

City of Coquitlam

Request for Proposals

RFP No. 21-070

Local Area Network (LAN) /  
Metropolitan Area Network (MAN)  
Replacement

**TABLE OF CONTENTS**

**DEFINITIONS .....4**

**1 INSTRUCTIONS TO PROPONENTS .....5**

1.1 Purpose..... 5

1.2 Proposal Submission ..... 5

1.3 Instructions to Proponents..... 5

1.4 Specifications and Alternatives..... 5

1.5 Requested Departures ..... 5

1.6 Evaluation Criteria ..... 5

1.7 Eligibility..... 7

1.8 Project Timeline ..... 7

1.9 Warranties..... 7

1.10 Sub-Consultants ..... 8

1.11 Examination of Proposal Documents..... 8

**2 GENERAL CONDITIONS OF CONTRACT .....9**

2.1 Terms and Conditions of Contract..... 9

2.2 Advertisement..... 9

**3 SCOPE OF SERVICES ..... 10**

3.1 General Requirements..... 10

3.2 Technical Environment..... 10

3.3 Equipment Design Document ..... 10

3.4 Scope of Services ..... 10

3.5 Security and Confidentiality ..... 11

3.6 Qualified Personnel ..... 11

3.7 Quality Assurance ..... 11

3.8 Warranties..... 11

3.9 Recall Notices ..... 12

3.10 Delivery, Storage, and Handling ..... 12

3.11 Site Control and Organization..... 12

3.12 Rejected Work ..... 12

3.13 Hours of Work ..... 12

3.14 Clean Up..... 12

[Appendix A – Technical Requirements](#)

[Appendix B – Non Disclosure Agreement](#)

[PROPOSAL SUBMISSION FORM](#)

**SUMMARY OF KEY INFORMATION**

<b>RFP Reference</b>	<b>RFP No. 21-070</b> <b>Local Area Network (LAN) / Metropolitan Area Network (MAN) Replacement</b>
<b>Overview of the Opportunity</b>	The purpose of this RFP is to invite Proposals from professional, qualified, experienced companies for the provision of <b>Local Area Network (LAN) / Metropolitan Area Network (MAN) Replacement</b> .
<b>Closing Date and Time</b>	<b>2:00 pm local time</b> <b>Wednesday, October 13, 2021</b>
<b>Instructions for Proposal Submission</b>	Proposals are to be consolidated into one PDF file and uploaded electronically through QFile, the City's file transfer service accessed at <a href="http://qfile.coquitlam.ca/bid">qfile.coquitlam.ca/bid</a> <b>1. In the "Subject Field" enter:</b> RFP Number and Name <b>2. Add files in .pdf format and Send</b> (Ensure your web browser remains open until you receive 2 emails from QFile to confirm receipt.)  Phone 604-927-3037 should assistance be required.  The City reserves the right to accept Proposals received after the Closing Date and Time.
<b>Obtaining RFP Documents</b>	RFP Documents are available for download from the City of Coquitlam's website: <a href="https://www.coquitlam.ca/Bid-Opportunities">https://www.coquitlam.ca/Bid-Opportunities</a>  Printing of RFP documents is the sole responsibility of the Proponents.
<b>Instructions to Proponents</b>	The guidelines for participation that will apply to this RFP are posted on the City's website: <a href="#">Instructions to Proponents</a>
<b>Questions</b>	Questions are to be submitted in writing quoting the RFP number and name up to 3 business days before the Closing Date sent to email: <a href="mailto:bid@coquitlam.ca">bid@coquitlam.ca</a>
<b>Addenda</b>	Proponents are required to check the City's website for any updated information and addenda issued, before the Closing Date at the following website: <a href="https://www.coquitlam.ca/Bid-Opportunities">https://www.coquitlam.ca/Bid-Opportunities</a>
<b>Withdrawal of Submission</b>	Proposals may be withdrawn by written notice only, made by an authorized representative of the Proponent sent to email: <a href="mailto:bid@coquitlam.ca">bid@coquitlam.ca</a> prior to the Closing Date and Time.
<b>Terms and Conditions of Contract</b>	City of Coquitlam <a href="#">Standard Terms and Conditions - Purchase of Goods and Services</a> are posted on the City's website and will apply to the Contract awarded as a result of this RFP.

## DEFINITIONS

**“Agreement” “Contract”** means the contract for services or City Purchase Order that will be issued to formalize with the successful Proponent through negotiation process with the City based on the proposal submitted and will incorporate by reference the Request for Proposals, Specifications, Drawings, any additional subsequent information, any addenda issued, the Proponent’s response and acceptance by the City.

