



ECI Proposal 2023

Network Design Implementation

PREPARED FOR:

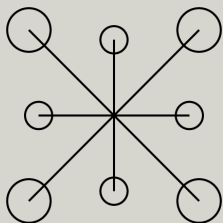
Energy Connections Inc.

CREATED BY:

Hung Chanh Huynh, Adrian Morris Han

Sol Jin, Stefan Htoo Aung Khant

Maegan Hermosa, Daniel Brown



This formal report documents a network solution, produced by J4 Incorporation, with office at 1414 Burnaby, BCV3W 2J4. This solution was created and designed from May 12, 2023 to May 24, 2023 for Energy Connection Inc. campuses in Vancouver, Calgary, Montreal, and Toronto Canada.

Proposal Report [2023]

1. Executive Summary

1.1 Introduction

1.2 Previous Work

1.3 Summary of RPF

2. Proposed Solution

2.1 Hardware

2.2 Network Implementation

2.3 Security

2.4 Linux

2.5 Windows

3. Proof of Concept

3.1 Network Functionality

3.2 Challenges

3.3 Troubleshooting & Solutions

3.4 Time Frame

4. Summary Statement

1. Executive Summary

1.1 Introduction

Dear Directors of Energy Connection Incorporation,

In regard to your Request for Proposal, J4 is thrilled to bid our network design that we believe will enhance the network environment of ECI. We understand your need for an optimized network to improve security, business performance, and efficiency. Our network infrastructure has been designed for all specifications discussed within the request for proposal. At J4, we pride ourselves in meeting all specifications to comply with your company needs. Our team is committed in providing quality network solutions for customer satisfaction. With this in mind, we intend to provide:

- a. A high-availability network with redundancy and failover services for hosts.
- b. Centrally logged Cisco equipment output and synchronized time on network devices.
- c. Security features for maximum security against network attacks.
- d. Linux servers with incremental backup and Cisco router and switch services.
- e. Active Directory domain structure that centralizes all users and computers for network management.

allow us to help you achieve your goals and establish a top quality network infrastructure. We would to thank you for your time and consideration of our proposal.

Sincerely,
J4 Inc.

Skill Requirements	Hardware & Software
<ul style="list-style-type: none">◦ Experience configuring Cisco networking devices.◦ Configuring access control lists	Cisco Catalyst 2960-X Series Switch Cisco Integrated Services Router 4321 Cat6 Shielded Ethernet Cables

- Implementing Layer 2 security features
- Creating a web server
- Performing security assessments

4 Workstations
Hyper-V
Packet Tracer

1.2 Previous Work

Experience:

Our team at J4 ensures that we work closely with all clients to precisely design a network infrastructure. We pride ourselves in providing cohesive network solutions to deliver customer satisfaction.

- | | |
|---|---|
| 1. Conducted risk assessment to scan for vulnerabilities in a network. Applied effective security policies for securing the network. | 4. Deployed and configured firewalls to specify access using IP address structuring, access control lists, firewall services and logging. |
| 2. Connected networking devices such as routers, switches, cables, and PCs to establish a structured LAN. | 5. Managed Group Policies on windows server to apply necessary access control to the network. |
| 3. Configured switches with advanced functionality including Spanning-Tree Protocol (STP), Dynamic Host Configuration Protocol (DHCP), and port-security. | 6. Implemented Active Directory services for structured and organized data management. |
| | 7. Installed and configured Apache web server for internet users to obtain files on web site pages. |

With these previous experiences, we are confident in producing and implementing our project. Throughout our previous achievements, we have attained all skills required to provide service that is more than adequate.

1.3 Summary of RPF

Our previous projects and experience have allowed us to gain knowledge and expertise. As a result, our clients have improved network performance for business efficiency. You can rely on our team to provide detailed design, implementation, and management to maintain a secure network.





2. Proposed Solution



1. All required hardware is specified below, along with the steps taken by each team member to create, configure, and managed our proposed network design. 2
2. Our team J4, has divided our solution into 4 categories that members specialize in; enterprise LAN implementation, Linux, Security, and Windows.
3. Upon successful setup, our network solution will



2.1 Hardware

The following table displays all hardware required to set up the network along with specifications of each device.

Hardware	Description	Image
Cisco Catalyst 2960-X Series Switches	<ul style="list-style-type: none">▪ 128 MB Flash Memory▪ Enterprise-level and stackable for campus network environment▪ Forwarding bandwidth: 108 Gbps▪ Switching bandwidth: 216 Gbps	 <p>Figure 2.1.1 - Cisco 2960-X Switch</p>
Cisco Integrated Services Router 4321	<ul style="list-style-type: none">▪ 4 GB Flash Memory▪ Offers network resiliency and connection options that allow load-balancing▪ Built-in network capabilities and convergence.	 <p>Figure 2.1.2 - Cisco ISR 4321 Router</p>

Hardware	Description	Image
Cat6 Shielded Ethernet Cables	<ul style="list-style-type: none"> ▪ High speed data transmission ethernet cables. ▪ Shielding ensures data is protected from outside interference such as EMI (Electromagnetic Interference). 	 <p data-bbox="1149 678 1424 707">Figure 2.1.3 - Cat6 Cable</p>
4 Workstations	<ul style="list-style-type: none"> ▪ Dell Precision 3000 3640 workstation ▪ Intel Core i7 2.90Gz ▪ 32GB RAM ▪ 512GB SSD 	 <p data-bbox="1156 1018 1417 1047">Figure 2.1.4 - Dell i5 PC</p>

2.2 Network Implementation

The fundamental of our solution is our network that is comprised of the access, distribution, and core layer. With the use of Cisco routers and switches, we have chosen to implement advanced protocols.

