

Final Report

Sandhy waer
u3165828@uni.canberra.edu.au

28 August 2025

1 Industrial Report

In this program, I had the privilege of contributing as a research partner in a collaboration between IP Tel Solution, an international logistics distributor, and Innovation Central Canberra (ICC). Our client, one of the world's largest supply chain providers, offers an end-to-end supply chain through a network of terminals across 60 countries, spanning all six continents. They provide global transportation services via rail, air, and sea, with a strong presence in Australia supported by ports in major cities. Renowned for services like direct shipments, contract logistics, port and terminal operations, and marine services, the company emphasises technology-driven solutions and sustainable principles. Its goal is to deliver affordable logistics while minimising environmental impact and mitigating climate change, aiming for zero carbon emissions within the next 25 years. The company is committed to strategic international distribution and expanding into next-generation, sustainable mechanisms. To achieve this, they employ strategies such as reducing diesel use, exploring low-carbon technologies, maximising renewable energy, producing low-carbon fuels, and implementing carbon offset methods. These efforts align with the mission of IP Tel and ICC to provide innovative technical solutions that turn challenges into opportunities for profitable and sustainable business growth.

IP Tel Solutions is a well-established provider of network system solutions for businesses of various sizes. They offer comprehensive designs incorporating technologies from Cisco, Aruba, and Meraki, supporting both wired and wireless networks. As a market leader, IP Tel specializes in Enterprise LAN, Wireless LAN, Cisco system design and implementation, and automated network configuration.

ICC is an innovative organisation within the University of Canberra, and was formed through a partnership with Cisco. It focuses on delivering advanced solutions to industries undergoing rapid technological and business changes. This initiative involves students and academics from diverse backgrounds, providing them with valuable hands-on experience in real-world projects. ICC's collaborative spaces are located in universities across Australia to address industry challenges in sectors such as health, education, private business, and government.

To achieve a sustainable operational system, the first step is to develop automated port services, which will initiate the reduction of fuel consumption at operational sites. Strengthening network connections across these sites is essential for this automation. Consequently, our client established a partnership with IP Tel for consultation, resulting in the creation of an initial process system that provides dual connectivity through private 5G technology and fast Wi-Fi roaming, as shown in Figure 1. The objective is to maintain a reliable network connection that consistently links critical infrastructure deployed on-site to the nearby data centre or control room.

2 Learning Outcomes

Through this internship, I was able to achieve the following learning outcomes:

2.1 Professional Application of Knowledge

I applied some of the knowledge I gained during my studies. I used concepts from the Unit, such as:

- Workflow and Process Management provides guidance on implementing Kanban and managing all tasks and processes throughout the project.
- Technology Engineering Management provides guidance on how to lead the project.
- Information Research and Methodology involves conducting a literature review of all devices deployed in the project.
- Engineering Work Experience offers guidance on how to conduct the project in a professional environment.
- Internet of Things helps in understanding how edge computing devices can create a robust and integrated network in critical infrastructure sites.
- Network Architecture develops an understanding of the conceptual design of the deployed network devices.
- Introduction to Network Engineering serves as the fundamental principle for configuring network devices.

2.2 Professional Skill Development

I gained a deeper understanding of the project development lifecycle. I was introduced to tools such as:

- Kanban for managing boards.
- Microsoft SharePoint and Google Drive serve as a professional platform to share my findings.
- Webex and Microsoft Teams for conducting professional meetings.

In addition to the project assistance tools mentioned above, I was able to develop my technical skills. I provided a literature review on some of the hardware and software involved in this program. This introduced me to various Cisco hardware devices, such as:

- Cisco Catalyst IR1835.
- Cisco Catalyst IW9165.
- Cisco Catalyst 9800.
- Cisco Air 3802i-z-k9.
- Cisco catalyst 8000v.

I also learned to perform initial configuration, understand system architecture, licensing, and configuration. I also performed virtual deployment, such as the Cisco 9800 and Cisco 8000v, which are deployed

virtually in our dedicated desktop computer and Azure cloud environment.

2.3 Networking and Mentorship

This project has also given me the opportunity to connect with people from various professional fields. I worked directly with other Network Engineers from IP Tel Solutions, who shared their insights and knowledge on how to approach this project and the technical skills needed to build the network setup. I built connections with well-known Cisco engineers, whom I often seek for technical advice. They shared their experience on tackling challenges I encountered and how these relate to similar projects they have completed. I also collaborated with our academic partners from UC and ICC to provide suitable solutions to the project's requirements. They demonstrated how to manage and guide the project from the initial planning stages through to the complete setup. I was also actively involved in weekly progress meetings with IP Tel and our academic partners. During these meetings, I presented my findings, discussed the necessary hardware and software for the project, provided reports on additional costs, and identified challenges along with estimates of how long it might take to resolve them. In general, I am confident that this project has offered me valuable professional insight into a real-world initiative that could potentially benefit our industrial partner by maximising their business profits.

2.4 Workplace Culture and Expectation

I also gained practical experience that significantly improved my communication skills. It also enhanced my productivity, as I am committed to making quick yet thoughtful decisions to tackle some of the project's challenges. During this decision-making process, I was motivated to collaborate professionally with other academics to foster a high-performance work culture. Additionally, this work environment has laid the groundwork for other vital aspects, such as maintaining a professional attitude in meetings and reporting, proper documentation, and transparency, all of which are essential. I also learned to be accountable for the results I delivered and the issues I raised, as well as to be flexible and adaptable when required.

2.5 Career Exploration and Refinement

This internship has also sparked my interest in exploring real-world applications that are profitable for industrial sectors. I was motivated to focus my career interests on technology-related areas, such as public and private 5G deployment, edge computing, network automation, and sustainability solutions in industrial sites. In short, this program could offer an opportunity to pursue a career in industrial network systems, sustainable solutions for the industrial sector, and technical consulting and innovation management.

2.6 Increase Self-Confident

I was able to develop my confidence to be presentable during a technical meeting, in which I was able to perform:

- Providing professional recommendations in technical discussions.
- Providing reliability and assurance when describing a technical concept.
- Self-reliance during the implementation of academic theory when tackling a specific issue.
- The self believes in providing valuable insights and contributing to the project team.

Overall, this internship has given me confidence that my contributions are valuable and useful in real-world projects and issues, potentially leading to profitable business outcomes.

2.7 Enhanced Employability

I am confident that this program is beneficial for career opportunities. It significantly improves my technical network engineering skills, which I can showcase through my professional portfolio and resume. I was directly involved in a 16 week real-life project, where the deliverables will be used in an actual industrial environment and for broader research opportunities. I believe that I am at least qualified for the next challenge and job opportunity based on some of the things I have done throughout this project, such as:

- Hands-on experience in real-world study cases and real network setups covers the latest Cisco technology.
- Documentation and reporting according to the industry standard.
- Gaining experience in actual project management, where I defined some required technical tasks under time constraints.
- Demonstrate the ability to present findings and results in a professional environment.

These general results are shaping my academic skills to a professional level that I can present in job applications and interviews.

2.8 Reflection and Self-awareness

However, despite all the positive results that I have gained from this program, I also reflect on some aspects that I need to improve, such as the following.

- Research in the broader network engineering field, staying up-to-date on the latest network innovations, exploring related case studies that yield similar results, and enhancing my technical skills using various online resources.
- I also reflect on how important the work environment is, as it plays a crucial role in determining the project's outcome.
- I was also able to reflect on how I respond professionally by acting under pressure, ambiguity, and feedback.

As a result, this project has improved my self-awareness in a team role and demonstrated how responsibility and determination are vital despite ongoing challenges. I also became more proactive in approaching tasks and taking the initiative to provide updates and findings on the project's progress.

2.9 Project Management Skills

This program also improves my management skills, enabling me to contribute effectively to the technical deployment. For this, I used some of the following tools.

- Using a Kanban board to add, manage, modify, update, prioritise, and track task progress.
- Coordinating meetings via Outlook and running a professional schedule using Outlook calendar search to book appointments according to other academic' schedules.

- Reporting and updating progress according to requirements and formatting professionally.

In general, it has helped me manage project development, understand milestones, carefully allocate helpful resources, and complete tasks on time alongside other priorities outside of the project.

2.10 Technical Skills Development

Key takeaways from my internship include developing valuable technical skills, working with widely-used Cisco devices across various industries, and gaining insights into key technical aspects.

- Successfully learned and configured all Cisco devices involved in this project.
- Completed a genuine network deployment using these devices in both WAN and LAN configurations.
- Able to troubleshoot wired and wireless connections.
- Understand the different modes in which the devices operate, such as Work Group Bridge (WGB), Universal Work Group Bridge (uWGB), Control and Provision Wireless Access Point (CAPWAP), Flex Connect, Bridge, Flex Mobility Express, Autonomous, and Control-Managed.
- study the system architecture of the Cisco operating system, such as IOS XE.
- The importance of the ISO layer was taken into account, especially layer two and layer three connections.
- Understand the type and model of Cisco devices and their designated regions in which they can be operated.
- Set up virtual deployment using VMware Workstation Pro to host Cisco devices.
- The interfaces of wireless connections were investigated, including 4G, 5G, and understanding the range over which these signals operate and the use of Access Point Name (APN) for cellular connections.
- Use and implement a variety of protocols such as SSH, HTTP/S, DHCP, TLS, DTLS, FTP, TCP, UDP, and ICMP.
- Measurement of signal strength using tools such as Ping and Iperf3.
- Server deployment using the Linux operating system.
- Cloud deployment of Cat8k on Azure.
- Understanding network security involves using firewalls, secure tunnels such as IPsec, VPN, and possibly deploying SD-WAN.
- Able to professionally provide documentation of network topologies, analysis, and architecture.