**“Contractor”** means the person(s) firm(s) or corporation(s) appointed by the City to carry out all duties, obligations, work and services described in the Request for Proposal and all associated documentation, which may also include mutually agreed revisions subsequent to submission of a Proposal. Both “Contractor” and “Proponent” are complementary in terms of duties, obligations and responsibilities contemplated at the Request for Proposals stage, through evaluation process, execution and performance of the services and works.

**“City” “Owner”** means City of Coquitlam;

**“LAN”** Local Area Network

**“MAN”** Metropolitan Area Network

**“Manufacturer”** means refers to the company that manufactures the components and equipment backed by a warranty against defects. They also provide recommendations on the proper application and installation methodology of their products;

**“Price”** means the amount that will be paid by the City to the Contractor for delivery and acceptance of goods and Services;

**“Proponent”** means responder to this Request for Proposals;

**“Proposal”** means the submission by the Proponent;

**“Request for Proposals” “RFP”** shall mean and include the complete set of documents, specifications and addenda incorporated herein, and included in this Request for Proposals;

**“Services” “Work” “Works”** means and includes the provision by the successful Proponent of all services, duties, and expectations as further described in this RFP. This will also mean the whole of the work, tools, materials, labour, equipment, travel, and all that is required to be done, furnished and performed by the Contractor;

**“Shall” “Must” “Will” “Mandatory”** means a requirement that must be met;

**“Supply” “Provide”** shall mean supply and pay for and provide and pay for.

## 1 INSTRUCTIONS TO PROPONENTS

### 1.1 Purpose

The City requests proposals from qualified, experienced companies to provide labour, equipment, materials, fuel, transportation, overhead and all that is necessary for the provision of Local Area Network (LAN) / Metropolitan Area Network (MAN) Replacement (the 'Services') as outlined in **Section 3 – Scope of Services**.

### 1.2 Proposal Submission

Proponents should complete and submit the information requested in this RFP document on the Proposal Submission Form or in a format that has been approved and is acceptable to the City.

### 1.3 Instructions to Proponents

Proponents are advised that the rules for participation that will apply to this RFP are located: [Instructions to Proponents](#).

By submission of a Proposal in response to this RFP, the Proponent agrees and accepts the rules by which the bid process will be conducted.

### 1.4 Specifications and Alternatives

Wherever the Specifications state a brand name, make, name of manufacturer, trade name, or Supplier catalogue number, it is for the purpose of establishing a grade or standard. It is not intended to rule out competition from equal brands or makes. If equipment other than that specified is offered, it is the Proponent's responsibility to provide information in its Proposal that enables the City to confirm equivalency and acceptance.

Except where stated otherwise, **Appendix A – Technical Requirements** describe what is considered necessary to meet the performance requirements of the City and Proponents should consider this in its Proposal. If the Proponent cannot meet Specifications, the Proponent may identify and offer an alternative which it believes to be an equal or better alternative.

Special consideration may be given to accessibility of the various units which require periodic maintenance and ease of operation.

Proponents shall clearly indicate any variances from the City's Specifications or conditions and attach descriptive literature.

The City will review proposed alternative equipment for suitability; however, the City is not obligated to accept any alternatives. The City will determine what constitutes acceptable deviations and overall best value.

### 1.5 Requested Departures

The Proponent acknowledges that the departures requested in the Proposal Submission Form will not form part of the Contract unless and until the City specifically consents in writing to any of them. The City will evaluate those departures as per Evaluation Criteria.

### 1.6 Evaluation Criteria

Evaluation Criteria of each proposal will be determined in accordance with the following:

Proposal Evaluation Summary	Maximum Points to be Awarded
<a href="#">Corporate Experience, Reputation, Capacity and Resources</a>	25
<a href="#">Technical</a>	55
<a href="#">Financial and Value Added</a>	20
Total	100

The criteria for evaluation of the Proposals may include, but is not limited to:

**Corporate Experience, Reputation, Capacity and Resources**

- Proponent’s qualifications, experience, and demonstrated performance providing services of similar size, scope and complexity
- Established local business presence
- Sub-contractors
- Key Personnel on project team, qualifications and experience

**Technical**

- Approach and Methodology
- Test and Acceptance Plan
- Compliance with the preferred specifications
- Delivery Lead Time
- Warranties
- Installation and Training
- Challenges, Risks and Opportunities
- Departures listed

**Financial and Value Added**

- Total Price
- Value Added / Sustainable benefits

These criteria will be used to determine best overall value to the City. Proposals will be compared to select one or more that are most advantageous.

