|  |  |
| --- | --- |
| ITRON Headend - Network Design | |
| Project/Product Name | ITRON Headend migration on prem.. |

|  |  |
| --- | --- |
| Status | Waiting Approval |
| Document Version | 0.7 |
| File name | 7 |
| Security Classification | Confidential |
| Date | 31 March 2023 |

Document Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description of Amendments |
| 0.1 | 19-03-2023 | Adeel Ahmed | Initial Draft |
| 0.2 | 21-03-2023 | Adeel Ahmed | Added UAT IP details, updated the ILO IP addresses of ODA, LO50 of Tunnel router, added IP addressing for UAT and relevant configurations |
| 0.3 | 22-03-2023 | Adeel Ahmed | Added firewall rules and IP addressing for UAT |
| 0.4 | 23-03-2023 | Adeel Ahmed | Added routing for UAT environment |
| 0.5 | 24-03-2023 | Adeel Ahmed | RACI updated, updated the firewall rules for TEST and UAT |
| 0.6 | 28-03-2023 | Adeel Ahmed | Backout plan added |
| 0.7 | 31-03-2023 | Adeel Ahmed | Firewall rules adjusted as AD user-based authentication, comments addressed after DRB |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Document Approvals

This table should be updated to reflect the Verifier, Signoff and Accountable Roles of the RACI-VS at the point of approval.

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Name | Date | Embed approval |
| Head of Stratergy & Architecture | Ian Hayton | Click or tap to enter a date. | Choose an item. |
| IT Operations Manager | Andrew Mackintosh | Click or tap to enter a date. | Choose an item. |
| IT Risk & Secuirty | Dheeraj Verma | Click or tap to enter a date. | Choose an item. |
| Delivery & Operations Manager | Darren Brown | Click or tap to enter a date. | Choose an item. |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Document Guidance 5](#_Toc131245949)

[1.1. Document Purpose 5](#_Toc131245950)

[1.2. Related Documents 5](#_Toc131245951)

[2. Document Governance 6](#_Toc131245952)

[2.1. Roles and Responsibilities 6](#_Toc131245953)

[2.2. Quality Control 6](#_Toc131245954)

[2.3. Guiding Principles 7](#_Toc131245955)

[3. Executive Overview 8](#_Toc131245956)

[3.1. Project Background 8](#_Toc131245957)

[3.2. Problem Statement 8](#_Toc131245958)

[3.3. Design Decisions 9](#_Toc131245959)

[3.4. Risks, Dependencies & Assumptions 10](#_Toc131245960)

[3.4.1. Risks 10](#_Toc131245961)

[3.4.1. Dependencies 10](#_Toc131245962)

[3.4.2. Assumptions 10](#_Toc131245963)

[3.5. Environments 11](#_Toc131245964)

[3.6. Pre-PROD Infrastructure 11](#_Toc131245965)

[3.6.1. Test Network Layout 11](#_Toc131245966)

[3.6.2. UAT Network Layout 13](#_Toc131245967)

[4. Network Architecture 14](#_Toc131245968)

[4.1. Network Diagram (Physical Layout) 14](#_Toc131245969)

[4.2. AP/Meter Traffic Flow 15](#_Toc131245970)

[4.2.1. 6-in-4 Tunnel 15](#_Toc131245971)

[4.3. ITRON Admin Link via existing IPSec tunnel 17](#_Toc131245972)

[4.3.1. Admin Link during Project Implementation for TES 19](#_Toc131245973)

[4.4. Oracle Database Appliance ODA 19](#_Toc131245974)

[4.4.1. Specification of ODA in Test Environment 19](#_Toc131245975)

[4.4.2. ODA Network Ports and Description 20](#_Toc131245976)

[4.5. HSM (Key safe) 20](#_Toc131245977)

[4.5.1. Network Ports of HSM 21](#_Toc131245978)

[5. IP Addressing and VLAN Database 21](#_Toc131245979)

[5.1. IP Addressing VLAN Test Environment 21](#_Toc131245980)

[5.2. IP Addressing VLAN UAT Environment 23](#_Toc131245981)

[5.3. IPv4/IPv6 Address Allocation 23](#_Toc131245982)

[5.4. Domain Name System DNS 25](#_Toc131245983)

[5.4.1. Domain Names for App Servers 25](#_Toc131245984)

[5.5. CNAMES Details of TEST environment 25](#_Toc131245985)

[5.6. CNAMES Details of UAT environment 27](#_Toc131245986)

[5.7. Network Time Protocol NTP 29](#_Toc131245987)

[5.8. SSL Certificates and Management 29](#_Toc131245988)

[6. Implementation and Configurations 31](#_Toc131245989)

[6.1. Core Switch Configurations 31](#_Toc131245990)

[6.2. NMSAPA01 SCADA Firewall Routing 34](#_Toc131245991)

[6.3. WELAPA01 35](#_Toc131245992)

[WELAPA01 35](#_Toc131245993)

[6.4. WEL-SSNFW-PO1 36](#_Toc131245994)

[WEL-SSNFW-PO1 36](#_Toc131245995)

[6.5. PAPN router managed by Spark 36](#_Toc131245996)

[PAPN Spark router 36](#_Toc131245997)

[6.6. Tunnel Router configurations WEL-TLMAUTUN-R01 36](#_Toc131245998)

[Tunnel Router Configurations WEL-TLMAUTUN-R01 36](#_Toc131245999)

[6.7. Mau.50 Router configuration 41](#_Toc131246000)

[Mau.50 router configurations 41](#_Toc131246001)

[6.8. Firewall Rules 41](#_Toc131246002)

[7. Backout Plan 42](#_Toc131246003)

[7.1. Core switch back out 42](#_Toc131246004)

[7.2. NMSAPA01 SCADA Firewall backout 43](#_Toc131246005)

[7.3. WELAPA01 Backout 44](#_Toc131246006)

[WELAPA01 44](#_Toc131246007)

[7.4. WEL-SSNFW-PO1 Backout 44](#_Toc131246008)

[WEL-SSNFW-PO1 44](#_Toc131246009)

[7.5. Mau.50 Router Backout 45](#_Toc131246010)

[7.6. Tunnel Router Backout 45](#_Toc131246011)

[8. RACI 46](#_Toc131246012)

[9. Solution Compliance 48](#_Toc131246013)

[9.1. WEL Technology Strategy and Roadmap 48](#_Toc131246014)

[9.2. Compliance Business Requirements 48](#_Toc131246015)

[Appendix A – Other Related Document Locations 50](#_Toc131246016)

# Document Guidance

## Document Purpose

The purpose of this document is to:

* Describe a network design that supports the defined solution requirements.
* Identify and highlight dependencies and any residual risks and issues.
* Provide input to Programme/Project Planning
* Enable effective stakeholder communication and decision making.

