access Point (AP) or Micro Access Point (MicroAP) and the devices connected to it make up a neighborhood area network (NAN) that has a unique IPv6 network prefix for all devices within it that is each AP has an IPv6 address with a unique 64-bit network prefix.

IPv6 has historically been unsupported by the carriers supplying the backhaul connection, the IPv6 traffic exchanged between the back-office servers and each mesh endpoint is encapsulated in a 6-in-4 tunnel that is established between each AP and the headend tunnel router.

An AP has two IPv6 addresses – a NAN address for communications within the mesh network and a WAN address for communication over the APN backhaul.

It is highly recommended to retain the same IPv6 address space from Itron SaaS deployment, including NAN, WAN prefixes and UIQ servers' IPv6 addresses. This is to avoid mesh network disruptive and avoid new BLOBs to be re-signed and sent to every AP/Meter in the field.

| Services | IPv6 IP addresses |
|---|---|
| DNS Server IPv6<br>WELA-TST-AMS-ITRON-02 | fdc9:ccbe:52c0:cd00:10:16:1:12/64 |
| NMS Trap Host IPv6 | fdc9:ccbe:52c0:cd00: 10:16:1:12/64 |
| DLCA Server IPv6 | fdc9:ccbe:52c0:cd00: 10:16:1:12/64 |
| NTP Server IPv6 | fdc9:ccbe:52c0:cd00: 10:16:1:12/64 |
| DNS Zone | tst.ami.wel |
| NAN IPv6 Prefixes | fdcd:34f7:6a49::/48 |
| WAN IPv6 Prefixes | fdb6:76ba:b303::/48 (CHS) |
| ODA Appliance Management IPv4 | 10.220.2.X ILO |

Table 2: IPv6 Details

## 5.3 Domain Name System DNS

There are two aspects to the DNS configuration that must be considered:

- DNS Server used to resolve host names for the application servers.
- DNS Server used by AMI applications that access devices on the AMI network (Registrar).

### 5.3.1 Domain Names for App Servers

WEL Networks DNS servers implemented with Microsoft Active Directory are used as the authoritative name servers for all application servers and network infrastructure utilized in the back-office. The domain names used for each environment will be as follows.

| Environment | DNS notations |
|---|---|
| Production/DR | prd.welnet.co.nz |
| UAT/PRE_PROD | uat.welnet.co.nz |
| TEST/DEV | tst.welnet.co.nz |

Table 3: DNS Notations

## 5.4 CNAME Detail/IP details of each server

Refer to the attached sheet for DEV/TEST build IP addresses of each server and also cnames

VM_IP_Assignment_in_progress v0.1.xlsx

| VM | COMPONENT | CNAME |
|---|---|---|
| **WELA-TST-AMS-ITRON-01** | | |
| IPv4<br>TBA | CATOOLS | control.tst.welnet.co.nz |
| | NETMGR | |
| IPv6<br>TBA | HSM-COP | |
| | HSM-KEYSAFE | |
| OS<br>RHEL 8.5 | HSM-CSLAN OS | |
| | HSM-Security OS | |
| | DEPLOYMENT BUNDLE | |
| **WELA-TST-AMS-ITRON-02** | | |
| IPv4<br>TBA | AMM DB | |
| | AMMJMSROUTE | ammjmsroute.tst.welnet.co.nz |
| IPv6<br>TBA | AMMWSROUTE | ammwsroute.tst.welnet.co.nz |
| | MT | mt.tst.welnet.co.nz |
| OS<br>RHEL 8.5 | CAAS | caas.tst.welnet.co.nz |
| | CRYPTKEEPER | cryptkeeper.tst.welnet.co.nz |
| | FWU | fwu.tst.welnet.co.nz |
| | MPC | mpc.tst.welnet.co.nz |
| | FSU-SAM | sam.tst.welnet.co.nz |
| | TIBCO-CONF | |
| | TIBCO | tibco.tst.welnet.co.nz |
| | TRAPROUTER | traprouter.tst.welnet.co.nz |
| | TMB | tmb01.tst.welnet.co.nz |
| | METER PLUGINS | |
| | DLCA | dlca.tst.welnet.co.nz |
| | REGISTRAR | reg01.tst.welnet.co.nz |
| | REGISTRATIONHANDLER | reghandler.tst.welnet.co.nz |
| | ZTP | ztp.tst.welnet.co.nz |