And, upon selection of one or more lead Proponent(s):

- References may be contacted
- Interviews may be conducted

The City reserves the right to check references on other projects even if they are not specifically listed. Information obtained from references will be confidential and will not be disclosed to any Proponents.

These criteria will be used to determine best overall value to the City as well as any other criteria that may become evident during the evaluation process.

The City may, at its discretion, request clarification or additional information from a Proponent with respect to any Proposal and the City may make such requests to only selected Proponents. The City may consider such clarifications or additional information in evaluating a Proposal.

Incomplete Proposals or Proposals submitted on forms other than the Proposal Form may be rejected.

Proponents agree the City may disclose names of Proponents and total award amount, however, unevaluated results, unit prices, rates or scores will not be provided to any Proponents.

The City reserves the right to reject without further consideration any Proposal which in its opinion does not meet the criteria it considers essential for the work outlined in this RFP.

Where only one Proposal is received, the City may reject such and re-issue the RFP on a selected basis.

Prices shall include the provision of all tools, materials, equipment, labour, transportation, fuel, supervision, management, overhead, materials, traffic control, services, all necessary packing and crating (where applicable), Canadian Customs import and export duties, freight, handling, transportation, insurance, all other associated or related charges, foreign, federal, provincial and municipal taxes, bonding costs, all licences, permits, inspections and all other requirements necessary for the commencement, performance and completion of Services as described.

#### 1.7 Eligibility

For eligibility, and as a condition of award, the successful Proponent would be required to meet or provide the equivalent:

- a) Commercial General Liability (CGL) insurance \$5M coverage provided on the [City's Standard Insurance Form](#)
- b) Be registered and provide WorkSafeBC clearance
- c) Accept the City's standard Terms and Conditions posted on the City's website: [Standard Terms and Conditions - Purchase of Goods and Services](#)
- d) Appendix B – Non Disclosure Agreement
- e) A City of Coquitlam or Tri Cities Intermunicipal [Business License](#)

#### 1.8 Project Timeline

The City understands these items have a long lead time. Estimated timelines for the project are:

**PO issued: October 2021**

**Estimated Delivery: January 31, 2022**

**Installation: February 15, 2022**

**The City will not take delivery or remit payment before Delivery date.**

#### 1.9 Warranties

The Proponent shall provide a full statement of the warranty period and terms, including extended warranty options, for items listed in **Appendix A – Technical Requirements**, as a minimum. This warranty should clearly describe the terms under which the equipment

manufacturer or sub-suppliers of the manufacturer accept responsibility for the cost to repair defects caused by faulty design, quality of work or material and for the applicable period of time after delivery.

1.10 Sub-Consultants

The use of sub-Consultants is acceptable providing they are fully identified in the Proposal and realize the conditions of this document will apply to all Consultants named. Joint submissions must identify a prime Proponent who assumes responsibility for the Proposal as well as for the professional standards, actions and performance for all Proponents, if awarded the work.

1.11 Examination of Proposal Documents

The Proponent must carefully examine the Proposal Documents. The Proponent may not claim, after the submission of a Proposal, that there was any misunderstanding with respect to the requirements and conditions imposed by the City.

There will be no opportunity to make any additional claim for compensation or invoice for additional charges that were not considered and included in the Proposal price submitted, unless the City, at its sole discretion, deems that it would be unreasonable to do so, or there are additional work requirements due to unforeseen circumstances.

All information in this RFP Document, Site Visit and any resulting Addenda will be incorporated into any Contract between the City and the successful Proponent, and therefore must be considered by the Proponent in preparing their Proposal.

## **2 GENERAL CONDITIONS OF CONTRACT**

### **2.1 Terms and Conditions of Contract**

The City's [Standard Terms and Conditions - Purchase of Goods and Services](#), as published on the City's website, the Conditions listed below, along with the accepted Proposal, addenda and any subsequent clarifications, correspondence, the totality of which will constitute the Contract.

### **PROJECT SPECIFIC TERMS AND CONDITIONS**

### **2.2 Advertisement**

The Contractor shall not advertise its relationship with the City without prior written consent from the City.

### 3 SCOPE OF SERVICES

#### 3.1 General Requirements

The Contractor is to provide **Local Area Network (LAN) / Metropolitan Area Network (MAN) Replacement** to be used in a municipal environment as specified in **Appendix A – Technical Requirements**.

The units are to be new and the current production models with all the latest updates including, all manuals.