## Related Documents

This solution design should be read in conjunction with the following referenced documents:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | Title and Hyperlink | Author | Version | Date |
| 1 | ITRON Environment Design  [Network Design TEST-UAT](https://welnetworks.sharepoint.com/:f:/r/sites/HeadendMigration/Shared%20Documents/General/Network%20Design%20TEST-UAT?csf=1&web=1&e=K5D4SH) | ITRON | v1.0 | 15-Mar-23 |
| 2 | ITRON Workshop PPT  [WEL Networks Licensed Transition Network Workshop.pptx](https://welnetworks.sharepoint.com/:p:/r/sites/HeadendMigration/Shared%20Documents/General/Network%20Design%20TEST-UAT/WEL%20Networks%20Licensed%20Transition%20Network%20Workshop.pptx?d=wb7a62b4b8439491bb4b3aaacf354905c&csf=1&web=1&e=gisRQr) | ITRON | v0.1 | 15-Mar-23 |
| 3 | Oracle ODA online information  <https://docs.oracle.com/en/engineered-systems/oracle-database-appliance/19.18/cmtxp/readying-oda.html#GUID-30812995-49C0-4FDB-9B87-2B9E313C2102> | Oracle |  | 15-Mar-23 |
| 4 | ODA Datasheet  Attached PDF document in Appendix A | Oracle |  | 15-Mar-23 |
| 5 | Key safe HSM  <https://www.licenciasonline.com/mx/es/productos/utimaco/lan-appliance> | ITRON |  | 15-Mar-23 |
|  |  |  |  | Click or tap to enter a date. |
|  |  |  |  | Click or tap to enter a date. |

# Document Governance

## Roles and Responsibilities

The RACI-VS for this document is as outlined in the following table, where:

* ***R = Responsible:*** The role tasked with the job of preparing the document. Typically, one role, though may be more in some circumstances.
* ***A = Accountable:*** The role that is ultimately answerable for the correct and thorough completion of the deliverable or task and has the overall approving authority. There can only be *one* named Accountable role.
* ***C = Consult:*** The role(s) that must be consulted for their opinions (often subject matter experts) before the document is finalised and verified, prior to signoff.
* ***I = Inform:*** The role(s) that need to be informed of document development progress, and once completed, advised of document approval (i.e. sent a copy to action further).
* ***V = Verify:*** The role(s) that will be required to review this document to ensure it is up to a standard of quality prior to signoff
* ***S = Signoff:*** The role(s) that will be expected to provide signoff on this document. Will include the Accountable role.

| Artefact | Accountable | Responsible | Consult | Verify | Signoff | Inform |
| --- | --- | --- | --- | --- | --- | --- |
| Network & Security Design | Project Sponsor | IT Operations Manager | IT Risk & Secuirty | IT Operations Manager | Delivery & Operations Manager |  |

## Quality Control

This document will be subjected to the following quality review processes:

* Verification via appropriate peer reviews
* Acceptance via embedding of electronic signoffs as listed above.

## 

## Guiding Principles

|  |  |
| --- | --- |
| Ref No. | Architecture Principle |
| AP1 | Process and systems are fit for purpose for WEL business and operating model. |
| AP2 | Reuse existing capability investments first, where it fits with business needs. |
| AP3 | Pre-integrated solutions are preferred to multi-vendor component solutions. |
| AP4 | Buy solutions that are business configurable rather than “toolkits” that require vendor projects for change. |
| AP5 | Invest in automation and integration where business benefits are justified (high volume – low complexity). |
| AP6 | Technology interoperability and compliance with key industry standards is essential. |
| AP7 | Capability investments are prioritised based on contribution to business and customer benefits. |
| AP8 | Technology selection considers full lifecycle costs including deployment, operations and support. |
| AP9 | Plan for and allow our systems to mature as business matures Capability and system design. |
| AP10 | Optimise and invest in core processes, design for “good enough” non-core processes. |
| AP11 | Maximise leverage out-of-the-box solution templates and processes. |
| AP12 | Build and deploy reusable Product, Service and Resource components with minimum development. |
| AP13 | Data is an enterprise asset that is managed using defined ILM processes and standards. |
| AP14 | Capability should be designed in a product agnostic manner. |
| AP15 | Allow for differentiated service levels and right-fit to business needs. |
| AP16 | Architect and design for an efficient supply chain. |
| AP17 | Customer and supplier inter-operability services should be flexible enough to accommodate change. |
| AP18 | Provide equivalence and non-discrimination across all customers. |
| AP19 | Products and services are designed for committed Service Level Agreements. |

# Executive Overview

WEL Networks is an electricity distributor in New Zealand covering the city of HAMILTON. WEL Networks have a current customer base of 70,000 meters and they are planning to increase this base to 100,000 electric meters. For this to happen WEL networks is planning to bring the SAAS based solution in house.

The migration of the work will happen in staged approach, TEST and UAT will be done first as part of this design while PROD and DR will happen separately and design for PROD and DR will be written later.

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 favour 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 only for pre-prod (TEST and UAT) network.

## Project Background

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 favour of an on premise (Licensed Customer) Solution.

The document aim is to layout the existing network component and connectivity required for new headend solution.

The migration from Itron Managed Service to an on premise will require (Test, UAT) to be commissioned in parallel with the existing ITRON Managed Service environments.

The purpose of this document is to describe the components used to implement the Itron AMI and associated components required for an End-to-End solution, as well as to provide an overview of how they work. The document will serve as a reference to guide informed decisions about how best to support the system, assess the impact of any changes and scale the system to address future business objectives.