In general, this project provides a practical overview of industrial technologies, including edge computing, industrial networking systems, and an introduction to remote management through SD-WAN functionality.

3 Task Undertaken

Our industrial partner is actively seeking innovative solutions to enhance network connections within critical infrastructure, thereby improving security, reliability, and privacy. This initiative is driven by the rapid expansion of the global economy, which has increased demand for robust, end-to-end supply chain solutions across various sectors. Consequently, our industrial partners have approached IP Tel and ICC to verify this transformation and collaborate on developing a comprehensive testbed environment. As a result, key hardware used in this testbed was fully funded through this partnership. This testbed will serve as a platform for building and testing similar network connections, ensuring the successful realisation of this transformation and supporting the evolving needs of critical infrastructure.

3.1 Task and Responsibilities

The initial plan was to establish two separate connections: one via private 5G and another using a high-speed Wi-Fi roaming connection, employing Cisco Catalyst Industrial Wireless 9165. These connections would be supported by an edge device, specifically a Cisco Catalyst Industrial Router 1835, connecting to a dummy server that could be deployed either locally on-site or in a cloud environment. To start this project, a simple initiation task was outlined, detailing the necessary steps and responsibilities involved in establishing this system as part of the core duties. Some of these responsibilities are listed below.

- Carrying out literature review and technical evaluation of Key Cisco Devices used in this project. This includes:
 - Ensuring that all funded hardware is listed and present.
 - Verifying that there are no faults in each item.
 - Providing hardware descriptions and functionalities.
 - Analysing the key components, such as the IR1835's 5G/4G/Wi-Fi modem, the LAN and WAN port, storage capacity, power adapter, power options, system architecture of IOS XE, a Suitable working mode for IW9165 AP bridge, Configuration option via console port, web interface, or SSH. For more information on equipment used in this project, see [3.3.2](#).
- Performing the initial configuration and network setup to mimic the same network connection intended for this project, such as shown in Figure [2](#). To achieve this task, the following are required:

Local Deployment

Cisco AIR AP 3802i - Z - K9

- Ensuring that Cisco AP 3802i is the regulated device in the Australian and New Zealand region, as indicated by the Z in the device model. More details of AIR AP can be seen in [3.3.2](#).
- Powering the AIR AP with an Ethernet cable RJ45 - 8 pin as in Figure [11](#), by connecting directly to the green Ethernet socket for accessing the testbed LAN.
- Using a USB-RJ45 console cable in Figure [12](#) to access the CLI of the AP.
- Ensuring that AP is operated in Control and Provisioning Wireless Access Point or CAPWAP mode. In this mode, the AP will automatically search for a nearby wireless LAN controller (Cisco Catalyst 9800v WLC) within the subnet. AP deployment can be seen in Figure [3](#).

Desktop Computer

- Setting up a dedicated desktop computer in the testbed environment such as shown in Figure 25.
- Connecting the computer to the LAN network of the testbed environment via an RJ45 Ethernet cable.
- Downloading and installing Putty. If it is not installed.
- Downloading and installing the VCP driver to enable Putty to access the console port.
- Downloading and installing VMware Workstation Pro.
- Downloading the OVA file of Cisco v9800 WLC.
- Running the file in VMware Workstation Pro to create a virtual 9800 wireless LAN controller.
- Performing day 0 configuration, such as setting the username, password, enable password, static IP (in the same subnet as the testbed LAN), and the IP routing
- Configuring v9800 wlc to be connected with Cisco AIR 3802i (If v9800 wlc is deployed in the same subnet as AIR AP 3802i then AIR AP will automatically assign to v9800 wlc via CAPWAP mode)
- Creating WAN profile. This includes: onboarding AIR AP 3802i.
- Accessing the Web UI of v9800 WLC through the configured static AP and confirming that the AIR AP is registered in the WAN dashboard.
- Creating the AIR AP profile (This can be done via CLI on a desktop computer or in the WEB UI)
- Through the WAN dashboard in the WEB UI, define the SSID name and SSID key to enable the AIR AP to provide Wi-Fi coverage around the testbed environment, which will be used as the parent AP for IW9165 that bridges traffic from IR1835.

Cisco IR1835 Router

- Performing initial installation for the IR1835, such as powering the router with a power adapter, since the router is not directly deployed in a fleet vehicle as intended with the OBD2 cable for CANBUS plus power combo. Information about OBD2 - CANBUS can be seen in [3.3.2](#).
- Installing an Appropriate SIM card for the 5G modem. In this case, we utilise a Telstra SIM as the Cisco-supported cellular service within the Australian region. Installing guide and modem details can be seen in [3.3.2](#). (*NOTE: Current private 5G deployments are in progress; therefore, the validation process is carried out by employing a public mobile operator*)
- Installing 9 in 1 Antenna for IR1835 Router as shown in Figure 3. More information about the antenna overview and installation guide can be seen in [3.3.2](#).
- Accessing router CLI via console port with USB-micro B console cable while using Putty in Windows OS or Minicom in Ubuntu Linux OS, with 9600 baud rate for IR1835.

- Performing the day 0 deployment or initial configuration, such as verifying the right IOS XE version, configuring username, password, and web interface management details.
- Configuring layer 3 GigabitEthernet 0/0/0 interface, to receive an IP address from our LAN DHCP server.
- Configuring cellular interface 0/5/0 to receive an IP address through Telstra Access Point Name(APN) to maintain a direct cellular connection as shown in Figure 6.
- Configuring the IP routing for Router IR1835 so that the layer three interface can direct traffic into the internet through the GigabitEthernet 0/0/0.

Cisco IW9165 Access Point

- Conducting initial installation of the access point by removing the antenna cover used for Wi-Fi transmission.
- Powering up the access point with an Ethernet Cable 8-pin RJ45 that is connected directly to the Wired 0 interface, which functions as Power over Ethernet (PoE). This is also reflected in the requirements, where the access point will be powered from IR1835's LAN port, indicating these two devices are on the same platform, and IW9165 is in WGB mode.
- Connecting GigabitEthernet 0/0/0 of IR1835 to wired 1 of IW9165 via an 8 pin Ethernet Cable RJ45
- Accessing the CLI of the access point via USB-RJ45 console cable through the Ethernet console port.
- Performing day 0 configuration, such as checking the right IOS XE version of the AP, setting the username, password, enable password.
- Checking the right software image that runs in the AP, ensuring that the AP runs the Unified Industrial Wireless (UIW) image, which supports the intended AP mode use in this setup, WGB/uWGB.
- Setting the static IP to be an unrouteable IP address. For example, if the DHCP pool of the LAN is 10.0.0.* Then the unrouteable IP is set to 10.10.1.1.
- Disabling the Wi-Fi 6/IEEE.802x, and just enable Wi-Fi 5/IEEE.802ac. *NOTE: The WGB is only working with the 5 GHz Wi-Fi band and not the 2.5 GHz band. Also, the AIR AP 3802i does not support Wi-Fi 6.*
- Creating the SSID profile. This includes defining the SSID profile name, assigning this profile to the SSID name of AIR AP 3802i, including the SSID key, and defining the authentication type used in the AIR AP 3802i SSID.
- Configuring the AP mode into Work Group Bridge by assigning the SSID profile to one of the three Wi-Fi antennas of IW9165 AP to establish a Wi-Fi bridge connection between AIR AP and IW9165 AP. The WGB configuration can be seen in Figure 5.
- Ensuring that the bridge connections are established between the two APs. To confirm this, check the CLI message on IW9165 or through the WAN dashboard of v9800 wlc that shows a client with GigabitEthernet 0/0/0 MAC address has been registered. *NOTE: If the connection is established correctly, then the interface GigabitEthernet 0/0/0 will receive an IP address from*

the testbed LAN DHCP server as presented in Figure 7.

Cloud Deployment

Azure Cloud

- Creating an Azure account with the staff ID to obtain the \$300 credit.
- Using the credit to obtain the Cisco Catalyst 8000v from the Azure Marketplace.
- Performing initial installation by deploying the Cat8k in Azure and selecting the appropriate subscription method, which in this case, uses a pay-as-you-go (PAYG) subscription, from which the \$300 credit is deducted.

Cisco Catalyst 8000v

- Performing the initial configuration, such as setting up the virtual device name, key management, enabling public IP address, enabling SSH protocol for remote access, defining other protocols used, defining device storage and capacity, defining the size of the Network Interface Card needed (by default, two NICs are automatically assigned to the virtual Cat8k), and creating the username, password, and enable password.
- Accessing the console port through Azure or SSH with remote access to check the current image version that is running. NOTE: For this project, the SD-WAN license is in progress to be finalised; hence, it is currently running in autonomous mode. To enable SD-WAN capability, the Cat8k needs to be configured in Controll-managed mode.
- Ensuring that Gigabit-Ethernet 1 is receiving an IP address from Azure DHCP by default. NOTE: This local IP is directly translated in Azure Network Address Translation (NAT) to receive outside traffic via a public IP.
- Creating a different subnet that faces inside the Cat8k by defining a static route to the Gigabit-Ethernet 2. This is where the dummy server will be deployed.

Ubuntu Linux

- Deploying a virtual Linux OS in the cloud, ensuring that the capacity is within the appropriate cost for the \$300 credit.
- Performing the initial configuration, such as defining device name, management key, protocols, and public IP address.
- Defining the network interface by giving the static IP to the device, and it needs to be in the same IP pool as GigabitEthernet 2 of Cat8k.
- Defining the IP route for the virtual machine where the last resort of the traffic is the GigabitEthernet 2 as its gateway.
- Ensuring the connection has been established by pinging the gateway from the server and vice versa.