| VM | COMPONENT | CNAME |
|---|---|---|
| | MPCWSROUTE | mpcwsroute.tst.welnet.co.nz |
| **WELA-TST-AMS-ITRON-03** | | |
| IPv4<br>TBA | GMR | gmr01.tst.welnet.co.nz |
| | METER PLUGINS | |
| IPv6<br>TBA | HIVEMQ BROKER | hivemq.tst.welnet.co.nz |
| | MQTT BROKER - HIVEMQPLUGINS | |
| OS<br>RHEL 8.5 | MQTT BROKER - HIVEMQSSNCFG | |
| | MQTT BROKER - TOPIC REMAPPER | |
| | DMS ES | |
| | DMS | dms.tst.welnet.co.nz |
| | GATEWAY | gateway.tst.welnet.co.nz |
| **WELA-TST-AMS-ITRON-04** | | |
| IPv4<br>TBA | GRIDSCAPE | gridscape.tst.welnet.co.nz |
| | CEPES | cepes.tst.welnet.co.nz |
| IPv6<br>TBA | CEPNMS | cepnms.tst.welnet.co.nz |
| | | |
| OS<br>RHEL 8.5 | | |
| | | |
| **WELA-TST-AMS-ITRON-05** | | |
| IPv4<br>TBA | DTA | dta.tst.welnet.co.nz |
| | ODS | ods.tst.welnet.co.nz |
| IPv6<br>TBA | ODSJMSROUTE | odsjmsroute.tst.welnet.co.nz |
| | ODSWSROUTE | odswsroute.tst.welnet.co.nz |
| OS<br>RHEL 8.5 | SENSORIQ | sensoriq01.tst.welnet.co.nz |
| | SENSORIQWSROUTE | sensoriqwsroute.tst.welnet.co.nz |
| | HCM | hcm.tst.welnet.co.nz |
| | HCMJMSROUTE | hcmjmsroute.tst.welnet.co.nz |
| | HCMWSROUTE | hcmwsroute.tst.welnet.co.nz |
| | NEC | nec.tst.welnet.co.nz |

Table 4: CNAME Details

## 5.5 Network Time Protocol NTP

Time synchronization is very important to correct operation of the AMI network. Beyond the obvious reasons associated with accurate billing data, security associations established between the back office and each network endpoint require accurate time – without time synchronization, secure communication from the back-office to a network device will fail.

- NTP1 welad5.welnet.co.nz – 10.220.1.12 – Maui Street
- NTP2 welad6.welnet.co.nz – 10.220.1.16 – Maui Street
- NTP3 welad4.welnet.co.nz – 10.220.1.15 – Avalon Drive

## 5.6 SSL Certificates and Management

Communication between, and with, components of the back-office applications utilize TLS/SSL. TLS/SSL requires X.509 certificates that must be signed by a trusted 3rd party Certificate Authority.

WEL Networks must obtain TLS/SSL certificates for each of the application servers that require them and manage renewals to these certificates on an ongoing basis.

Java applications authenticate the TLS/SSL certificates via a local CACERTS file which contains the trusted roots.

Note that there may be different Java versions required by different applications and all relevant cacerts files must include the root certificate for the CA that signed the TLS/SSL certificates.