## Problem Statement

Setup the WEL Networks in house ITRON Headend and the methodology for the migration from ITRON Managed Service to an on premise requires four new environments (Test, UAT) to be commissioned in parallel with the existing ITRON Managed Service environments. The existing SAAS environment of TEST and will be migrated to on premise TEST, UAT and environments respectively. This document details the network and security solution and supporting infrastructure requirements and configurations.

Existing WEL Networks infrastructure and capabilities (such as networking and security infrastructure) will be leveraged to reduce cost where the operating risk is manageable.

## Design Decisions

The following design decisions relating to the network design (verified with WEL Security)

|  |  |  |  |
| --- | --- | --- | --- |
| **Subject Area** | SVI on the firewall of App/Oracle/DB/HSM servers | **Topic** | Layer-3 |
| **Architectural Decision** | TEST 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 rather than on the cooperate firewalls | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **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 in TEST network while similar of servers are required for UAT network, hence the total bandwidth required will not be more than 1G. therefore current infrastructure will cater for the required bandwidth | **ID** | 02 |
| **Summary** | Existing link between core switches and CORP firewall will not congest | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Subject Area** | HSM must reside within an isolated VLAN protected by a firewall and be physically separated from the AMI application servers | **Topic** | Isolated VLAN |
| **Architectural Decision** | TEST/UAT networks will use current infrastructure based on the existing design already in place. | **ID** | 03 |
| **Summary** | PROD and DR design will cover all aspects of network and security best practices when designed. | | |

## Risks, Dependencies & Assumptions

### Risks

|  |  |  |  |
| --- | --- | --- | --- |
| No | Description | Impact: High/Medium/Low | Owner/Assigned to |
| 1 | Data Centre power and cooling – The current datacentre infrastructure across Maui Street have enough capacity for both the cooling and power requirements for pre-prod infrastructure for Itron.  This is estimated to be less than 2 kW and facilities has confirmed that is available. In the event of power contention, pre-prod can be shut down cleanly | Low | Facilities |

### Dependencies

|  |  |
| --- | --- |
| No | Description |
| 1 | Availability of resource to deliver the project in time. |
| 2 |  |
|  |  |

### Assumptions

|  |  |  |
| --- | --- | --- |
| No | Description | Mitigation Plan |
| 1 | Aruba switches will not be connected to the existing core switches while ODA appliance will be directly patched to core switches on 1/10G interfaces |  |
| 2 | ODA appliance, tunnel router and core switches are close to each other and required only short cables for connectivity, cables are available on site |  |
| 3 | 10G SFP are available for the connectivity to establish between core switches and ODA |  |

## Environments

WEL network will have different environments to deliver the smart meter services. But we are currently working on TEST and UAT deployment using the current infrastructure.

* UAT and Test: Maui Street Data Centre

## Pre-PROD Infrastructure

Pre-prod (TEST and UAT) infrastructure will have one ODA appliance where all the applications will be built, database of the test environment will also reside

inside ODA in the separate broadcast domain.

One tunnel router (Cisco 8300) will be used for TEST and UAT where all the 6-in-4 tunnels will be terminated initiated from APs. Cisco Catalyst 8000 (a replacement for Cisco ISR), otherwise referred to as a rfc2893 tunnel router within this document, is used to establish an IPsec 6in4 tunnel with every AP and Micro AP on the field network.

Key safe HSM will be connected to the core switch which will have hardware and software solution that protects cryptographic material such as private keys and

certificates. KeySafe consists of a firmware module that resides on a hardware security module (HSM) as well as a collection of command line interface (CLI)

tools for managing certificate material in the HSM. The protected memory of the HSM stores the private keys that are required by various applications to securely

communicate with devices on the network.

### Test Network Layout

The Test network will be required to perform small scale performance acceptance testing. The diagram shows the logical view of connectivity from APs to tunnel router. Same tunnel router, ODA and HSM will be used for both TEST and UAT environments.



Figure : TEST Logical Network Layout

### UAT Network Layout

User Acceptance Test, UAT 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.



Figure : UAT Logical Network Layout

# Network Architecture

## Network Diagram (Physical Layout)



Figure 3: Network Topology

Physical layout will have fibre connections from ODA appliances to the core switches and separate dedicated 1G interfaces for HSM and for tunnel router.

## AP/Meter Traffic Flow

### 6-in-4 Tunnel

6to4 tunnel will allow [IPv6 packets](https://en.wikipedia.org/wiki/IPv6_packet) to be transmitted over an IPv4 network. 6to4 performs three functions.

* Assigns a block of IPv6 address space to any host or network that has a global IPv4 address.
* Encapsulates IPv6 packets inside IPv4 packets for transmission over an IPv4 network using [6in4](https://en.wikipedia.org/wiki/6in4).
* Routes traffic between 6to4 and "native" IPv6 networks.