#### 3.2 Technical Environment

- A Metro Area Network (MAN) with Dark Fibre
- Internet Connections with different ISPs
- 2 Data Centers
- Switches are Avaya/Extreme Networks and few Juniper.
- Nortel Routers & L3 switches
- 800 desktops & VOIP phones
- 300 servers
- 19-20 buildings with main equipment in 2-3 major buildings
- >1600 staff
- Oracle Database
- Remote work capability using Citrix and VPN

#### 3.3 Equipment Design Document

##### **Appendix A – Technical Requirements**

#### 3.4 Scope of Services

The Services include, but are not limited to:

- Supply and Delivery of the equipment proposed. Equipment should include support, technical assistance, RMAs, licensing and allowing the City to work directly with equipment vendor as well as proving online dashboards for ticket management. Please provide separate pricing for 3 years and 5 years
- Project Management Plan, at a minimum should include plans for the following
  - Configure and test equipment to meet security and network performance requirements
  - Provide detailed action and test plans, documentation, and change management
  - Provide complete test plan to reflect and prove the same or better network performance
  - Suggest any recommendations for additional/different components and/or module that may better suit City's needs
  - Scheduling of maintenance windows so as to minimize impact to City of Coquitlam
- Low level design in collaboration with the City Architecture and Operations Team

- Documentation and Training Plan: The City shall require a proper Knowledge Transfer to City Staff before project is considered complete, including training that will provide staff the skills to support and manage the equipment
- Updated network diagrams and documentation using templates provided by the City
- Professional Services
  - Rack, Stack and follow implementation standards as dictated by the City of Coquitlam
  - Project Management
- Provide local (Metro Vancouver) dealer warranty service; and
- Provide post-delivery services and parts.
- Completion criteria: the equipment must be online, fully tested, documented, functional, in production environment and support staff fully trained

### 3.5 Security and Confidentiality

The Contractor will be required to complete and submit the City's **Appendix B – Non Disclosure Agreement** upon award.

### 3.6 Qualified Personnel

All Work shall be performed by qualified and skilled persons pertaining to the licensing and qualifications for the respective trades in strict accordance with the applicable Municipal, Provincial, Federal and other laws, regulations, standards, codes, etc. including, the abatement of hazardous materials if required. All workmanship and materials will be subject at any time to the inspection and approval of the City.

The Contractor and persons hired by it to perform the Work shall at all times be properly attired and shall be courteous to the public and all other trades / work crews, and perform the Work in a manner that minimizes any inconvenience or nuisance to the public.

All actions performed by Contractor must be properly recorded and all new installations must be accompanied by appropriate permits, drawings, engineering reports, maintenance manuals and training at completion must be provided to the City.

### 3.7 Quality Assurance

The Contractor shall be responsible for inspection and Quality Assurance (QA) for all materials and workmanship provided.

The components shall be manufactured by firms regularly engaged in the manufacture of equipment of the types, sizes and service required.

The Contractor shall be a factory certified contractor specializing and experienced in the type of equipment.

### 3.8 Warranties

The Supplier agrees to repair or replace any faulty equipment and that any defects discovered and failures which occur during the guarantee period will be rectified to the satisfaction of the City within a reasonable amount of time at no cost to the City.

3.9 Recall Notices

In the event of any recall notice, technical service bulletin, or other important notification affecting units purchased under this Contract, a notice shall be sent to the City. It shall be the responsibility of the Supplier to assure that all notices are sent directly to the City.

3.10 Delivery, Storage, and Handling

All materials and equipment to be new.

All packaging material must be removed from sites at the Contractor's expense.

3.11 Site Control and Organization

The Contractor shall at all times keep the site secure, safe, clean and orderly as the Work allows.

\*\*\*\*\*COVID - 19 Site Safety Requirements\*\*\*\*\*

Contractor is responsible for following all COVID - 19 site safety requirements which are posted by WorkSafeBC and subject to change as the situation evolves:

<http://www.bccasn.com/media/Guidance%20to%20Construction%20Sites%20Operating%20During%20COVID19.pdf>

[Contractor COVID-19 Info Sheet](#)

3.12 Rejected Work

Defective Work, whether the result of poor workmanship, use of defective products or damage through carelessness or other act or omission of the Contractor, shall be rectified at the Contractor's expense.

3.13 Hours of Work

The City's preference is for the Contractor to carry out the Work during normal working hours (8am-5pm). Requests for Work outside normal business hours may be accepted and are to be sent in writing with forty-eight (48) hours' notice in advance of the work.

3.14 Clean Up

At the end of each day the Contractor shall ensure the site is safe and secure and, at the conclusion of Work, the Contractor shall clean out all debris promptly remove any equipment or materials and leave the site of the work in a clean and tidy condition.