NOTE: The Cat8k is reachable from outside traffic; however, it can not pass the traffic to see the content that is deployed in the Linux server behind it. Therefore, an additional Linux virtual machine

is deployed outside the above-configured subnet for temporary testing.

- Deploying another Ubuntu Linux with minimal storage that fits with \$300 credit.
- Allowing the server to receive a public IP address
- Configuring device name, management key, SSH protocol for remote access, and defining the required protocol.
- Ensuring the connection is established by SSH into the device from the local machine.

If the deployment is correct, there will be three virtual machines deployed as shown in Figure 4.

- Testing the connection of the testbed network, ensuring that the end device IR1835 can reach the stand alone server deployed in Azure.
- Documenting, updating, and reporting each milestone as the project progresses through weekly meetings.

3.2 Tools and Application Utilised

- VMware Workstation Pro. It was used as the host for some of the virtual images that are essential for this project.
- Microsoft Teams and Webex for a professional meeting and chat platform.
- Microsoft Outlook for emailing and scheduling.
- Microsoft SharePoint and Google Drive for a file sharing, version control, and storage platform.
- Microsoft Visio to draw and illustrate the network topology and to carry out system models.
- Kanban via Azure DevOps to display project management, task initiation, and track workflow.
- Virtual Cisco Catalyst 9800. It was used as a replacement for the actual Cisco 9800. It functions as a wireless LAN controller to manage lightweight Cisco APs, such as Cisco AIR AP 3802i, that was used in this setup. This was achieved by obtaining the OVA file from the official Cisco website, and the deployment was made on VMware Workstation Pro.
- Virtual Cisco Catalyst 8000. This was used to provide SD-WAN capability, which will be deployed in the next phase of this project.
- Virtual Ubuntu Linux for a dummy server, to which data is sent.
- Azure cloud environment to host both Catalyst 8000v and the dummy server.
- Putty for Windows OS and Minicom for Ubuntu Linux were utilized to gain access to Cinco devices' command line interface (CLI) via the console cable.

3.3 Data, Research Materials, and Work Outputs

3.3.1 Data

Figure 1: System Approach

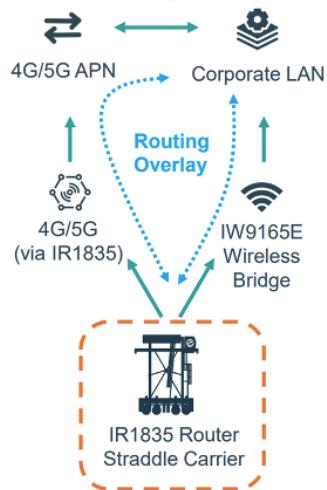


Figure 2: Testbed Implementation Network

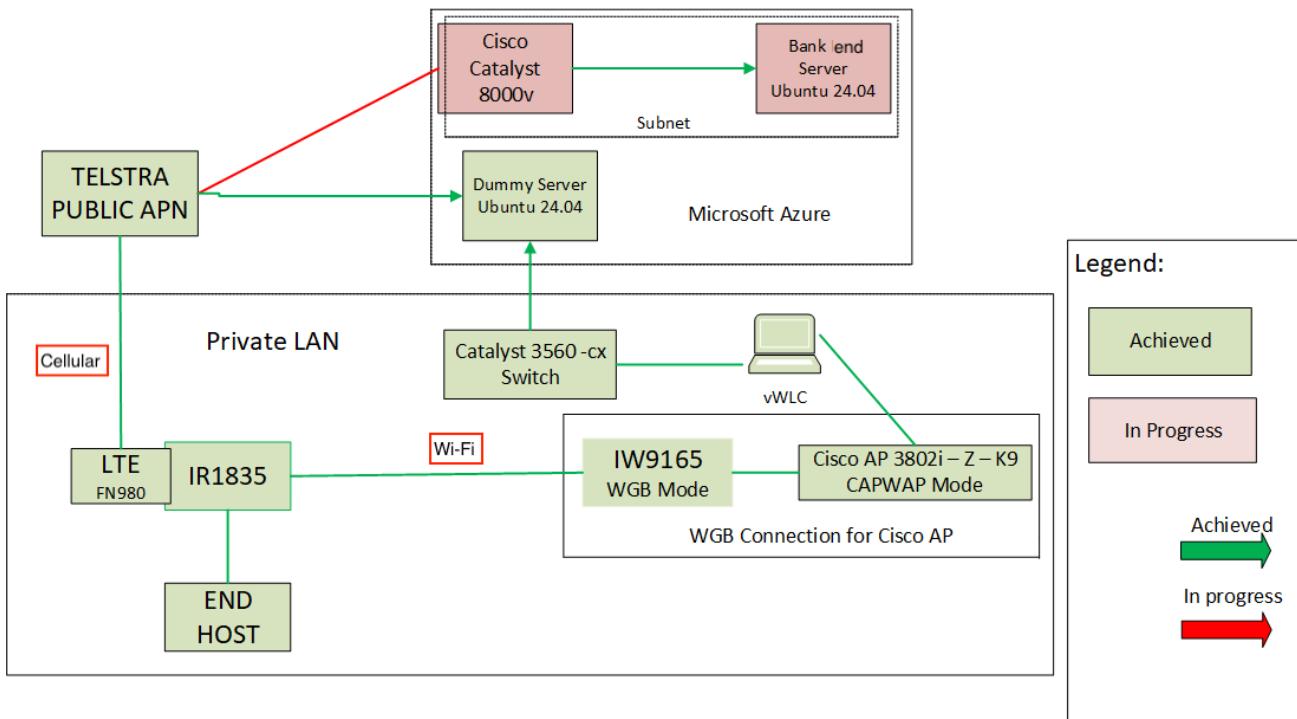


Figure 3: Local deployment within a private LAN according to the testbed network

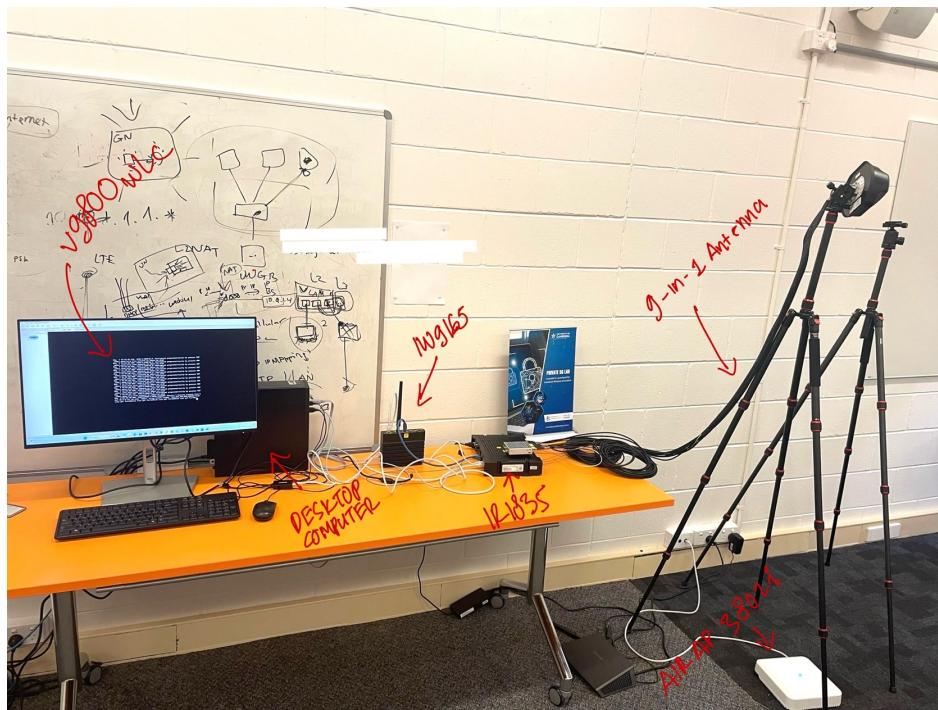


Figure 4: Cloud deployment for Cat8k, backend server via cat8k, and stand alone server

Azure services



Resources

Recent	Favorite						
Stand alone virtual machine		Type	Last Viewed				
	vServer	Virtual machine					a day ago
	Cisco8000v-vnet	Virtual network					3 days ago
	backend-server	Connected	Virtual machine				3 days ago
	cisco8000v	Virtual machine					3 days ago
	catalysts8000v	Resource group					3 weeks ago
	UCICC	Route table					3 weeks ago
	backend-server812_z1	Network Interface					3 weeks ago
	cisco8000v127_z1	Network Interface					3 weeks ago
	cisco8000vip746	Public IP address					3 weeks ago
	c8000v-inside-nic	Network Interface					3 weeks ago
	backend-server-ip	Public IP address					3 weeks ago
	Virtual-server	Resource group					a month ago

See all

Figure 5: WGB Configuration for Cisco IW9165 AP

```
### WGB Running config - Hostname: Router-IW9165 ###

configure ap management add username UCICC password $1$$e0C6lzD.33KSjvp1mod/K. secret $1$$e0C6lzD.33KSjvp1mod/K.
configure ap hostname Router-IW9165
configure ap address ipv4 static 10.0.1.10 255.255.255.0 10.0.1.245
configure ssid-profile UCICC-PROFILE ssid UCICC-WIFI authentication psk U2FsdGVkX19zcVmOKp9uyXkKKeXUiMGzK7KbMAQX8xc= key-management wpa2
configure dot11Radio 1 mode wgb ssid-profile UCICC-PROFILE
configure dot11Radio 1 enable
configure wgb uclient timeout 300
configure wgb mobile station interface dot11Radio 1 scan 36 add
configure l2nat default-vlan 1
configure wgb ethport 0 native-vlan id 1
configure dot11Radio 1 802.11ax disable
configure dot11Radio 1 profile customized-wmm enable

*** End of WBridge configurations ***
```