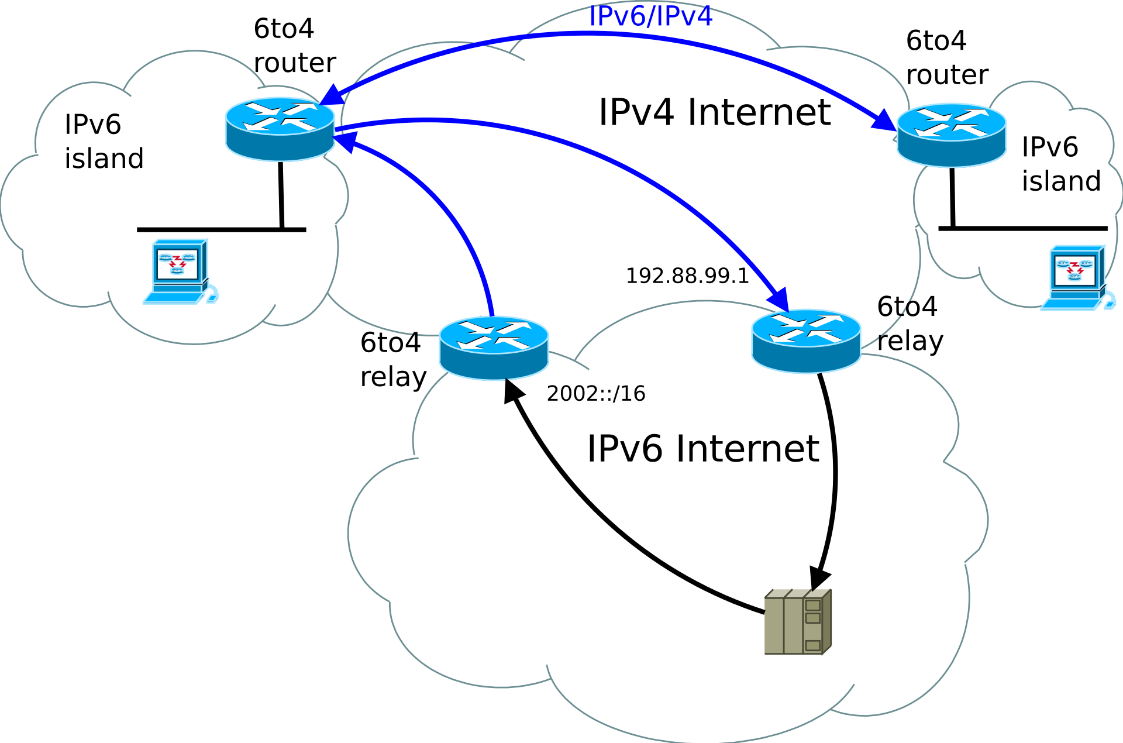


Figure : 6-in-4 Tunnel



Figure : 6-in-4 Tunnel Router Logical

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 only IPv6 addresses, and AP will have both IPv4 and IPv6 addresses.

Timeline

Description automatically generated

Figure 6: AP/Meter Traffic Flow Diagram

## ITRON Admin Link via existing IPSec tunnel

There is a single IPsec VPN connection between WEL Network’s data centre and Itron’s LAS datacentre for carrying fronthaul and backhaul traffic. Currently there is IPSec tunnel which would be modified to cater the pre-production subnets/jumphost to access AMI servers/Database servers/HSM etc.

The ITRON admin link will be re-configured 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.



Figure : Admin Link via IPSec Tunnel for Maintenance

### Admin Link during Project Implementation for TES

* FH: Allow WEL to access UIQ in Itron Datacentre
* BH: Route WEL APN network into Itron Datacentre
* Replication: Allow data replication from SaaS to Licensed servers.
* Admin: Allow Itron project team remotely connect to Licensed networks for implementation.

## 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.

### Specification of ODA in Test Environment

UAT and TEST 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.

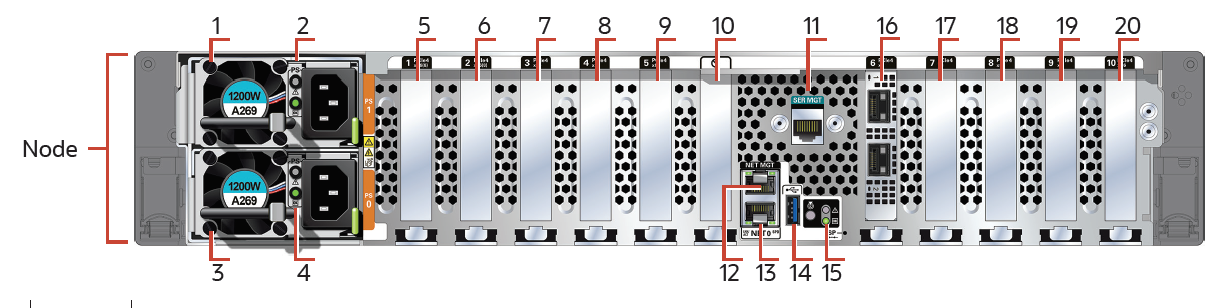


Figure 8: ODA X9-2L

### 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 = 10.221.1.190 (ILO) VLAN 221 GW= 10.221.1.1

|  |  |  |
| --- | --- | --- |
| Switch Name | Port for connectivity for ILO |  |
| WELSRVMISC-SW | Gi1/0/30 | Access port configuration with VLAN 211 |

ODA Management IPv4 = 10.100.0.65 (MGMT) VLAN 221 VLAN 100 GW= 10.100.0.1 and connect to core switch 2 “WEL-MAUCORE-P01”

## HSM (Key safe)

Key safe 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.

A picture containing diagram

Description automatically generated

Figure 9: key safe HSM

### 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.

# IP Addressing and VLAN Database

## IP Addressing VLAN Test Environment

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN Number | Services | Subnet/IP address | Gateway IP address |
| Loopback50 | Anycast Gateway of Tunnel Router | 10.16.0.1/32 | NA |
| WEL-TLMAUTUN-R01 | Tunnel router MGMT IP | 10.100.0.100 | 10.100.0.1 - VLAN 100 Connected to Core switch both for MGMT and Data |
| 300 | P2P Tunnel Transit | 10.16.0.248/29  fdc9:ccbe:00cc:ccdd::/64 | .249/29 on switch  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 |

## IP Addressing VLAN UAT Environment

Loopback50 IP address of Tunnel router will be same as that of Test environment.