The following table lists protocols that have implemented on the Cisco networking devices in order to protect the network against man-in-the-middle attacks and to control how traffic is transmitted and received within the network:

Feature	Function
HSRP	HSRP avoids administrative and processing overhead and security issues so that there are failover services for the following hosts.
DHCP	<p>Snooping enabled on every VLAN and every switch so that inbound traffic. This determines which traffic is trusted or untrusted.</p> <p>Network security is attained by ensuring that traffic that is untrusted is dropped by layer 2 security technology.</p>
OSPFv2	Used for the distribution of routing information throughout the network.
STP Attack	All ports that are connected to end devices have PortFast BPDU enabled so that loops are prevented. BPDUs will not be received on PortFast-enabled switch ports to avoid potential spanning tree loops.
Port Security	<ol style="list-style-type: none">1. To block unwanted traffic from attempting to access ports, the allocated maximum number of ports is set to 1 so that any devices that attempt to access the network.2. Once a security violation has occurred the ports have been configured to enter shutdown mode.3. For the ports to retain MAC address information, switches with a sticky mac address enabled then dynamically learn and save MAC addresses.

Feature	Function
ARP Inspection	Protects the network against Address Resolution Protocol (ARP) spoofing attacks by validating the ARP packets once received.

Dynamic Routing Protocols -

Our network uses Open Shortest Path First (OSPF)

2.3 Security

Nessus Scanning -

To ensure that all security measure are to proper standard we used Nessus Vulnerability Scanner to evaluate the security of the network. We've performed penetration testing on the network the ensure that it is safe from malicious attacks. The examination of ports is done so that hackers can't exploit these ports and launch attacks that can be damaging to the network. This scan displays vulnerabilities that were found throughout the network and with these results we then applied the corresponding solutions.

The first scan this procedure is launching a host discovery that displays full qualified domain name (FQDN), along with other details such as IP address and open ports. Upon discovery of the network, we then proceeded with the vulnerability scan.



The following table displays the results found after the whole network has been scanned.

Vulnerability	Description	Solution
1. Critical - Telnet Vulnerability Affecting Cisco Products	The Cisco IOS Xe Software is compromised if the feature of persistent Telnet is enabled.	Cisco bug ID CSCvu66723 Persistent Telnet feature should be disabled.
2. Critical - Cisco IOS XE Software NETCONF RESTCONF	A bypass vulnerability makes the authentication process weak because it could allow attackers to bypass Cisco IOS Xe Software. <ul style="list-style-type: none"> Attackers could bypass authentication such NETCONF and RESCONF 	Cisco bug ID CSCvt53563 Upgrade the version of this ID

2.4 Linux

The Linux server that are within the network infrastructure are reinforced with numerous python scripts for purposes such as automation, backup scripts, and fallback. This scripts make it so that administrative tasks are issued automatically.

The scripts that have been written include:

- Cisco SSH Automation
- DHCP Backup Automation
-

Rsync stands for remote sync and it is a tool mostly used for Linux systems to synchronize files across remote and local networks.

A python script has been written to perform the incremental backups in order to back up the data that has been changed to the disk space.

For all files to be managed and synchronized through the network, a utility called is used.

2.5 Windows

IT Security Group has been configured with specific group policies to ensure maximum security.

1. Unless the loss

3. Proof of Concept

3.1 Network Functionality

1.

3.2 Challenges

Date	Challenges and Solutions
May 15, 2023	<p>Networking - The initial challenge of the project was designing the network topology that catered to all protocols that needed to be implemented to meet requirements</p> <p>Solution: This process involved the re-arranging of network devices and comparing various network designs that equipped the scenario.</p>
May 16, 2023	<p>Windows - Failed login attempts once policy was applied for remote users,</p> <p>Solution: Manage the policies so that the users are not affected by the security policies and have login access.</p>
May 17, 2023	<p>Networking - The network topology was changed based on feedback. Campuses needed to vary in size.</p> <p>Solution: Re-arrange networking devices so that campus 1 is the larger campus out of the 2.</p> <p>Linux - Additional python scripts were written for Linux, but have not been tested yet, due to waiting on network section to be set up for testing.</p> <p>Solution: Test python scripts once network is set up and running.</p>
May 18, 2023	<p>Networking – DHCP snooping is not working on hardware</p> <p>Solution: missing command line found in Network Security lecture slides (Security Assessment Pt. 2 near the end) * Find the exact command that was missing.</p>

Date	Challenges and Solutions
May 19, 2023	<p>Linux – Python script for Cisco backup is not working.</p> <p>Solution: *Might need to do backup on router as appose to writing a python script for it</p> <p>Networking – OSPF is currently no working, which is delaying Linux and Security testing.</p> <p>Solution: Troubleshoot OSPF, so that other section can proceed with testing network connectivity. Static NAT was removed from R1 to fix this issue.</p>
May 23, 2023	<p>Windows – Unable to get IPs for PC due to DHCP, problem with NTP</p> <p>Solution:</p>
May 24, 2023	<p>Networking –</p>

3.3 Troubleshooting & Solutions

3.4 Time Frame

4. Summary Statement

We appreciate and look forward to working with Energy Connections Inc. and we hope to work together to establish our proposed network infrastructure.

05 / 24 / 2023