Figure 6: Cellular Configuration with an active APN profile

```
Router-IR1835#show cellular 0/5/0 all
Hardware Information
=====
Modem Firmware Version = M0H.030202
Host Firmware Version = A0H.000302
Device Model ID = FN980
International Mobile Subscriber Identity (IMSI) = 505012000505581
International Mobile Equipment Identity (IMEI) = 351533923292937
Integrated Circuit Card ID (ICCID) = 89610180004292541341
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) = +61497445858
Modem Status = Modem Online
Current Modem Temperature = 39 deg C
PRI version = 1080-115, Carrier = Telstra
OEM PRI version = 1080-115

Profile Information
=====
Profile 1 = ACTIVE* *
-----
PDP Type = IPv4
PDP address = 100.90.214.145
IPv4 PDP Connection is successful
Access Point Name (APN) = telstra.internet
Authentication = None
    Primary DNS address = 10.3.41.226
    Secondary DNS address = 10.3.24.11
```

Figure 7: Gigabit Ethernet Configuration

```

Router-IR1835#show ip interface brief
Interface          IP-Address      OK? Method Status           Protocol
GigabitEthernet0/0/0 10.0.0.182    YES DHCP   up                up
GigabitEthernet0/1/0 unassigned     YES unset  up                up
GigabitEthernet0/1/1 unassigned     YES unset  administratively down down
GigabitEthernet0/1/2 unassigned     YES unset  down               down
GigabitEthernet0/1/3 unassigned     YES unset  down               down
W10/1/4            unassigned     YES unset  up                up
Cellular0/4/0       unassigned     YES NVRAM administratively down down
Cellular0/4/1       unassigned     YES NVRAM administratively down down
Cellular0/5/0       10.242.16.64   YES IPCP   up                up
Cellular0/5/1       unassigned     YES NVRAM down               down
Async0/2/0          unassigned     YES unset  up                down
Async0/2/1          unassigned     YES unset  up                down
VirtualPortGroup0  192.168.0.1   YES NVRAM up                 up
Vlan1              unassigned     YES unset  up                up
Vlan4              unassigned     YES DHCP   administratively down down

Router-IR1835#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is 10.0.0.1 to network 0.0.0.0

S*  0.0.0.0/0 [1/0] via 10.0.0.1
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C  10.0.0.0/24 is directly connected, GigabitEthernet0/0/0
L  10.0.0.182/32 is directly connected, GigabitEthernet0/0/0
C  10.242.16.64/32 is directly connected, Cellular0/5/0
    192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C  192.168.0.0/24 is directly connected, VirtualPortGroup0
L  192.168.0.1/32 is directly connected, VirtualPortGroup0

```

3.3.2 Research Materials

- IR1835-K9 refers to a highly modular rugged series router designed to maximise IoT features in industrial areas, with key functions such as 5G, 4G LTE, Wi-Fi 6, Gigabit Ethernet, CAN BUS, dead reckoning and Global Navigation Satellite System (GNSS). It is also powered by Cisco IOS XE, an advanced operating system to enhance its performance. Installation and initial configuration were

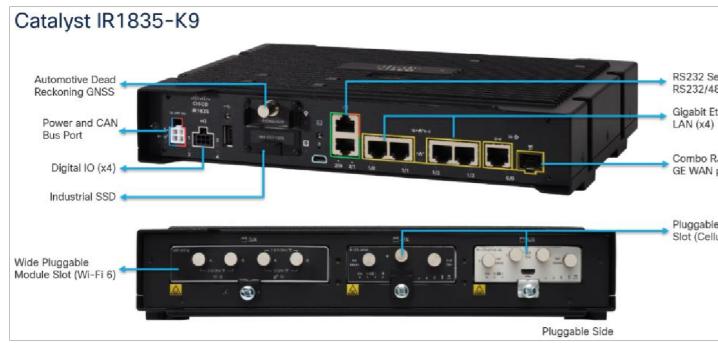


Figure 8: Cisco Catalyst IR1835-k9

based on the following Cisco manuals: [Router IR1800 Overview](#), [Router IR1835-K9 installation guide](#), [IOS XE Configuration for IR1800](#).

- OBD2-J1962YA-MF4 is an OBD-II (J1962) Type A to IR1800 cable wired; OBD → On Board Diagnostic, used to transfer data between the vehicle's OBD2 system and external devices, such as diagnostic tools or computers. It is also compatible with the CAN BUS connector with its Mini Fit 4 (MF4) Connector.



Figure 9: OBD2-J1962YA-MF4 cable

For more details, see the following: [Cable Overview \(NOT THE ACTUAL ITEMS FROM CISCO OFFICIAL WEBSITE\)](#), and [Digital Input Output, Ignition, and CAN Bus Connectivity](#).

- USB Type A to USB Micro-B (2m) cable used to connect the router IR1835 through its USB micro-B port to a USB Type A in an external device, such as a user computer, for initial configuration or troubleshooting. However, User computers are required to have a VCP (Virtual COM Port) drive to enable communication with the CP210x USB to UART.



Figure 10: USB Type A to USB Micro-B (2m)

This cable requires the installation of a VCP driver. The use of this cable was based on the following Cisco manual: [IR1800 Connecting Process](#) and [VCP Driver installation link for those who do not have VCP installed in their devices](#).

- 8-pin RJ45 Ethernet Cable Connector with PoE capability. This is used to connect devices to the green Ethernet socket wall in the test bed environment. It was also used to provide a connection between the edge devices IR1835 and IW9165.

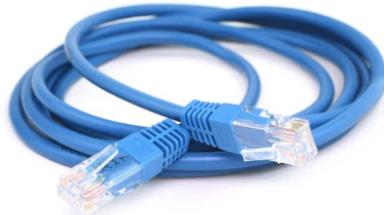


Figure 11: Ethernet Cable RJ45 - 8 pin

- RJ45 - USB console cable, which provides access to perform initial configuration on Cisco Catalyst IW9165 and Cisco air AP 3802i - Z - K9. The baud rate is 115200, which is according to the IW9165 configuration guideline.



Figure 12: URJ45 - USB console cable

This cable requires the installation of a VCP driver. The use of this cable was based on the following Cisco manual: [IW9165 Connector and Ports](#) and [USB-RJ45 Console Cable Overview](#)

- IR1800-DINRAIL is a DIN RAIL kit for IR1800. It was used to mount IR1835 in the preferred mount position according to the project's requirements.

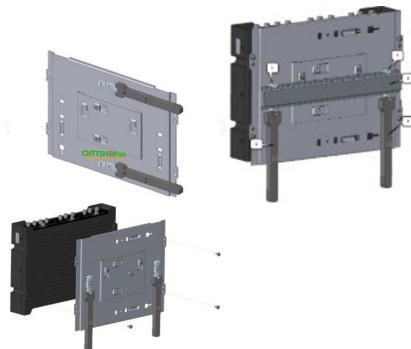


Figure 13: IR1800-DINRAIL

However, the router is not mounted in a specific position but is placed in a safe working space to provide mobility during the configuration process. For more information on the DIN RAIL Kit, see the following: [IR1800 Rugged Series Din Rail Installation Guide](#).

- P-LTEAP18-GL is a plug-in modem with CAT18 LTE Advanced PRO. As a Cisco LTE Advanced Pro



Figure 14: P-LTEAP18-GL

CAT 18 pluggable Interface Module (PIM), it is designed to offer high-speed cellular 4G LTE connectivity for the Cisco IR1800 router. The installation guide was based on the following Cisco manual: [P-LTEA18-GL PIM Overview](#) and [Installing SIM card into PIM](#).

- P-5GS6-GL is an interface module for IoT Routers, particularly the IR1800, which is a pluggable interface module (PIM) designed for Cisco routers, including the IR1800 series. Key features include 5G connectivity, global coverage, and enhanced performance, providing reliable and high-quality wireless WAN connectivity. However, to maximize connection to the 5G band signal range, such as in n77 or n78, the modem model must be in EM9293 and not in FN980.



Figure 15: P-5GS6-GL

During deployment, this PIM connects to a 5GANTM 0-4-B antenna to initiate its operation, with configuration accessible through the Cisco IOS XE operating system. The installation guide was based on the following Cisco manual: [5G pluggable Interface Module Overview](#) and [Installing SIM card into PIM](#).

- A Telstra SIM card is required to enable the modem to work properly, since Telstra is the only mobile network operator that supports the above Cisco modems within the Australian region. For information on SIM card installation, use the SIM card to PIM installation link above from the P-5GS6-GL section.



Figure 16: Telstra SIM card

- WiFi6 pluggable modem for IoT routers such as the IR1800 model. This module improves the ability of the router to provide robust and reliable wireless connectivity in various industrial and mobile environments. However, this Wi-Fi modem is not used in this setup, as the IW9165 AP is used to provide a Wi-Fi bridge to a nearby parent AP.



Figure 17: WP-WIFI6-Z

Installation and configuration can be found in the following, [Wireless Interface Module overview](#)

- IRM-GNSS-ADR is an Automotive Dead Reckoning GNSS Module. It is used to provide an accurate location during the disturbance of the satellite signal in the GPS system.



Figure 18: IRM-GNSS-ADR

It uses previously recorded data to estimate the exact location of the object by measuring speeds, time, and directions. To enable this feature, manual configurations are required through the Cisco IOS XE software/operating system. The installation guide was based on the following Cisco manual: [IRM-GNSS-ADR installation](#) and [GNSS configuration with Cisco IOS XE software](#).

- IRM-SSD-100GB is a 100 GB SSD storage module designed for industrial environments.