# **Appendix A – Technical Requirements**



**City of Coquitlam**

**LAN / MAN upgrade**

**RFP - Technical Requirements**

**V0.1 – Sep 2021**

## Contents

<b>1</b>	<b>Summary .....</b>	<b>4</b>
1.1	Scope.....	4
<b>2</b>	<b>High Level Topology and Requirements .....</b>	<b>5</b>
2.1	Resiliency Requirements .....	5
2.2	Capacity Requirements .....	6
2.3	DC and Campus L3 Core Requirements.....	7
2.3.1	Connectivity .....	7
2.3.2	Capacity & Performance.....	8
2.3.3	Dynamic routing.....	8
2.3.4	QoS.....	9
2.3.5	Routing Segmentation.....	9
2.3.6	Security Segmentation .....	9
2.3.7	Security Inspection .....	9
2.3.8	Authentication.....	9
2.3.9	Resiliency - Automatic failover to alternate DC.....	9
2.3.10	Lifecycle.....	10
2.3.11	Operational Surveillance .....	10
2.3.12	Operational Management .....	10
2.3.13	Event management .....	10
2.3.14	Backups .....	10
<b>3</b>	<b>Design .....</b>	<b>11</b>
3.1	DC Core and Campus Layer 3 switching .....	13
3.1.1	Requirements for the Layer 3 core design element .....	13
3.1.2	Layer 3 Core design .....	14
3.2	Server Farm or DC Switching Fabric .....	15
3.2.1	Switching Fabric Design Approach .....	15
3.3	Internet, Edge Networks and DMZ access.....	17
3.3.1	Internet, Edge and DMZ access design .....	18
3.4	Access and Distribution Switches.....	20
3.5	Network Management and Surveillance.....	21
3.5.1	Typical requirements needed for a Network Operations team.....	21
3.5.2	Integration to other external systems.....	21

# LAN / MAN Design Requirements

## 1 Summary

This document describes the high-level design requirements for the new Coquitlam Campus and Data Centres Network.

The campus and data center network is central to the overall Coquitlam architecture. The DC is where most organization-critical applications are hosted, and various types of services are provided to the organization. Proper planning of the data center network design is critical, and performance, resiliency, and scalability need to be carefully considered.

### 1.1 Scope

The following elements are in scope to be replaced or included in the new design.

- Core switching and routing.
- Server Farm Ethernet switching.
- DMZ switching.
- Internet routing.
- Access switching.
  - The replacement of the existing legacy access switches will be done in a **phased** approach. The initial phase will include **one** switch stack at the City Hall building (stack with 3x48 port SWs) and **one** at a close venue (Pine Tree Community Centre – single 48 port SW) to use as initial proof of concept.
  - All other access switches will be replaced in the following phase. To execute as a subsequent acquisition using the same reseller and products.
- Management Servers – Those needed for centralized node configuration (configuration generation and backups) and those used for management authentication (while using SSH).

Not in scope for this RFP:

- Firewalls & IPS replacement.
- Wi-Fi APs and controllers.
- VPN termination devices.
- Sniffing servers.
- Terminal servers and out-of-band connections.
- Any external fibre runs

