DPTech ÉLECTRONIQUES Inc.
61 Irving Boul.
Bouctouche, NB E4S 3J6
(506) 743-5577
sales@dptech.ca

QUOTE

Quote No.: 1140
Date: Apr 15, 2025

Quoted To:
Five Rivers - 5065236921

QUOTE ONLY - DO NOT PAY!

Business No.: 84320 2201 RT0001

Item No.	Quantity	Description	Tax	Unit Price	Amount
840030703300	1	TP-Link OMADA ER8411 VPN Router with 10G Ports	H	999.99	999.99
845973088682	1	TP-Link OMADA SG2428P 28-Port Switch with 24 PoE+	H	499.99	499.99
840030704307	2	TP-Link OMADA EAP613 Access Point	H	199.99	399.98
845973089863	1	TP-Link OMADA OC300 Hardware Controller	H	249.99	249.99
CAT6	50	Cat6 Ethernet Cable - $0.50/ft	H	0.50	25.00
888620040831	2	Cat6 RJ45 Keystone Jack	H	9.99	19.98
EZCAT6	2	EZ Cat6 RJ45 Male Connector	H	2.50	5.00
Service Call (Hours)	15	On-Site Service @ $120/hr (Minimum 1 Hour) - Program network equipment offsite - Install programmed equipment onsite - Run and terminate 2 data drops for Access Points - Install 2 Access points to ceiling	H	120.00	1,800.00
		Subtotal:			3,999.93
		H - HST 15% HST			600.00

Comments	Total	4,599.93

From:	DPTech Electroniques
To:	Five Rivers
Subject:	Municipal Network Security & Infrastructure Upgrade
Date:	March 24, 2026 11:23:49 AM

Proposal: Municipal Network Security & Infrastructure Upgrade

Prepared By: DPTech

Project Quote: #1140

Date: April 15, 2025

Executive Summary

The current network infrastructure at the municipality relies on a basic internet provider modem with no dedicated security layer. This proposal outlines the transition to a professional-grade "managed" network. This upgrade is designed to protect municipal data, meet the security standards held by all neighboring municipalities, and resolve ongoing Wi-Fi connectivity issues within the building.

1. Why a Dedicated Firewall is Required

A firewall is the most critical piece of equipment for any government office. Currently, our "front door" to the internet is effectively unlocked.

- Cyber-Threat Prevention: The TP-Link Omada VPN Router acts as a digital security guard, inspecting every piece of data entering or leaving the building to block hackers and malicious software before they reach staff computers.
- Regional Standards: All other municipalities currently supported in this area have already moved to this dedicated firewall standard. This upgrade ensures we are not the only unprotected "weak link" in the regional network.
- Liability and Privacy: A firewall ensures that sensitive municipal files remain private and are not accessible via the public or guest Wi-Fi signals.

2. Solving Wi-Fi "Dead Zones" and Interference

The current system relies on a single access point that does not cover the entire building and suffers from signal interference.

- Total Coverage: We are moving from one single point of failure to a system of two High-Performance EAP613 Access Points. These will be professionally mounted to the ceiling to provide a strong, seamless signal in every office.
- Interference Management: The OC300 Hardware Controller acts as the "brain" of the Wi-Fi, automatically adjusting signals to prevent the interference and "dropped calls" currently experienced by staff.

3. Professional Implementation

This is not a "plug-and-play" consumer setup. It is a business-grade system that requires expert configuration.

- Offsite Programming: Equipment is pre-configured at our lab to ensure security protocols are active before the hardware even enters your building.
- Onsite Installation: The quote includes 15 hours of professional labor to run new Cat6 data lines, terminate connections, and physically mount hardware for a clean, permanent installation.

FAQ:

1. "We already have a modem from our internet provider. Why do we need a $1,000 router?"

- The Difference: A provider's modem is a basic "gateway" designed for home use; it does not have the processing power to manage a secure government office.
- Professional Security: The ER8411 VPN Router is a high-capacity "firewall" that actively filters out cyber-threats and hackers before they reach our internal computers.
- Performance: This hardware can handle high-speed data for all staff members simultaneously without the "freezing" or slowing down common with basic modems.

2. "Why can't we just buy a cheaper Wi-Fi booster from a big-box store?"

- The Coverage Gap: Boosters often "repeat" a weak signal, which leads to slow speeds and dropped connections.
- The Solution: This quote uses EAP613 Access Points that are physically wired into the building's infrastructure. This provides a "fresh" signal in every corner of the building rather than a recycled, weak one.
- Centralized Management: These units are managed by a dedicated controller

(OC300), which ensures staff can move from room to room without ever losing their connection.

3. "Is this really a standard for small municipalities?"

- Industry Standard: Yes. Every other municipality we currently support in this region has already moved to a dedicated firewall and managed Wi-Fi system.
- Security Risk: Without this, we are the only local government office in the area operating without a dedicated security layer, making us a primary target for data breaches.

4. "Why is there 15 hours of labor on the quote?"

- Custom Configuration: We don't just "plug it in." The equipment is programmed offsite to meet specific security and privacy protocols before installation.
- Physical Infrastructure: The labor includes running 50 feet of professional-grade Cat6 cabling and installing permanent "data drops" in the walls and ceilings.
- Turnkey Setup: This ensures that once we leave, the system is fully tested, secure, and requires zero daily maintenance from municipal staff.

5. "What happens if we don't do this upgrade?"

- Ongoing Issues: The current interference and "dead zones" in our Wi-Fi will continue to hinder staff productivity.
- Security Liability: If a data breach occurs, the municipality would have to explain why it didn't implement the same basic firewall protections used by all neighboring communities.

6. "REVISED SECTION: The "Layered Safety" Approach"

A common question from staff is: *"If we already have Avast Business Antivirus on our computers, why do we need a dedicated firewall?"* The answer lies in Layered Security. Think of the municipality's safety like a vehicle:

- The Antivirus (The Airbag): Your antivirus is like an airbag inside the car. It is the last line of defense. If something managed to get inside your computer, the antivirus tries to stop the damage from the inside.
- The Firewall (The Seatbelt): The firewall is like your seatbelt. It is your first line of defense. It holds the "threat" back and prevents you from being thrown into a dangerous situation in the first place.

The Reality of Risk:

Just like in a car, having a seatbelt doesn't mean it’s impossible to get hurt, but it significantly reduces the probability and the severity of the injury. Relying on antivirus alone is like driving with an airbag but no seatbelt—you are technically "protected," but you are taking a much higher risk of total failure.

Thanks
Steven Richard
DPTech