TLS certificates are based on public-private key pairs and a hierarchy of trusted certificate authorities (CAs) known to all TLS/SSL client applications (including web browsers). The clients use their internal list of trusted root certificates to decide whether the TLS/SSL certificate chain presented by the server can be trusted. If the client recognizes the Root CA certificate that is presented, it then validates all the certificates in the chain, ensuring that they are signed by their parent in the chain and that they are not expired or revoked.

| **SSL Certificate Requirement** |
| --- |
| one wildcard certificate for each environment.<br>Like,<br><br>Production / DR: *.prd.welnet.co.nz<br>UAT:*.uat.welnet.co.nz<br>Test:*.tst.welnet.co.nz |

**Note**: Quote has been shared with PM/Ian for approval.

# 6 Implementation

This will include detail outline of WEL Network and integration with the existing infrastructure for DEV/TEST environment. All the implementation will be carried out after presenting the change in CAB and going through peer review process.

## 6.1 Core Switch Configurations (WEL-MAUCORE-P01)

**WEL-MAUCORE-P01**

```
!
ipv6 unicast-routing
!
interface Port-channel10
switchport trunk native vlan 999
switchport trunk allowed vlan 300,301,302,303,304
 switchport mode trunk
!
!
interface GigabitEthernet1/0/16
switchport trunk native vlan 999
switchport trunk allowed vlan 300,301,302,303,304
 switchport mode trunk
logging event trunk-status
logging event bundle-status
auto qos trust dscp
channel-protocol lacp
channel-group 10 mode active
service-policy input AutoQos-4.0-Trust-Dscp-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
!
!
interface GigabitEthernet2/0/7
!
!
interface Vlan300
 description P2P Tunnel Transit
 ip address 10.16.0.249 255.255.255.248
 ipv6 address fdc9:ccbe:00cc:ccdd:10:16:0:249/64
!

!
interface Vlan301
 description TEST/DEV App servers VLAN
 ip address 10.16.1.1 255.255.255.0
 ipv6 address fdc9:ccbe:52c0:cd00:10.16.1.1/64
!
```

```
!
interface Vlan302
 description TEST/DEV Oracle/DB servers VLAN
 ip address 10.16.2.1 255.255.255.0
!

!
interface Vlan303
 description TEST/DEV HSM VLAN
 ip address 10.16.3.1 255.255.255.0
!
!
interface Vlan304
 description TEST/DEV ODA VLAN
 ip address 10.16.4.1 255.255.255.0
!

ip route 10.16.1.0 255.255.255.0 10.220.1.170
ip route 10.16.0.1 255.255.255.255 10.220.1.170
```

## 6.2 NMSAPA01 SCADA Firewall Routing

**NMSAPA01 SCADA FW**

**Route for AMI/App servers**

set network virtual-router vr_vsys1 routing-table ip static-route "Route 46" nexthop ip-address 192.168.50.2

set network virtual-router vr_vsys1 routing-table ip static-route "Route 46" interface ethernet1/1.42

set network virtual-router vr_vsys1 routing-table ip static-route "Route 46" metric 10

set network virtual-router vr_vsys1 routing-table ip static-route "Route 46" destination 10.16.1.0/24

set network virtual-router vr_vsys1 routing-table ip static-route "Route 46" route-table unicast

**Route for Anycast loopback address of tunnel router**

set network virtual-router vr_vsys1 routing-table ip static-route "Route 47" nexthop ip-address 192.168.50.2

set network virtual-router vr_vsys1 routing-table ip static-route "Route 46" interface ethernet1/1.42

set network virtual-router vr_vsys1 routing-table ip static-route "Route 46" metric 10

set network virtual-router vr_vsys1 routing-table ip static-route "Route 46" destination 10.16.0.1/32

set network virtual-router vr_vsys1 routing-table ip static-route "Route 46" route-table unicast