## 2 High Level Topology and Requirements

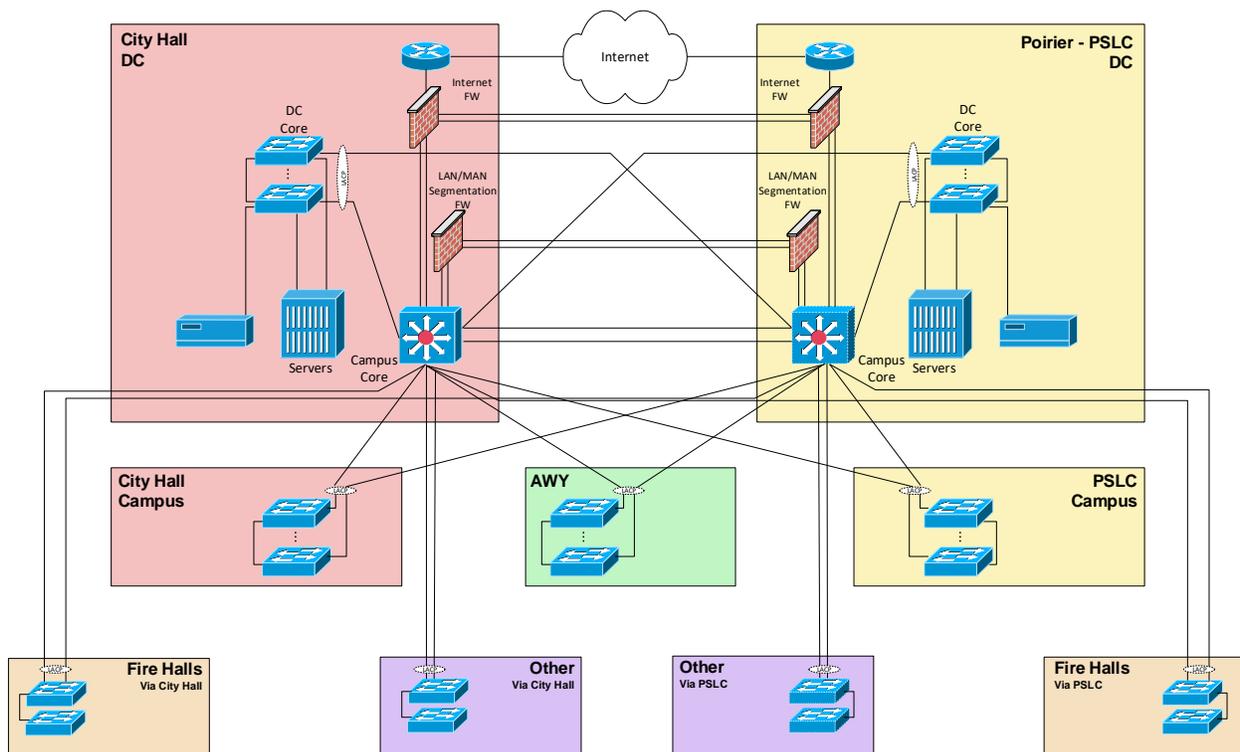
The following diagram provides a high-level view of the new City Network. As can be seen, the design includes core switches located at two Data Centres (DC). It is highly desirable for these core switches to work as a single logical node running a single control plane.

### 2.1 Resiliency Requirements

Some of the main improvements this new design brings, is **higher availability** for the most **critical** users.

As the following diagram shows, the **Fire Halls** are considered mission critical as part of the 911 emergency notification. They must be able to continue in full operation even if one of the core switches fails. Even more, even if a complete DC is out of service because of electrical disruptions, they will still be able to reach the alternate DC. Other critical locations with POS or tax collection could follow this approach.

Having diverse fibre paths is desirable. Having at least diverse fibre strands and diverse active equipment at both ends is highly recommended.



The design also includes uplinks from both critical access, distribution and server farm switches reaching both cores (instead of a single one as it is the case in the old network).

Finally, the Internet access tier exposed to public and 3<sup>rd</sup> party flows is decoupled from the core; an extra internet and perimeter firewall is introduced.

## 2.2 Capacity Requirements

This is the opportunity to **upgrade** in general all **interface speeds** from the previous network design. If an interface was operating at 10 Gbps, even if we do not have an immediate need, we can aim to take advantage and migrate all to 40 or 100 Gbps.

Fibre interfaces in between switches operating today at 1 Gbps can be improved to the newer standards of 10 or 25 Gbps (available in both single and multi-mode fibre).

Finally, access switches feeding end users at 1 Gbps in copper, can now be turned into multi-gigabit ports operating at 2.5 or 5 Gbps. This is especially important for Wi-Fi access points, and in a potential near future for power-users as well (graphic files, GIS, AutoCAD).

Still, during this migration not all interface speeds will be upgraded at the same time. The new network will need to provide several interfaces that can still satisfy legacy devices. This includes access switches that are gradually migrated.

The type of available fibre can be a limitation to jump immediately into faster speeds. The City includes lots of multi-mode OM1 type fibre. Newer speeds do not support this legacy type. Single mode fibre is also available for long distance runs.

## 2.3 DC and Campus L3 Core Requirements

The following list includes requirements that directly affect the experience of any user or device connected to the network.

### 2.3.1 Connectivity

Provide connectivity to all Network and Server elements.

#### 2.3.1.1 Core

One **campus core switch** will be located at the City Hall DC while the other at the PSLC DC; just like the old network did. A trunk interface will be created in between both during the migration.

Using the old network architecture as an initial reference for the new connectivity requirements, this is what can be used as initial **minimum** requirement per core switch:

Totals "Slow Speed"	1G	12
	10G	23
	25G	13
Sub Total		48
50% growth		24
<b>Total Slow Speed</b>		<b>72</b>

Totals "High Speed"	40G	12
Sub Total		12
50% growth		6
<b>Total High Speed</b>		<b>18</b>

Each new core switch will be able to reach directly or through an aggregation layer all locations to provide core diversity.