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN Number | Services | Subnet/IP address | Gateway IP address |
| Loopback50 | Anycast Gateway of Tunnel Router | 10.16.0.1/32 | Same as that of TEST environment |
| WEL-TLMAUTUN-R01 | Tunnel router MGMT IP | 10.100.0.100 | 10.100.0.1 - VLAN 100  Same as that of TEST environment |
| 310 | P2P Tunnel Transit | Just reserved if required | Same as that of TEST environment |
| 311 | App servers. AMI servers IPv4 | 10.16.9.0/24 | 10.16.9.1 |
|  | App servers. AMI servers IPv6 | fdc9:ccbe:52c0:cd00::/64 | fdc9:ccbe:52c0:cd00:10.16.9.1/64 |
| 312 | Oracle/DB | 10.16.10.0/24 | 10.16.10.1 |
| ~~313~~ | ~~HSM~~ | ~~10.16.11.0/24~~ | ~~10.16.11.1~~ |
| ~~314~~ | ~~ODA~~ | ~~10.16.12.0/24~~ | ~~10.16.12.1~~ |

**Note**: VLAN 313 and VLAN 314 will not be required as UAT HSM and ODA will be same as that of TEST environment.

## 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 neighbourhood 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 (Neighbourhood Area Network) 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  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 | 10.221.1.65 ILO GW = 10.221.1.1/24 |

## 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).

### 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.

* ip name-server 10.220.1.12
* ip name-server 10.220.1.15

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

## CNAMES Details of TEST environment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VM** | **COMPONENT** | **CNAME** | **IPv4 Address** | **IPv6 Address** |
| **WELA-TST-AMS-ITRON-01** |  |  | 10.16.1.11 | fdc9:ccbe:52c0:cd00:10.:16:1:11 |
|  | CATOOLS | control.tst.welnet.co.nz |  |  |
|  | NETMGR |  |  |  |
|  | HSM-COP |  |  |  |
|  | HSM-KEYSAFE |  |  |  |
|  | HSM-CSLAN OS |  |  |  |
|  | HSM-Security OS |  |  |  |
|  | DEPLOYMENT BUNDLE |  |  |  |
| **WELA-TST-AMS-ITRON-02** |  |  | 10.16.1.12 | fdc9:ccbe:52c0:cd00:10.:16:1:12 |
|  | AMM DB |  |  |  |
|  | AMMJMSROUTE | ammjmsroute.tst.welnet.co.nz |  |  |
|  | AMMWSROUTE | ammwsroute.tst.welnet.co.nz |  |  |
|  | MT | mt.tst.welnet.co.nz |  |  |
|  | 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 |  |  |
|  | MPCWSROUTE | mpcwsroute.tst.welnet.co.nz |  |  |
| **WELA-TST-AMS-ITRON-03** |  |  | 10.16.1.13 | fdc9:ccbe:52c0:cd00:10.:16:1:13 |
|  | GMR | gmr01.tst.welnet.co.nz |  |  |
|  | METER PLUGINS |  |  |  |
|  | HIVEMQ BROKER | hivemq.tst.welnet.co.nz |  |  |
|  | MQTT BROKER - HIVEMQPLUGINS |  |  |  |
|  | 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** |  |  | 10.16.1.14 | fdc9:ccbe:52c0:cd00:10.:16:1:14 |
|  | GRIDSCAPE | gridscape.tst.welnet.co.nz |  |  |
|  | CEPES | cepes.tst.welnet.co.nz |  |  |
|  | CEPNMS | cepnms.tst.welnet.co.nz |  |  |
| **WELA-TST-AMS-ITRON-05** |  |  | 10.16.1.15 | fdc9:ccbe:52c0:cd00:10.:16:1:15 |
|  | DTA | dta.tst.welnet.co.nz |  |  |
|  | ODS | ods.tst.welnet.co.nz |  |  |
|  | ODSJMSROUTE | odsjmsroute.tst.welnet.co.nz |  |  |
|  | ODSWSROUTE | odswsroute.tst.welnet.co.nz |  |  |
|  | 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 |  |  |

## CNAMES Details of UAT environment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **UAT Environment** |  |  |  |  |
| **VM** | **COMPONENT** | **CNAME** | **IPv4 Address** | **IPv6 Address** |
| **WELA-UAT-AMS-ITRON-01** |  |  | 10.16.9.11 | fdc9:ccbe:52c0:cd20:10:16:9:11 |
|  | CATOOLS | control.uat.welnet.co.nz |  |  |
|  | NETMGR |  |  |  |
|  | HSM-COP |  |  |  |
|  | HSM-KEYSAFE |  |  |  |
|  | HSM-CSLAN OS |  |  |  |
|  | HSM-Security OS |  |  |  |
|  | DEPLOYMENT BUNDLE |  |  |  |
| **WELA-UAT-AMS-ITRON-02** |  |  | 10.16.9.12 | fdc9:ccbe:52c0:cd20: 10:16:9:12 |
|  | AMM DB |  |  |  |
|  | AMMJMSROUTE | ammjmsroute.uat.welnet.co.nz |  |  |
|  | AMMWSROUTE | ammwsroute.uat.welnet.co.nz |  |  |
|  | MT | mt.uat.welnet.co.nz |  |  |
|  | CAAS | caas.uat.welnet.co.nz |  |  |
|  | CRYPTKEEPER | cryptkeeper.uat.welnet.co.nz |  |  |
|  | FWU | fwu.uat.welnet.co.nz |  |  |
|  | MPC | mpc.uat.welnet.co.nz |  |  |
|  | FSU-SAM | sam.uat.welnet.co.nz |  |  |
|  | TIBCO-CONF |  |  |  |
|  | TIBCO | tibco.uat.welnet.co.nz |  |  |
|  | TRAPROUTER | traprouter.uat.welnet.co.nz |  |  |
|  | TMB | tmb01.uat.welnet.co.nz |  |  |
|  | METER PLUGINS |  |  |  |
|  | DLCA | dlca.uat.welnet.co.nz |  |  |
|  | REGISTRAR | reg01.uat.welnet.co.nz |  |  |
|  | REGISTRATIONHANDLER | reghandler.uat.welnet.co.nz |  |  |
|  | ZTP | ztp.uat.welnet.co.nz |  |  |
|  | MPCWSROUTE | mpcwsroute.uat.welnet.co.nz |  |  |
| **WELA-UAT-AMS-ITRON-03** |  |  | 10.16.9.13 | fdc9:ccbe:52c0:cd20:10:16:9:13 |
|  | GMR | gmr01.uat.welnet.co.nz |  |  |
|  | METER PLUGINS |  |  |  |
|  | HIVEMQ BROKER | hivemq.uat.welnet.co.nz |  |  |
|  | MQTT BROKER - HIVEMQPLUGINS |  |  |  |
|  | MQTT BROKER - HIVEMQSSNCFG |  |  |  |
|  | MQTT BROKER - TOPIC REMAPPER |  |  |  |
|  | DMS ES |  |  |  |
|  | DMS | dms.uat.welnet.co.nz |  |  |
|  | GATEWAY | gateway.uat.welnet.co.nz |  |  |
| **WELA-UAT-AMS-ITRON-04** |  |  | 10.16.9.14 | fdc9:ccbe:52c0:cd20:10:16:9:14 |
|  | GRIDSCAPE | gridscape.uat.welnet.co.nz |  |  |
|  | CEPES | cepes.uat.welnet.co.nz |  |  |
|  | CEPNMS | cepnms.uat.welnet.co.nz |  |  |
| **WELA-UAT-AMS-ITRON-05** |  |  | 10.16.9.15 | fdc9:ccbe:52c0:cd20:10:16:9:15 |
|  | DTA | dta.uat.welnet.co.nz |  |  |
|  | ODS | ods.uat.welnet.co.nz |  |  |
|  | ODSJMSROUTE | odsjmsroute.uat.welnet.co.nz |  |  |
|  | ODSWSROUTE | odswsroute.uat.welnet.co.nz |  |  |
|  | SENSORIQ | sensoriq01.uat.welnet.co.nz |  |  |
|  | SENSORIQWSROUTE | sensoriqwsroute.uat.welnet.co.nz |  |  |
|  | HCM | hcm.uat.welnet.co.nz |  |  |
|  | HCMJMSROUTE | hcmjmsroute.uat.welnet.co.nz |  |  |
|  | HCMWSROUTE | hcmwsroute.uat.welnet.co.nz |  |  |
|  | NEC | nec.uat.welnet.co.nz |  |  |