Figure 19: IRM-SSD-100GB

It provides mainly an extra 100GB of flash memory for the router and is also used for application data in the Cisco IOS XE operating system. The installation was performed in the following Cisco manual: [SSD module overview](#).

- PWR-MF4-125W-AC is a power supply adapter that converts AC to DC for IR1800.



Figure 20: PWR-MF4-125W-AC

It has a sleek industrial design and provides 125 watts of power. The adapter supports multi-voltage input from 12 to 14 V DC and can be adjusted from 9 to 36 V DC. It effectively transforms power from a standard outlet. The overview of the adapter can be found as follows [Adapter Overview](#).

- The 5G-ANTM-O-4-B is a 9-in-1 outdoor black antenna 5G Sub-6GHz / 4G LTE. This omnidirectional 5G antenna is designed for Cisco industrial routers, such as the IR1800 model.



Figure 21: 5G-ANTM-O-4-B

It offers high-performance 5G and LTE cellular connectivity, dual-band Wi-Fi, and GNSS (GPS). During deployment, the antenna connects to a plug-in module interface, as shown in Figure 21. The installation was carried out according to the following [Antenna Overview and Installation Guide](#).

- The IW9165E-Z-WGB, also known as an IW9165, 11ax 6E, with 4 RF ports and a Z domain W, refers to the IW9165E Cisco Catalyst access point supporting IEEE 802.11ax (Wi-Fi 6), as shown in the description as 11ax 6e.



Figure 22: IW9165E-Z-WGB

It features four removable radio frequency ports for external antennas (4 RF ports) and is used to deploy wireless infrastructure for system automation through a wireless network. The installation and configuration were made according to the following, [Router IW9165 Overview, Installation Guide, Cisco IW9165 access point configuration](#).

- IW-PWRADPT-MFT4P is a Power Adapter AC-DC Micro-Fit 4 Pin connector.



Figure 23: IW-PWRADPT-MFT4P

IW-PWRADPT-MFT4P is a power supply adapter that provides an option to generate power for the Cisco IW9165 access point in addition to Power over Ethernet (PoE) capability. The overview of the device can be found in the following, [IW-PWRADPT-MFT4P Adapter Overview](#).

- The Cisco AIR 3802i-Z-K9 was used to connect to IW9165 via Wi-Fi.



Figure 24: Cisco AIR AP 3802i - Z - k9

As a lightweight access point, it must operate in CAPWAP mode so that IW9165 can be used in the Work Group Bridge to connect IR1835 to a dummy server. The configuration and general configuration of the Aironet 3800 were performed according to the following Cisco manual: [Cisco 3800 Overview](#).

- A dedicated desktop computer to host VMware Workstation Pro as a virtual platform running Cisco v9800 WLC. This desktop is equipped with a keyboard, a monitor, and a mouse, as shown in the figure below.

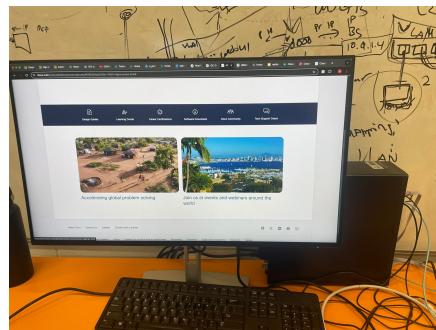


Figure 25: Dedicated desktop

3.3.3 Licensing and Agreement

- CON-L1NBD-IR1835RK or known as CX LEVEL 1 8X5XNBD Cisco Catalyst IR1835 is licensed to receive the right to Cisco customer service level 1 for 8 hours a day in 5 business days, for equipment support on the Cisco IR1835 router when the device was purchased.
- SL-1800-NA / PRF-K9 or known as the Network Advantage License for Cisco IR1800 is intended as a license that gives permission to the router IR1800 and its software capability and security during the deployment stage.
- CON-L1NBD-IW9165BG or known as CX LEVEL 1 8X5XNBD IW9165, 11ax 6E, 4 RF. It refers to Cisco customer care level 1, which provides technical support for the IW9165 router if it is not working properly or experiencing a technical issue.

3.3.4 Works Output

Test Plan

To check the stability of the connection according to Figure 2, the following set of tests was established.

- Confirming that both of the interfaces are receiving an IP address.
- Confirming that the IR1835 can reach outside traffic by pinging the Google DNS server IP: 8.8.8.8.
- Running a lightweight Iperf docker in the IR1835. (*NOTE: Due to the NDA, these steps can not be presented*)
- Testing the cellular connection via P5GS6- GL modem that directly connected to the Telstra APN. During this testing, the GigabitEthernet 0/0/0 is shutdown mode.
 - Sending an ICMP packet by pinging the cloud-deployed server from the Docker.
 - Testing TCP and UDP with Iperf3 from the Docker.
- Testing the Wi-Fi connection via gigabitethernet 0/0/0 that directly connected to IW9165, which bridges traffic to the parent AP, Cisco AIR AP 3802i. During this testing, the cellular 0/5/0 is in shutdown mode.
 - Sending an ICMP packet by pinging the cloud-deployed server from the Docker.
 - Testing TCP and UDP with Iperf3 from the Docker.

Result

- Both interfaces are assigned an IP address, and the IR1835 can reach the outside network as shown in the Figures below.

Figure 26: Cellular Configuration

```
Router-IR1835#show running-config interface cellular 0/5/0
Building configuration...

Current configuration : 185 bytes
!
interface Cellular0/5/0
  mtu 1456
  ip address 100.90.225.9 255.255.255.0
  ip tcp adjust-mss 1416
  dialer in-band
  dialer watch-group 1
  dialer-group 1
  ipv6 enable
  pulse-time 1
end

Router-IR1835#
```

Figure 27: GigabitEthernet Configuration

```
Router-IR1835#show running-config interface gigabitethernet 0/0/0
Building configuration...

Current configuration : 156 bytes
!
interface GigabitEthernet0/0/0
  ip dhcp client update dns server both
  ip address 10.0.0.177 255.255.255.0
  negotiation auto
  spanning-tree portfast
end

Router-IR1835#
```

Figure 28: IR1835 as an end host is able to reach Google DNS server

```
Router-IR1835#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/96/280 ms
Router-IR1835#ping www.google.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.26.60, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/38/44 ms
Router-IR1835#
```

- The network Connection via the cellular interface 0/5/0 with the P5GS6-GL modem and Telstra APN is properly established, indicating that data can be transferred to the server via the Cellular pathway. This proves that the system approach in Figure 1 and Figure 2 has been achieved.

- ICMP testing.

```
/app # ping 4.147.153.81
PING 4.147.153.81 (4.147.153.81): 56 data bytes
64 bytes from 4.147.153.81: seq=0 ttl=50 time=31.234 ms
64 bytes from 4.147.153.81: seq=1 ttl=50 time=40.336 ms
64 bytes from 4.147.153.81: seq=2 ttl=50 time=39.868 ms
64 bytes from 4.147.153.81: seq=3 ttl=50 time=39.531 ms
64 bytes from 4.147.153.81: seq=4 ttl=50 time=29.805 ms
64 bytes from 4.147.153.81: seq=5 ttl=50 time=39.495 ms
64 bytes from 4.147.153.81: seq=6 ttl=50 time=39.365 ms
64 bytes from 4.147.153.81: seq=7 ttl=50 time=39.112 ms
64 bytes from 4.147.153.81: seq=8 ttl=50 time=38.912 ms
64 bytes from 4.147.153.81: seq=9 ttl=50 time=39.170 ms
64 bytes from 4.147.153.81: seq=10 ttl=50 time=37.947 ms
64 bytes from 4.147.153.81: seq=11 ttl=50 time=38.236 ms
64 bytes from 4.147.153.81: seq=12 ttl=50 time=28.509 ms
^C
--- 4.147.153.81 ping statistics ---
13 packets transmitted, 13 packets received, 0% packet loss
round-trip min/avg/max = 28.509/37.040/40.336 ms
```