Gradual growth for the future should provide at least 50% spare interfaces of each type.

High-Speed interfaces will now be considered as 40G or 100G instead of 10G as the previous core did. Slow-Speed interfaces will still include 1G as an option in aggregation or core switches. The core itself will allow 10G and 25G downlinks.

It is highly desirable for the core to be implemented selecting equipment that offers interface **ASIC diversity**. In the data plane, one ASIC controlling a group of ports can be allowed to be unavailable without bringing down the whole switch functionality. This can be achieved by using a modular switch with multiple equivalent blades, or at least using fixed switches whose architecture is known internally and ASIC diversity among ports is validated.

### 2.3.1.2 Server Farms

A new server chassis design is also due as the existing ones already reached their end-of-life.

The introduction of new server farm switches is an option. The design can also consider consolidating few server connections directly into the core switch without requiring the deployment of server farm switches.

Related to the server chassis, we also wish to move to 40G connectivity. Each new chassis will require 2 x 40G links. There could exist two chassis per DC location. We can include the option to provide 2 links per SW into the Chassis; that will mean 4 connection in total with about 160 Gbps per server chassis. This is mainly for resiliency, not for capacity needs. 4 x 2 = 8 x 40G links used for chassis connectivity. The sever farm can include at least two different switches able to provide this connectivity type. Half of these connection can come from a single switch; this is about **4 x 40G ports per switch** for server connectivity.

Connectivity requirements can grow from 15% to 20% per year. In 5 years, this represents close to 100%. This means we could double the 40G connectivity requirements. These will go from 4 x 40G to **8 x 40G** ports for server connectivity.

1 Gbps copper interfaces are still needed for management ports in the DCs. We can consider 96 ports at each DC.

10G fibre connectivity is also needed for some legacy devices still expecting this.

Bottom line, each DC server farm / switching fabric must be able to provide a dozen or more 40G ports while also allowing 20 or more 10G ports and 20 or more 1G copper ports.

The previous matrix considers these points.

### 2.3.1.3 Access Switches

These will still be needed to provide connectivity to end users at all edge locations of the network.

These will include any “manned” devices like desktops, laptops or IP phones. PoE+ (30 Watt) will be available. There seem not to be requirements for UPOE (60 Watt) and beyond.

Wi-Fi access points will be able to connect at multi-gigabit speeds via copper ports (2.5 or 5 Gbps).

Other unmanned IoT or building systems devices are also included. For example, CCTV with cameras potentially requiring PoE+ (still, all aggregated at 1 Gbps).

## 2.3.2 Capacity & Performance

The solution should be able to forward packets at the described speeds without dropping packets because of reaching CPU or memory buffer limits (wire-speed switching).

## 2.3.3 Dynamic routing

Be able to peer with WAN service providers using the specific protocols (BGP & OSPF) they specify.

#### 2.3.4 QoS

Related to Quality-of-Service and traffic priorities for LAN and MAN flows, the solution should honor IP DSCP priorities while queueing and will have the option to apply policies that remark specific flows (lower priorities).

The solution should also be able to police and shape traffic. Specific flows should be able to be restricted to use only a maximum allowed capacity.

#### 2.3.5 Routing Segmentation

Routing should be separated into multiple domains / **VRFs** according to the security zoning and framework. At **least 40** of these must be available on day one; also having enough memory for all routing entries.

#### 2.3.6 Security Segmentation

The solution should include a way to define very strict stateful security policies that govern which flows can cross in between different zones at the DC and the MAN links. Including a NGFW in the design will happen in future phases. For now, all segmentation implemented by existing Firewalls will be migrated into the new core switch including multiple VRFs.

#### 2.3.7 Security Inspection

The eventual solution must be able to accommodate **discrete** IPS devices working in-line and facing the DMZ/Internet and also the server farms. We will eventually move those to 40G when the new Firewall replacement project happens (future phase). For now, the Firewall migration into the new core will be a like-for-like migration (in other words, there is no IPS in the immediate picture) and Firewall connectivity happens at 10G.

#### 2.3.8 Authentication

All network elements deployed at the DCs, LAN and MAN must allow central authentication while being managed by the network or security administrator. TACACS or Radius should be the alternative to consider.

#### 2.3.9 Resiliency - Automatic failover to alternate DC

The core must be virtualized in a way that the failure of one of the switches at each DC should result in a transparent failover to the other.

### 2.3.10 Lifecycle

The proposed equipment should not be close to the end of its sales life and in the same way it should not be a product recently introduced into the market. The same applies for the software being used.