## 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. There are three NTP in the existing infrastructure.

* 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

## 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 ca certs 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.  Like,  Production / DR: \*.prd.welnet.co.nz  UAT:\*.uat.welnet.co.nz  Test:\*.tst.welnet.co.nz |

# Implementation and Configurations

## Core Switch Configurations

|  |
| --- |
| **WEL-MAUCORE-P01** |
| !  ipv6 unicast-routing  !  interface Port-channel10  description ODA-appliance  switchport trunk native vlan 999  switchport trunk allowed vlan 301,302,303,304,311,312,313,314  switchport mode trunk  !  !  interface TenGigabitEthernet2/1/4  description ODA-appliance  switchport trunk native vlan 999  switchport trunk allowed vlan 300,301,302,303,304,311, 312,313,314  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 Port-channel11  description WEL-TLMAUTUN-R01  switchport trunk native vlan 999  switchport trunk allowed vlan 300  switchport mode trunk  !  !  interface Gi1/0/16  description WEL-TLMAUTUN-R01  switchport mode trunk  switchport trunk allowed vlan 300  channel-protocol lacp  channel-group 11 mode active  !  interface Gi2/0/19  description WEL-TLMAUTUN-R01  switchport mode trunk  switchport trunk allowed vlan 300  channel-protocol lacp  channel-group 11 mode active  !  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 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 Oracle/DB servers VLAN  ip address 10.16.2.1 255.255.255.0  !  !  interface Vlan303  description TEST HSM VLAN  ip address 10.16.3.1 255.255.255.0  !  !  interface Vlan304  description TEST ODA VLAN  ip address 10.16.4.1 255.255.255.0  !  !  interface Vlan311  description UAT App servers VLAN  ip address 10.16.9.1 255.255.255.0  ipv6 address fdc9:ccbe:52c0:cd00:10.16.9.1/64  !  !  interface Vlan312  description UAT Oracle/DB servers VLAN  ip address 10.16.10.1 255.255.255.0  !  # Note: HSM/ODA for UAT will be same as that of Test therefore VLAN 313 and VLAN 314 will not be # required at this stage  ip route 10.16.0.1 255.255.255.255 10.16.0.250 name Loopback-TEST-Tunnel-RT  ipv6 route fdcd:34f7:6a49::/48 fdc9:ccbe:00cc:ccdd:10:16:0:250 name TEST- NAN-Prefix  ipv6 route fdb6:76ba:b303::/48 fdc9:ccbe:00cc:ccdd:10:16:0:250 name TEST- WAN-Prefix  ipv6 route fdc9:cbee:f77b::/48 fdc9:ccbe:00cc:ccdd:10:16:0:250 name UAT- NAN-Prefix  ipv6 route fdcd:34f7:6a69::/48 fdc9:ccbe:00cc:ccdd:10:16:0:250 name UAT- NAN-Prefix  ipv6 route fdc9:ccbe:2313::/48 fdc9:ccbe:00cc:ccdd:10:16:0:250 name UAT- WAN-Prefix  ipv6 route fdb6:76ba:b323::/48 fdc9:ccbe:00cc:ccdd:10:16:0:250 name UAT- WAN-Prefix |
|  |

## NMSAPA01 SCADA Firewall Routing

|  |
| --- |
| **NMSAPA01 SCADA FW** |
| **Route for AMI/App servers for TEST environment**  set network virtual-router vr\_vsys1 routing-table ip static-route "Route 46" nexthop ip-address 10.220.0.1  set network virtual-router vr\_vsys1 routing-table ip static-route "Route 46" interface ethernet1/2  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 10.220.0.1  set network virtual-router vr\_vsys1 routing-table ip static-route "Route 47" interface ethernet1/2  set network virtual-router vr\_vsys1 routing-table ip static-route "Route 47" metric 10  set network virtual-router vr\_vsys1 routing-table ip static-route "Route 47" destination 10.16.0.1/32  set network virtual-router vr\_vsys1 routing-table ip static-route "Route 47" route-table unicast  **Route for AMI/App servers for UAT environment**  set network virtual-router vr\_vsys1 routing-table ip static-route "Route 48" nexthop ip-address 10.220.0.1  set network virtual-router vr\_vsys1 routing-table ip static-route "Route 48" interface ethernet1/2  set network virtual-router vr\_vsys1 routing-table ip static-route "Route 48" metric 10  set network virtual-router vr\_vsys1 routing-table ip static-route "Route 48" destination 10.16.9.0/24  set network virtual-router vr\_vsys1 routing-table ip static-route "Route 48" route-table unicast |