Figure 29: Ping result for cellular connection

- TCP and UDP testing.

```

REMOTE-SERVER@vServer:~$ iperf3 -s
-----
[ Server listening on 5201 (test #1)
Accepted connection from 1.145.25.43, port 2760
[ 5] local 10.0.0.4 port 5201 connected to 1.145.25.43 port 2761
[ ID] Interval Transfer Bitrate
[ 5] 0.00-1.00 sec 2.00 MBytes 16.8 Mbits/sec
[ 5] 1.00-2.00 sec 6.12 MBytes 51.4 Mbits/sec
[ 5] 2.00-3.00 sec 1.25 MBytes 60.8 Mbits/sec
[ 5] 3.00-4.00 sec 6.50 MBytes 54.5 Mbits/sec
[ 5] 4.00-5.00 sec 6.75 MBytes 56.7 Mbits/sec
[ 5] 5.00-6.00 sec 7.00 MBytes 58.7 Mbits/sec
[ 5] 6.00-7.00 sec 7.38 MBytes 61.9 Mbits/sec
[ 5] 7.00-8.00 sec 7.12 MBytes 59.8 Mbits/sec
[ 5] 8.00-9.00 sec 6.50 MBytes 54.5 Mbits/sec
[ 5] 9.00-10.00 sec 6.75 MBytes 56.6 Mbits/sec
[ 5] 10.00-10.08 sec 640 KBytes 65.9 Mbits/sec
[ ID] Interval Transfer Bitrate
[ 5] 0.00-10.08 sec 64.0 MBytes 53.3 Mbits/sec
----- receiver
[ Server listening on 5201 (test #2)
Accepted connection from 1.145.25.43, port 2762
[ 5] local 10.0.0.4 port 5201 connected to 1.145.25.43 port 2758
[ ID] Interval Transfer Bitrate Jitter Lost/Total Datagrams
[ 5] 0.00-1.00 sec 1.16 MBytes 9.71 Mbit/sec 1.778 ms 0/872 (0%)
[ 5] 1.00-2.00 sec 1.19 MBytes 10.0 Mbit/sec 1.625 ms 0/900 (0%)
[ 5] 2.00-3.00 sec 1.19 MBytes 10.0 Mbit/sec 1.531 ms 0/900 (0%)
[ 5] 3.00-4.00 sec 1.19 MBytes 9.98 Mbit/sec 1.594 ms 0/896 (0%)
[ 5] 4.00-5.00 sec 1.19 MBytes 9.99 Mbit/sec 1.655 ms 0/897 (0%)
[ 5] 5.00-6.00 sec 1.20 MBytes 10.0 Mbit/sec 1.594 ms 0/901 (0%)
[ 5] 6.00-7.00 sec 1.19 MBytes 9.98 Mbit/sec 1.611 ms 0/896 (0%)
[ 5] 7.00-8.00 sec 1.19 MBytes 10.0 Mbit/sec 1.625 ms 0/898 (0%)
[ 5] 8.00-9.00 sec 1.19 MBytes 9.94 Mbit/sec 1.777 ms 0/893 (0%)
[ 5] 9.00-10.00 sec 1.19 MBytes 10.0 Mbit/sec 1.835 ms 0/899 (0%)
[ 5] 10.00-10.03 sec 38.1 KBytes 10.6 Mbit/sec 1.695 ms 0/29 (0%)
[ ID] Interval Transfer Bitrate Jitter Lost/Total Datagrams
[ 5] 0.00-10.03 sec 11.9 MBytes 9.97 Mbit/sec 1.695 ms 0/8981 (0%) receiver
----- receiver
[ Server listening on 5201 (test #3)
Accepted connection from 1.145.25.43, port 2763
[ 5] local 10.0.0.4 port 5201 connected to 1.145.25.43 port 2759
[ ID] Interval Transfer Bitrate Jitter Lost/Total Datagrams
[ 5] 0.00-1.00 sec 6.51 MBytes 54.6 Mbit/sec 0.309 ms 2457/7358 (33%)
[ 5] 1.00-2.00 sec 6.38 MBytes 53.5 Mbit/sec 0.298 ms 4269/9976 (47%)
[ 5] 2.00-3.00 sec 6.27 MBytes 52.6 Mbit/sec 0.238 ms 4280/9900 (48%)
[ 5] 3.00-4.00 sec 7.52 MBytes 63.1 Mbit/sec 0.307 ms 3424/9900 (38%)
[ 5] 4.00-5.00 sec 8.80 MBytes 73.8 Mbit/sec 0.166 ms 2594/9223 (28%)
[ 5] 5.00-6.00 sec 7.44 MBytes 62.4 Mbit/sec 0.198 ms 3224/8827 (37%)
[ 5] 6.00-7.00 sec 7.45 MBytes 62.5 Mbit/sec 0.361 ms 3224/8837 (36%)
[ 5] 7.00-8.00 sec 7.42 MBytes 62.3 Mbit/sec 0.299 ms 3443/9934 (38%)
[ 5] 8.00-9.00 sec 6.46 MBytes 54.2 Mbit/sec 0.592 ms 3352/8215 (41%)
[ 5] 9.00-10.00 sec 7.10 MBytes 59.5 Mbit/sec 0.360 ms 4524/9870 (46%)
[ 5] 10.00-10.28 sec 1.15 MBytes 34.7 Mbit/sec 0.451 ms 409/1275 (32%)
[ ID] Interval Transfer Bitrate
[ 5] 0.00-1.00 sec 11.9 MBytes 100 Mbit/sec 0.000 ms 0/8981 (0%) receiver
----- receiver
[ ID] Interval Transfer Bitrate Total Datagrams
[ 5] 0.00-1.00 sec 11.9 MBytes 100 Mbit/sec 0.000 ms 0/8981 (0%) receiver
[ 5] 1.00-2.00 sec 11.9 MBytes 99.9 Mbit/sec 0.000 ms 0/8980 (0%) receiver
[ 5] 2.00-3.00 sec 11.9 MBytes 100 Mbit/sec 0.000 ms 0/8980 (0%) receiver
[ 5] 3.00-4.00 sec 11.9 MBytes 100 Mbit/sec 0.000 ms 0/8980 (0%) receiver
[ 5] 4.00-5.00 sec 11.9 MBytes 100 Mbit/sec 0.000 ms 0/8980 (0%) receiver
[ 5] 5.00-6.00 sec 11.9 MBytes 100 Mbit/sec 0.000 ms 0/8980 (0%) receiver
[ 5] 6.00-7.00 sec 11.9 MBytes 100 Mbit/sec 0.000 ms 0/8980 (0%) receiver
[ 5] 7.00-8.00 sec 11.9 MBytes 100 Mbit/sec 0.000 ms 0/8980 (0%) receiver
[ 5] 8.00-9.00 sec 11.9 MBytes 100 Mbit/sec 0.000 ms 0/8980 (0%) receiver
[ 5] 9.00-10.00 sec 11.9 MBytes 100 Mbit/sec 0.000 ms 0/8980 (0%) receiver
[ ID] Interval Transfer Bitrate Jitter Lost/Total Datagrams
[ 5] 0.00-10.00 sec 11.9 MBytes 100 Mbit/sec 0.000 ms 0/8980 (0%) receiver
[ 5] 0.00-10.28 sec 72.5 MBytes 59.2 Mbit/sec 0.451 ms 35200/8980 (39%) receiver
----- receiver

```

Figure 30: TCP & UDP result for cellular connection

- The network Connection via the Gigabit interface 0/0/0 with Cisco Catalyst IW9165 that bridges traffic via Wi-Fi transference to AIR AP 3802i, as shown in Figure 2, has been achieved. This validates the system approach in Figure 1.

- ICMP testing.

```

/app # ping 4.147.153.81
PING 4.147.153.81 (4.147.153.81): 56 data bytes
64 bytes from 4.147.153.81: seq=0 ttl=52 time=10.316 ms
64 bytes from 4.147.153.81: seq=1 ttl=52 time=11.574 ms
64 bytes from 4.147.153.81: seq=2 ttl=52 time=9.981 ms
64 bytes from 4.147.153.81: seq=3 ttl=52 time=10.519 ms
64 bytes from 4.147.153.81: seq=4 ttl=52 time=10.452 ms
64 bytes from 4.147.153.81: seq=5 ttl=52 time=10.140 ms
64 bytes from 4.147.153.81: seq=6 ttl=52 time=10.675 ms
^C
--- 4.147.153.81 ping statistics ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 9.981/10.522/11.574 ms