## 6.3 Tunnel Router configurations

**Tunnel Router Configurations**

```
!#################################################################
!## Configuration for {{Hostname}}
!#################################################################
!
!# Step 1: Initial Configuration From Web Console.
!
hostname {{Hostname}}
vrf definition Mgmt-intf
address-family ipv4
 exit-address-family
!
interface GigabitEthernet1
vrf forwarding Mgmt-intf
ip address 10.100.0.X 255.255.255.0
no shutdown
!
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 {{MGMT Gateway}}
!
username {{Local_User1}} privilege 15 secret {{Local_User1_PW}}
enable secret {{Enabled_PW}}
aaa new-model
end
wr
!
!# Step 2: Smart License Provisioning.

license boot level network-advantage addon dna-advantage
end
wr
reload
! reboot is required before you could apply the rest of the configuration
!
!
ip name-server vrf Mgmt-intf <DNS Server>
ip domain lookup
!
platform hardware throughput level MB 200
ip http client source-interface GigabitEthernet1
service call-home
license smart transport callhome
call-home
source-interface GigabitEthernet1
vrf Mgmt-intf
```

```
end
license smart trust idtoken {{Cisco_Registration_Token}} local
wr
!
!# Step 3: Apply the basic configuration.
!
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
service sequence-numbers
no service dhcp
!
hostname {{Hostname}}
!
vrf definition Mgmt-intf
 !
address-family ipv4
 exit-address-family
!
logging userinfo
logging buffered informational
no logging console
!
username {{Local_User1}} privilege 15 secret {{Local_User1_PW}}
enable secret {{Enabled_PW}}
!
aaa new-model
!
aaa group server tacacs+ ISE_AUTH
server name {{AAA Server}}
 server name {{AAA Server}}
 ip vrf forwarding Mgmt-intf
 ip tacacs source-interface GigabitEthernet1
!
aaa authentication login default group ISE_AUTH local
aaa authentication enable default group ISE_AUTH enable
aaa authorization exec default group ISE_AUTH none
aaa authorization commands 0 default group ISE_AUTH none
aaa authorization commands 1 default group ISE_AUTH none
aaa authorization commands 15 default group ISE_AUTH none
aaa accounting send stop-record authentication failure
aaa accounting session-duration ntp-adjusted
aaa accounting update periodic 1440
aaa accounting exec default start-stop group ISE_AUTH
aaa accounting connection default start-stop group ISE_AUTH
aaa accounting system default start-stop group ISE_AUTH
```

```
aaa accounting resource default start-stop group ISE_AUTH
!
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 {{MGMT Gateway}}
ip domain lookup
ip domain lookup vrf Mgmt-intf source-interface GigabitEthernet1
ip domain name {{domain name}}
ip domain name vrf Mgmt-intf {{domain name}}
!
ipv6 unicast-routing
!
crypto isakmp policy 10
encryption 3des
authentication pre-share
group 2
!
crypto isakmp policy 20
 encryption aes
authentication pre-share
 group 2
!
crypto ipsec transform-set AES_SHA esp-aes esp-sha-hmac
mode tunnel
crypto ipsec transform-set MANUAL_TRANSFORM_SET01 esp-aes esp-sha-hmac
mode transport
!
crypto isakmp keepalive 120 10 periodic
!
interface Loopback50
description anycast_GW
 ip address 10.16.0.1 255.255.255.255
!
interface GigabitEthernet1
vrf forwarding Mgmt-intf
ip address {{Mgmt_IPv4}} 255.255.255.0
 no shutdown
!
interface GigabitEthernet2
no ip address
no shutdown
!
!
no ip http server
no ip http secure-server
ip scp server enable
!
ip tftp source-interface GigabitEthernet1
ip tacacs source-interface GigabitEthernet1
ip http client source-interface GigabitEthernet1
```

```
ip ssh source-interface GigabitEthernet1
ip ssh logging events
ip ssh version 2
!
line vty 0 15
access-class SSH_ACCESS in vrf-also
exec-timeout 15 0
privilege level 15
transport input ssh
transport output none
!
ntp logging
ntp source GigabitEthernet1
ntp server vrf Mgmt-intf {{NTP Server}} prefer
!
!## Manually Generate RSA SSH Session Key
crypto key generate rsa general-keys modulus 2048
!
end
wr
```