## WELAPA01

|  |
| --- |
| WELAPA01 |
| set network virtual-router WEL-PA-VR-01 routing-table ip static-route ITRON-Connectivity-AMI nexthop ip-address 10.217.1.1  set network virtual-router WEL-PA-VR-01 routing-table ip static-route ITRON-Connectivity-AMI bfd profile None  set network virtual-router WEL-PA-VR-01 routing-table ip static-route ITRON-Connectivity-AMI interface ethernet1/5  set network virtual-router WEL-PA-VR-01 routing-table ip static-route ITRON-Connectivity-AMI metric 10  set network virtual-router WEL-PA-VR-01 routing-table ip static-route ITRON-Connectivity-AMI destination 10.16.0.0/16  set network virtual-router WEL-PA-VR-01 routing-table ip static-route ITRON-Connectivity-AMI route-table unicast |

## WEL-SSNFW-PO1

|  |
| --- |
| WEL-SSNFW-PO1 |
| route TRUSTED-WEL 10.16.0.0 255.255.0.0 10.218.13.1 1 |

## PAPN router managed by Spark

|  |
| --- |
| PAPN Spark router |
| Note: Static route will be required from PAPN router towards the corp firewall interface for 10.16.1.0/24, 10.16.9.0/24, 10.16.0.1/32  As default route therefore no configuration changes are required |

## Tunnel Router configurations WEL-TLMAUTUN-R01

|  |
| --- |
| Tunnel Router Configurations WEL-TLMAUTUN-R01 |
| !#######################################################  !## Configuration for WEL-TLMAUTUN-R01  !#######################################################  !  !# Step 1: Initial Configuration From Web Console.  !  hostname WEL-TLMAUTUN-R01  vrf definition Mgmt-intf  address-family ipv4  exit-address-family  !  interface GigabitEthernet1  vrf forwarding Mgmt-intf  ip address 10.100.0.65 255.255.255.0  no shutdown  !  ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.100.0.1  !  username cisco privilege 15 secret XXXXX  enable secret XXXX  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 10.220.1.12  ip name-server vrf Mgmt-intf 10.220.1.15  no ip domain lookup  ip domain-name welnet.co.nz  !  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 WEL-TLMAUTUN-R01  !  vrf definition Mgmt-intf  !  address-family ipv4  exit-address-family  !  logging userinfo  logging buffered informational  no logging console  !  username cisco privilege 15 secret XXXX  enable secret XXXX  !  aaa new-model  !  !  ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.100.0.1  no ip domain lookup  ip domain lookup vrf Mgmt-intf source-interface GigabitEthernet1  ip domain name welnet.co.nz  ip domain name vrf Mgmt-intf welnet.co.nz  !  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 10.100.0.65 255.255.255.0  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 prefer 10.220.1.12  ntp server vrf Mgmt-intf prefer 10.220.1.15  ntp server vrf Mgmt-intf prefer 10.220.1.16  !  !## Manually Generate RSA SSH Session Key  crypto key generate rsa general-keys modulus 2048  !  end  wr  Specific APs configurations will be generated by GridScape, those configurations will be added as part of implementation |

## Mau.50 Router configuration

|  |
| --- |
| Mau.50 router configurations |
| ip route 10.16.1.0 255.255.255.0 192.168.50.1 name-TEST-AMI-Servers  ip route 10.16.9.0 255.255.255.0 192.168.50.1 name-UAT-AMI-Servers  ip route 10.16.0.1 255.255.255.255 192.168.50.1 name-TES-Tunnel-RT |

## Firewall Rules





# Backout Plan

Implementation will be done in steps along with verification of the services in each step. Kevin Wong will help in implementation of changes.

## Core switch back out

|  |
| --- |
| **WEL-MAUCORE-P01** |
| !  no ipv6 unicast-routing  !  no vlan 300  no vlan 301  no vlan 302  no vlan 303  no vlan 304  no vlan 311  no vlan 312  no ip route 10.16.0.1 255.255.255.255 10.16.0.250 name Loopback-TEST-Tunnel-RT  no ipv6 route fdcd:34f7:6a49::/48 fdc9:ccbe:00cc:ccdd:10:16:0:250 name TEST- NAN-Prefix  no ipv6 route fdb6:76ba:b303::/48 fdc9:ccbe:00cc:ccdd:10:16:0:250 name TEST- WAN-Prefix  no ipv6 route fdc9:cbee:f77b::/48 fdc9:ccbe:00cc:ccdd:10:16:0:250 name UAT- NAN-Prefix  no ipv6 route fdcd:34f7:6a69::/48 fdc9:ccbe:00cc:ccdd:10:16:0:250 name UAT- NAN-Prefix  no ipv6 route fdc9:ccbe:2313::/48 fdc9:ccbe:00cc:ccdd:10:16:0:250 name UAT- WAN-Prefix  no ipv6 route fdb6:76ba:b323::/48 fdc9:ccbe:00cc:ccdd:10:16:0:250 name UAT- WAN-Prefix  !  interface Port-channel10  shutdown  -Prefix |

## NMSAPA01 SCADA Firewall backout

|  |
| --- |
| **NMSAPA01 SCADA FW** |
| **Route for AMI/App servers for TEST environment**  delete network virtual-router vr\_vsys1 routing-table ip static-route "Route 46" nexthop ip-address 10.220.0.1  delete network virtual-router vr\_vsys1 routing-table ip static-route "Route 46" interface ethernet1/2  delete network virtual-router vr\_vsys1 routing-table ip static-route "Route 46" metric 10  delete network virtual-router vr\_vsys1 routing-table ip static-route "Route 46" destination 10.16.1.0/24  delete network virtual-router vr\_vsys1 routing-table ip static-route "Route 46" route-table unicast  **Route for Anycast loopback address of tunnel router**  delete network virtual-router vr\_vsys1 routing-table ip static-route "Route 47" nexthop ip-address 10.220.0.1  delete network virtual-router vr\_vsys1 routing-table ip static-route "Route 47" interface ethernet1/2  delete network virtual-router vr\_vsys1 routing-table ip static-route "Route 47" metric 10  delete network virtual-router vr\_vsys1 routing-table ip static-route "Route 47" destination 10.16.0.1/32  delete network virtual-router vr\_vsys1 routing-table ip static-route "Route 47" route-table unicast  **Route for AMI/App servers for UAT environment**  delete network virtual-router vr\_vsys1 routing-table ip static-route "Route 48" nexthop ip-address 10.220.0.1  delete network virtual-router vr\_vsys1 routing-table ip static-route "Route 48" interface ethernet1/2  delete network virtual-router vr\_vsys1 routing-table ip static-route "Route 48" metric 10  delete network virtual-router vr\_vsys1 routing-table ip static-route "Route 48" destination 10.16.9.0/24  delete network virtual-router vr\_vsys1 routing-table ip static-route "Route 48" route-table unicast |