```

Figure 31: Ping result for Gigabit Ethernet for Wi-Fi connection

- TCP and UDP testing.

```

REMOTE-SERVER@vServer:~$ iperf3 -s
Server listening on 5201 (test #1)

Accepted connection from 110.174.134.130, port 5062
[ 5] local 10.0.0.4 port 5201 connected to 110.174.134.130 port 5063
[ ID] Interval Transfer Bitrate
[ 5] 0.00-1.00 sec 12.4 MBbytes 104 MBits/sec
[ 5] 1.00-2.00 sec 15.0 MBbytes 126 MBits/sec
[ 5] 2.00-3.00 sec 16.0 MBbytes 134 MBits/sec
[ 5] 3.00-4.00 sec 11.9 MBbytes 99.6 MBits/sec
[ 5] 4.00-5.00 sec 11.8 MBbytes 98.6 MBits/sec
[ 5] 5.00-6.00 sec 11.9 MBbytes 99.6 MBits/sec
[ 5] 6.00-7.00 sec 10.9 MBbytes 91.2 MBits/sec
[ 5] 7.00-8.00 sec 11.6 MBbytes 97.5 MBits/sec
[ 5] 8.00-9.00 sec 11.1 MBbytes 93.3 MBits/sec
[ 5] 9.00-10.00 sec 9.38 MBbytes 78.6 MBits/sec
[ 5] 10.00-10.01 sec 128 Kbytes 114 MBits/sec
[ ID] Interval Transfer Bitrate receiver
[ 5] 0.00-10.01 sec 122 MBbytes 102 MBits/sec

Server listening on 5201 (test #2)

Accepted connection from 110.174.134.130, port 5064
[ 5] local 10.0.0.4 port 5201 connected to 110.174.134.130 port 5063
[ ID] Interval Transfer Bitrate Jitter Lost/Total Datagrams
[ 5] 0.00-1.00 sec 1.18 MBbytes 9.90 MBits/sec 0.215 ms 0/1000 (0%)
[ 5] 1.00-2.00 sec 1.18 MBbytes 9.89 MBits/sec 0.298 ms 0/999 (0%)
[ 5] 2.00-3.00 sec 1.20 MBbytes 10.1 MBits/sec 0.359 ms 0/1020 (0%)
[ 5] 3.00-4.00 sec 1.19 MBbytes 10.0 MBits/sec 0.437 ms 0/1010 (0%)
[ 5] 4.00-5.00 sec 1.19 MBbytes 10.0 MBits/sec 0.368 ms 0/1010 (0%)
[ 5] 5.00-6.00 sec 1.19 MBbytes 9.99 MBits/sec 0.355 ms 0/1009 (0%)
[ 5] 6.00-7.00 sec 1.19 MBbytes 10.0 MBits/sec 0.191 ms 0/1010 (0%)
[ 5] 7.00-8.00 sec 1.19 MBbytes 10.0 MBits/sec 0.267 ms 0/1010 (0%)
[ 5] 8.00-9.00 sec 1.19 MBbytes 9.99 MBits/sec 0.386 ms 0/1009 (0%)
[ 5] 9.00-10.00 sec 1.19 MBbytes 9.99 MBits/sec 0.091 ms 0/1010 (0%)
[ 5] 10.00-10.01 sec 13.3 Kbytes 9.21 MBits/sec 0.186 ms 0/11 (0%)

[ ID] Interval Transfer Bitrate Jitter Lost/Total Datagrams
[ 5] 0.00-10.01 sec 11.9 MBbytes 9.99 MBits/sec 0.186 ms 0/10098 (0%) receiver

Server listening on 5201 (test #3)

Accepted connection from 110.174.134.130, port 5065
[ 5] local 10.0.0.4 port 5201 connected to 110.174.134.130 port 5064
[ ID] Interval Transfer Bitrate Jitter Lost/Total Datagrams
[ 5] 0.00-1.00 sec 11.6 MBbytes 97.6 MBits/sec 0.927 ms 6/9865 (0.06%)
[ 5] 1.00-2.00 sec 12.1 MBbytes 101 MBits/sec 0.094 ms 0/10235 (0%)
[ 5] 2.00-3.00 sec 11.9 MBbytes 99.9 MBits/sec 0.103 ms 5/10097 (0.05%)
[ 5] 3.00-4.00 sec 11.9 MBbytes 100 MBits/sec 0.088 ms 0/10099 (0%)
[ 5] 4.00-5.00 sec 11.9 MBbytes 99.9 MBits/sec 0.085 ms 0/10090 (0%)
[ 5] 5.00-6.00 sec 11.9 MBbytes 100 MBits/sec 0.092 ms 0/10097 (0%)
[ 5] 6.00-7.00 sec 11.9 MBbytes 100 MBits/sec 0.108 ms 0/10101 (0%)
[ 5] 7.00-8.00 sec 11.9 MBbytes 99.8 MBits/sec 0.113 ms 8/10088 (0.07%)
[ 5] 8.00-9.00 sec 11.9 MBbytes 99.9 MBits/sec 0.105 ms 9/10101 (0.08%)
[ 5] 9.00-10.00 sec 11.9 MBbytes 99.8 MBits/sec 0.095 ms 2/10074 (0.02%)
[ 5] 10.00-10.01 sec 150 Kbytes 103 MBits/sec 0.155 ms 0/124 (0%)

[ ID] Interval Transfer Bitrate Jitter Lost/Total Datagrams
[ 5] 0.00-10.01 sec 119 MBbytes 99.9 MBits/sec 0.155 ms 30/100971 (0.03%) receiver

Server listening on 5201 (test #4)

[ 5] local 192.168.0.7 port 38130 connected to 4.147.153.81 port 5201
[ ID] Interval Transfer Bitrate Retr Cwnd
[ 5] 0.00-1.00 sec 13.8 MBbytes 115 MBits/sec 1 453 Kbytes
[ 5] 1.00-2.00 sec 15.0 MBbytes 126 MBits/sec 0 475 Kbytes
[ 5] 2.00-3.00 sec 16.0 MBbytes 134 MBits/sec 9 348 Kbytes
[ 5] 3.00-4.00 sec 12.1 MBbytes 102 MBits/sec 4 278 Kbytes
[ 5] 4.00-5.00 sec 11.6 MBbytes 97.5 MBits/sec 7 213 Kbytes
[ 5] 5.00-6.00 sec 12.0 MBbytes 101 MBits/sec 0 245 Kbytes
[ 5] 6.00-7.00 sec 11.0 MBbytes 92.3 MBits/sec 8 203 Kbytes
[ 5] 7.00-8.00 sec 11.1 MBbytes 93.3 MBits/sec 0 236 Kbytes
[ 5] 8.00-9.00 sec 11.4 MBbytes 95.4 MBits/sec 16 149 Kbytes
[ 5] 9.00-10.00 sec 9.12 MBbytes 76.5 MBits/sec 0 179 Kbytes
[ ID] Interval Transfer Bitrate Retr
[ 5] 0.00-10.00 sec 123 MBbytes 103 MBits/sec 45 sender
[ 5] 0.00-10.01 sec 122 MBbytes 102 MBits/sec receiver

iperf Done.
/app# iperf3 -c 4.147.153.81 -u -b 10M -i 1
Connecting to host 4.147.153.81, port 5201
[ 5] local 192.168.0.7 port 36637 connected to 4.147.153.81 port 5201
[ ID] Interval Transfer Bitrate Total Datagrams
[ 5] 0.00-1.00 sec 1.19 MBbytes 10.0 MBits/sec 1011
[ 5] 1.00-2.00 sec 1.19 MBbytes 10.0 MBits/sec 1010
[ 5] 2.00-3.00 sec 1.19 MBbytes 10.0 MBits/sec 1009
[ 5] 3.00-4.00 sec 1.19 MBbytes 10.0 MBits/sec 1010
[ 5] 4.00-5.00 sec 1.19 MBbytes 10.0 MBits/sec 1009
[ 5] 5.00-6.00 sec 1.19 MBbytes 10.0 MBits/sec 1010
[ 5] 6.00-7.00 sec 1.19 MBbytes 10.0 MBits/sec 1010
[ 5] 7.00-8.00 sec 1.19 MBbytes 10.0 MBits/sec 1010
[ 5] 8.00-9.00 sec 1.19 MBbytes 10.0 MBits/sec 1010
[ 5] 9.00-10.00 sec 1.19 MBbytes 9.99 MBits/sec 1009
[ ID] Interval Transfer Bitrate Jitter Lost/Total Datagrams
[ 5] 0.00-10.00 sec 11.9 MBbytes 10.0 MBits/sec 0.000 ms 0/10098 (0%) sender
[ 5] 0.00-10.01 sec 11.9 MBbytes 9.99 MBits/sec 0.186 ms 0/10098 (0%) receiver

iperf Done.
/app# iperf3 -c 4.147.153.81 -u -b 100M -i 1
Connecting to host 4.147.153.81, port 5201
[ 5] local 192.168.0.7 port 50676 connected to 4.147.153.81 port 5201
[ ID] Interval Transfer Bitrate Total Datagrams
[ 5] 0.00-1.00 sec 11.9 MBbytes 100 MBits/sec 10097
[ 5] 1.00-2.00 sec 11.9 MBbytes 100 MBits/sec 10086
[ 5] 2.00-3.00 sec 11.9 MBbytes 100 MBits/sec 10086
[ 5] 3.00-4.00 sec 11.9 MBbytes 100 MBits/sec 10107
[ 5] 4.00-5.00 sec 11.9 MBbytes 100 MBits/sec 10088
[ 5] 5.00-6.00 sec 11.9 MBbytes 100 MBits/sec 10097
[ 5] 6.00-7.00 sec 11.9 MBbytes 100 MBits/sec 10050
[ 5] 7.00-8.00 sec 11.9 MBbytes 100 MBits/sec 10104
[ 5] 8.00-9.00 sec 11.9 MBbytes 100 MBits/sec 10096
[ 5] 9.00-10.00 sec 11.9 MBbytes 100 MBits/sec 10089
[ ID] Interval Transfer Bitrate Jitter Lost/Total Datagrams
[ 5] 0.00-10.00 sec 119 MBbytes 100 MBits/sec 0.000 ms 0/100971 (0%) sender
[ 5] 0.00-10.01 sec 119 MBbytes 99.9 MBits/sec 0.155 ms 30/100971 (0.03%) receiver

iperf Done.
/app#
CTRL-A Z for help 9600 B8N1 NOR Minicom 2.9 VT102 Offline ttyUSB0
```

Figure 32: TCP & UDP result for Gigabit Ethernet for Wi-Fi connection

Future Works

The results demonstrate that the initial solution shown in Figure 1 was validated, indicating that a reliable network connection can be achieved using 5G Cellular and Fast Wi-Fi roaming. Therefore, this milestone will be used for further development to maximise network reliability and security in order to meet our industrial partner's sustainable plan. Some of the further developments are listed as follows:

- Implement an end-to-end tunnel for both interfaces from the end device IR1835 to the server by utilising Cat8k.
 - Deploying SD-WAN for centralised control and maximising security.
 - Deploying private 5G to secure and isolate the network system from public services.
 - Test the set-up in the actual environment for real-life data connection, utilising the OBD2 cable in Figure 9 in the actual vehicle.
 - Providing a platform for further studies with critical infrastructure research and potential automation process.

3.4 Alignment with Organisation Goals and Impact

This internship project has offered a validation process that an industrial partner could potentially adopt to shape their business approach in the future, which I believe this project's outcome can lead to.

- Transitioning process to zero-emission business operation for the next 25 years.
- Automation process to decrease fuel consumption by employing reliable network models with high-speed connections in a critical infrastructure environment.
- Private operation networks and enhancing network resilience.

In this program, my contribution was directly involved in helping with the following mission:

- Verifying that dual connectivity using Cellular 5G and fast Wi-Fi roaming is achievable.
- Providing an initial process that can strengthen network security to be aligned with the compliance of SOCI (Security of Critical Infrastructure).
- Creating a network foundation for further studies in digital twin implementation.

In conclusion, this validation process is crucial to establishing a scalable pathway for network upgrades that aligns with their primary objective of transforming into sustainable business operations.

4 Appendix

Appendix A: Activity Journal and Time-sheet

Below is a weekly summary report for the 6 weeks of working hours, totalling approximately 120 hours, as per the requirements.