## 6.4 Firewall Rules

Firewall rules are attached

VM_IP_Assignment_and_FW_Rules_WIP.xlsx

| TEST Environment - Firewall Rules | | | | |
|---|---|---|---|---|
| **Corporate Firewall** | | | | |
| **IP Stack** | **Source IP** | **Destination IP** | **Protocol - Ports/Services** | **Description** |
| IPv4 | <Coporate Network> | 10.16.1.0/24 | TCP 3010 – AMM<br>TCP 6343 – CAAS<br>TCP 8243 – SAM<br>TCP 6444 – HCM<br>TCP 6943 – NEC<br>TCP 5044 – MPC<br>TCP 4043 – FWU<br>TCP 7543 – NC<br>TCP 7643 – CEPES<br>TCP 8043 – Gridscape<br>TCP 6843 – SIQ<br>TCP 3144 – ODS | For WEL Application Operators to access application UI. |
| IPv4 | <Coporate Network> | 10.16.1.0/24 | TCP 5627 – AMM JMSRoute<br>TCP 5602 – AMM WSRoute<br>TCP 9443 – CryptKeeper<br>TCP 3090 – AMM MT<br>TCP 7388 – DLCA<br>TCP 7343 – DLCA<br>TCP 7061 – DMS<br>TCP 7043 – DMS<br>TCP 7885 – Gateway<br>TCP 9091 – GMR<br>TCP 9090 – GMR<br>TCP 8188 – Registrar<br>TCP 3060 – AMM MT<br>TCP 7060 – DMS<br>TCP 7851 – Gateway<br>TCP 9060 – GMR<br>TCP 9080 – GMR<br>TCP 7080 – DMS<br>TCP 8182 – Registrar<br>TCP 5633 – MPC WSRoute<br>TCP 7590 – Network Centre<br>TCP 5630 – ODS JMSRoute<br>TCP 5626 – ODS WSRoute<br>TCP 7243 – Tibco | For WEL Application Admins to monitor and troubleshoot application running status. |
| IPv4 | <Coporate Network> | 10.16.0.1/32<br>10.16.1.0/24<br>10.16.2.0/24<br>10.16.4.0/24 | TCP 22 - SSH<br>ICMP | For WEL Application Admins to perform servers and services management tasks. |
| IPv4 | 172.20.116.0/22 | 10.16.1.12/32 | UDP 647<br>ICMP | Allow SPARK PAPN to reach Gridscape CHS via TMB. |
| IPv4 | 10.16.1.12/32 | 172.20.116.0/22 | UDP 648<br>UDP 645<br>ICMP | Allow Gridscape CHS to reach SPARK PAPN for AP configuration push. |
| IPv4 | 172.20.116.0/22 | 10.16.0.1/32 | ESP<br>UDP 500<br>UDP 4500<br>ICMP | Allow SPARK PAPN to reach Tunnel Router for IPsec tunnel establishment. |
| IPv4 | 10.16.0.1/32 | 172.20.116.0/22 | ESP<br>UDP 500<br>UDP 4500<br>ICMP | Allow Tunnel Router to reach SPARK PAPN for IPsec tunnel establishment. |
| IPv4 | <Itron Admin Subnets> | 10.16.0.1/32<br>10.16.1.0/24<br>10.16.2.0/24<br>10.16.4.0/24 | TCP 3010 – AMM<br>TCP 6343 – CAAS<br>TCP 8243 – SAM<br>TCP 6444 – HCM<br>TCP 6943 – NEC<br>TCP 5044 – MPC<br>TCP 4043 – FWU<br>TCP 7543 – NC<br>TCP 7643 – CEPES<br>TCP 8043 – Gridscape | Allow Itron project team to remotely configure and troubleshoot AMI application stacks. TBD |

# 7 Failover Test plan

Failover testing is not applicable to DEV/Test environment as Test is built for only small scale in one Data Centre.

# 8 Backout plan

In the event of an unexpected impact that cannot be resolved by troubleshooting, then document the procedure to back out the implementation to a working point. This may be going back to original state (show detailed Method of Procedure on how to get to original state). Or may be a partial change to get to a stable working state.