## WELAPA01 Backout

|  |
| --- |
| WELAPA01 |
| delete network virtual-router WEL-PA-VR-01 routing-table ip static-route ITRON-Connectivity-AMI nexthop ip-address 10.217.1.1  delete network virtual-router WEL-PA-VR-01 routing-table ip static-route ITRON-Connectivity-AMI bfd profile None  delete network virtual-router WEL-PA-VR-01 routing-table ip static-route ITRON-Connectivity-AMI interface ethernet1/5  delete network virtual-router WEL-PA-VR-01 routing-table ip static-route ITRON-Connectivity-AMI metric 10  delete network virtual-router WEL-PA-VR-01 routing-table ip static-route ITRON-Connectivity-AMI destination 10.16.0.0/16  delete network virtual-router WEL-PA-VR-01 routing-table ip static-route ITRON-Connectivity-AMI route-table unicast |

## WEL-SSNFW-PO1 Backout

|  |
| --- |
| WEL-SSNFW-PO1 |
| no route TRUSTED-WEL 10.16.0.0 255.255.0.0 10.218.13.1 1 |

## Mau.50 Router Backout

|  |
| --- |
| **Mau.50 router configurations** |
| no ip route 10.16.1.0 255.255.255.0 192.168.50.1 name-TEST-AMI-Servers  no ip route 10.16.9.0 255.255.255.0 192.168.50.1 name-UAT-AMI-Servers  no ip route 10.16.0.1 255.255.255.255 192.168.50.1 name-TES-Tunnel-RT |

## Tunnel Router Backout

Not applicable

# RACI

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **R** | **Responsible** | | **A** | **Accountable** | | **C** | **Consulted** | | **I** | **Informed** | | | **Chief Technology Officer** | **Delivery & Operations Manager** | **Operations Manager** | **Network Designer** | **Network Specialist** | **IT Risk and Security** | **Core Architecture** | **Itron** | **Oracle** | **Cisco** | **Palo Alto** |
|  | **Deliverable or Task** | **Ext** | **Ext** |  |  |  | | | | | | |
|  | **Network** |  |  |  |  |  |  |  |  |  |  |  |
|  | Network Design | A | A | A | R | C | C | C | C | C | - | - |
|  | Network Implementation | A | A | A | R | C | C | C | - | - | - | - |
|  | **Support** |  |  |  |  |  |  |  |  |  |  |  |
|  | Network Support - L1 | C | C | C | C | C | C | C | C | C | C | C |
|  | Network Support - L2 | A | A | A | C | R | C | C | C | C | C | C |
|  | Network Support - L3 | A | A | A | C | R | C | C | C | C | C | C |
|  | **Deliverable or Task** | **Ext** | **Ext** |  |  |  | | | | | | |
|  | Major Incident Management | A | A | A | C | R | C | C | C | C | C | C |
|  | Network Incident Management | A | A | A | C | R | C | C | C | C | C | C |
|  | Change Management | A | R | R | C | C | C | C | C | C | C | C |
|  | Problem Management | A | R | R | C | C | C | C | C | C | C | C |
|  | Annual DR Testing | A | R | R | C | C | C | C | C | C | C | C |
|  | Network Support Documentation | A | R | R | C | C | C | C | C | C | C | C |
| *Insert new rows above this one* | |  |  |  |  |  |  |  |  |  |  |  |

# Solution Compliance

The following section defines the specific WEL Architecture compliance requirements to meet our internal and external obligations. Any identified deviation from these compliance requirements should be documented, approved by an authorised Technical Delegated Authority and logged in the WEL Architecture Exemption Register for tracking and audit purposes.

## WEL Technology Strategy and Roadmap

|  |  |
| --- | --- |
|  | |
| Has the proposed Solution Design been reviewed against the WEL Technology Strategy and Roadmap? |  |
| Has an Enterprise Architect (EA) reviewed and verified the design for alignment with WEL Technology Strategy, and Roadmap? |  |
| Has WEL Networks & Security reviewed and verified the design for alignment to WEL Technology Strategy and Roadmap? |  |
| Are there any identified misalignments that need to be resolved or approved?  Any identified misalignment must be clearly documented with appropriate rationale and actions. |  |
| If YES, Have all the unresolved misalignments been documented as an Architecture or SecurityExemption and approved by an authorised Technical Authority? |  |

## Compliance Business Requirements

There may be specific compliance business requirements captured as part of the project scoping and requirements definition. For example, this may include non-discrimination requirements to ensure the designed processes and systems treat all Retain Service Providers on an equivalence basis.

|  |  |
| --- | --- |
|  | |
| Does the programme/project specify any other compliance requirements? |  |
| Does this design fully meet the additional compliance business requirements? |  |
| If YES, has an Enterprise Architect (EA) and Network designer reviewed and verified the Solution for alignment with the identified compliance requirements? |  |
| Are there any identified misalignments that need to be resolved or approved?  Any identified misalignment must be clearly documented with appropriate rationale and actions. |  |
| If YES, have all the unresolved misalignments been documented as a WEL Architecture Exemption and approved by an authorised Delegated Technical Authority? |  |
| Does this Solution Design define the recovery strategy/solution to be delivered or identify the existing DR capability as meeting recovery objectives? |  |

# Appendix A – Other Related Document Locations

* 1. Configuration Backup
  2. Login Credential Management
  3. Supporting Diagrams
  4. Related Project Documents

ODA Data Sheets