Week 1

Weekly Summary Report	
Date	
1/4/2025 – 3/4/2025	Tota hours: 11.50 Hours
Overview	
This week, I participated in the internal kick-off meeting with the industry partner, which provided valuable insights into the project objectives. I also conducted initial research on both routers, the IR1835 and IW9165, to build an understanding of their capabilities. In particular, I outlined the key features of the IR1835, which will support its role in our network setup and guide the next stages of the project.	
Communication Log	
1/4/2025	Introduction to industrial stakeholder, brief overview of the project, brief overview of the system approach intended to meet the requirement for the client.
Challenges Faced	
Minimum resource of the hardware manuals	
Next Steps	
<ul style="list-style-type: none">- Provide the literature of each device- Understand the functionalities- Exploring the system architecture of each device	

Week 2

Weekly Summary Report	
Date	
7/4/2025 – 10/4/2025	Tota hours: 21.30 Hours
Overview	
This week, I focused on a literature review of the IR1835 rugged series router to better understand its features and functionality and presented an evaluation of the progress so far. I also examined the key functionalities of the IW9165, contributed to the ICC photoshoot, and carried out initial research related to hardware delivery.	
Communication Log	
8/4/2025	Presenting my findings on the industrial router IR1835 and evaluating some of the features that will be used in the project so far.
Challenges Faced	
Due to limited resources, the configuration and hardware installation were based on assumptions.	
Next Steps	
<ul style="list-style-type: none">- Identify steps that need to take to ensemble the hardware- What type of power resource that is required- How the whole devices can be connected into the network	

Week 3

Weekly Summary Report	
Date	
14/4/2025 – 18/4/2025	Tota hours: 21.50 Hours
Overview	
<p>This week, I analysed key components from the order list and reviewed their functionality using manuals and documentation from the Cisco official site. The findings were compiled into a presentable table for the literature review section, with additional details on functionality and sources included for reference. I also reviewed feedback from the literature review, initiated Sprint 3 planning, and attended the IPTel/ICC project kick-off meeting.</p>	
Communication Log	
15/4/2025	In this meeting, I updated some of the possibilities for the power source of the router. The router IR1835 offers two options for power supply: via PoE and a power adapter. I also raise the concern regarding the common ground point in the location where the set-up is deployed.
Challenges Faced	
<ul style="list-style-type: none"> - The common ground point cannot be located in the lab. - Potentially use the power adapter as the power source, where data cannot be in real time but is simulated since the power adapter and the data extraction cable (OBD2 cable) share the same port. OBD2 is often used in vehicles, with it is employed as both a CAN BUS extractor and power source simultaneously. 	
Next Steps	
<ul style="list-style-type: none"> - Identify the OBD2 is require a adapter converter from OBD2 to USB. - Use the power cable as the power source 	

Week 4

Weekly Summary Report	
Date	
21/4/2025 – 25/4/2025	Tota hours: 24 Hours
Overview	
<p>This week, I investigated the software requirements for both routers and continued to build an understanding of the IOS XE operating system and its key functionalities. I also reviewed the software architecture in more detail, aligned it with the overall project requirements, and extended research in this area. In addition, I identified additional hardware items that need to be ordered.</p>	
Communication Log	

22/4/2025	In this meeting, I updated that the router is can only be powered through the power updater. I also suggested using an OBD2–USB CAN BUS adapter scanner to bridge the connection directly from the laptop to the route via the OBD2 cable.
Challenges Faced	
<ul style="list-style-type: none"> - The OBD2 cannot be a power source if it directly connects to the laptop - The OBD2 may require a full reconstruction to separate the power and earth pins from the pin that generates sensors. - This approach it is not suitable due to time constraints 	
Next Steps	
<ul style="list-style-type: none"> - Identify the OBD2 is require an adapter converter from OBD2 to USB. - Use the power cable as the power source. - Conduct a review of the architecture review of IOS XE IR1835 router. 	

Week 5

Weekly Summary Report	
Date	
28/4/2025 – 2/5/2025 Total hours: 11 Hours	
Overview	
<p>This week, I reviewed progress on the Cisco IOS XE router operating system and ensured all relevant aspects of the software architecture were addressed. I attended the Project progress update meeting, updated the Kanban board, and participated in the IPTel/ICC project progress session. On the hardware side, I checked 5G and 4G LTE coverage in Lab 6B42, updated the timesheet for recorded hours, moved hardware from the ICC office to the lab, and unboxed all delivered equipment to confirm that components matched the order list. Initial installation steps were also started, and the project board was updated during meetings to define the next actions.</p>	
Communication Log	
29/4/2025	<p>In this meeting, I showcase the IOS XE system architecture and ensure it covers all necessary aspects involved in the project. We also discuss the Wi-Fi access point that will be used, as the lab environment where the deployment takes place has already been equipped with a Netgear access point.</p> <p>We also decide to proceed with the power adapter as the power source and generate data from the laptop for the data source.</p>
Challenges Faced	
<ul style="list-style-type: none"> - The NETGEAR AP in the lab cannot be accessed by other user other than the lab manager - There are specification on the OBD2 – USB adapter scanner 	
Next Steps	

- Confirm that the only cellular coverage around the lab environment is only 4G with the Vodafone provider.
- Utilising other cellular provider such Telstra to indicate if there is 5G coverage around the lab environment.

Week 6

Weekly Summary Report	
Date	
5/5/2025 – 9/5/2025	Tota hours: 31.50 Hours
Overview	
<p>This week, I focused on configuring the Cisco IW9165E by attempting to connect it to Wi-Fi and reviewing the IW9165E configuration guide. I attended a project meeting on Monday (05/05/2025, 2:30 PM – 4:30 PM), which included clarifications on CAN Bus integration. Work was also carried out on designing the system architecture to connect data sources across the IR1835-K9, IW9165E, private network, and dummy server.</p> <p>Additionally, I identified the types of CAN Bus data that could potentially be extracted and considered whether an additional switch may be required alongside the IW9165E wireless client and access point. Security measures were also reviewed to ensure data confidentiality, integrity, and availability throughout the system. Measurement tripods were also included in planning for data collection setup.</p>	
Communication Log	
6/5/2025	<p>In this meeting, I confirmed that I was able to provide another NETGEAR AP in similar spec with our lab AP. I can confirm that this AP will provide Wi-Fi signal that will be connected to IW9165</p> <p>Provide progress in IW9165 Cisco manual in which I use as guidance for the installation.</p> <p>Confirming that the signal coverage around the lab is also able to pick up 5G.</p>
Challenges Faced	
<ul style="list-style-type: none"> - The Cisco manual for IW9165 indicating that there are two modes in which the AP need to operate, WGB (work group bridge and uWGB (universal workgroup bridge) - The bridge AP is only able to operate in uWGB mode in which works only with a non-cisco access point 	
Next Steps	
<ul style="list-style-type: none"> - Confirm the connection IW9165 with the NETGEAR AP - Identify what type of Cisco devices are deployed whether actual client deployment sites, confirming that if there are also third-party devices or only Cisco-designated hardware 	

Appendix B: Signed Internship Evaluation Report



DISTINCTIVE BY DESIGN

INTERNSHIP EVALUATION REPORT

Employer name: Innovation Central Canberra

Supervisor's Name: Ella Swift

Contact E-mail: ella.swift@canberra.edu.au

Student name & ID: Sandhy Waer & u3165828

Contact E-mail: Sandhy.Waer@canberra.edu.au & u3165828@uni.canberra.edu.au

Unit and convenor 12091 & 7900 and Nishant Jagannath

Internship period:	01 / 04 /2025	to	25 / 07 / 2025	Hours completed: 450 Hours	
--------------------	---------------	----	----------------	----------------------------	--

FEEDBACK ON STUDENT

- What tasks did the intern do best, and what did they struggle with?

Fantastic written and verbal communication with various stakeholders and peers. Technical excellence and ability to follow and digest technical documentation

- Did the intern have/gain sufficient knowledge to complete projects and assignments given to him/her?

Yes, navigated technical tasks individually and collaboratively within expected timeframes and regularly provided transparency and updates regarding his progress

- Did you think the intern improved or learned throughout the placement term? If yes, in what areas?
If not, why do you think there was no improvement?

Communication of complex technical topics to a range of audiences. Practical application of theoretical knowledge and concepts. Quick learner.

- Did you have any issues with the intern? If so, what were they, and are they resolved?

- What were the intern's most outstanding characteristics?

- Proactive (often saw pathways to get things done and navigated them without awaiting confirmation)
- Problem solving capabilities & strategies
- Driven and highly motivated
- Eagerness to learn and grow

6. What areas do you think the intern still needs to address?

Continue refining critical thinking and problem-solving capabilities.

7. How would you evaluate the intern on the following?

	Poor	Below average	Average	Above average	Excellent	Comments
<i>Motivation/initiative</i>	1	2	3	4	5	
<i>Dependability</i>	1	2	3	4	5	
<i>Interpersonal skills</i>	1	2	3	4	5	
<i>Teamwork</i>	1	2	3	4	5	
<i>Task performance:</i>						
<i>Professionalism</i>	1	2	3	4	5	
<i>Strategic thinking</i>	1	2	3	4	5	
<i>Critical thinking</i>	1	2	3	4	5	
<i>Organisation</i>	1	2	3	4	5	
<i>Planning</i>	1	2	3	4	5	
<i>Creativity</i>	1	2	3	4	5	

FEEDBACK ON INTERNSHIP PROGRAM

8. Do you think the internship was mutually beneficial (you and intern)? Yes No

Comments:

9. Do you have any ideas or suggestions for how the internship program could be improved?

Supervisor name

Student name

Ella Swift

Sandhy Waer

Supervisor signature

Student signature



Date 25/7/25

Date 25/07/2025

Thank you for participating in the University of Canberra's Internship Program.

Attention students: Please attach this evaluation to your Final Report