As a recommendation, we should consider equipment that has already been sold since 1 to 2 years ago. On the other hand, it should not be 1 or 2 year from being discontinued (should consult with the vendor). **5 years lifecycle** is the standard followed for all network nodes in this design.

### 2.3.11 Operational Surveillance

All elements in the network solution must be integrated to a central surveillance solution able to detect real time availability and historical capacity usage. SNMP surveillance is a starting point. Still, telemetry that can report spikes in between polling cycles is desirable and now present in new platforms.

We will go beyond simply checking the interface status port in a manual way. The new solution will include the creation of dashboard, notifications, and reports.

### 2.3.12 Operational Management

All elements in the solution should be able to generate flow information (Netflow ver 5, 9 or FnF, sflow, IPFIX or equivalent). A flow collector is not in scope.

### 2.3.13 Event management

Security, switching and routing events should be centralized and available via (SNMP traps, Syslog and proprietary if these exist). The logging server is not in scope.

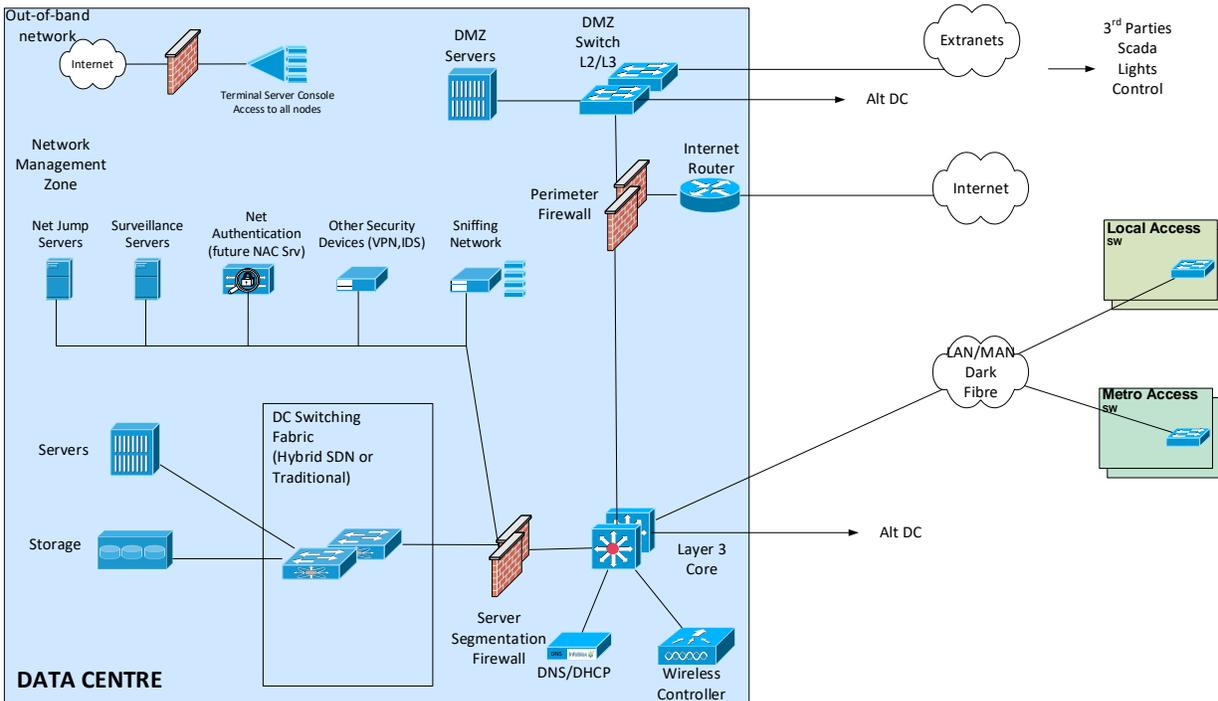
### 2.3.14 Backups

All network elements configuration must be backed up daily from at least two remote locations.

### 3 Design

This design follows a modular approach. The different elements in the DC / Campus design integrate as separate building blocks.

The following diagram shows at a very high level all different building blocks considered for the DC / Campus network architecture:



- The data center and campus L3 core interconnects all the building blocks. It is also used to connect the rest of the City network (MAN) and elements located in other data centers; it also connects the Internet block. It is intentionally a separate block that is less dynamic in terms of daily operational changes.
- The DC switching fabric interconnects and aggregates all traffic coming from Platform elements (Servers and Storage).
- The Campus and DC Segmentation Firewall implements all internal Platform zoning (PCI and other). It forces all flows originating in Platform elements (Servers and Storage) to be subject to strict security access and inspection policies.
- The perimeter / edge Firewalls deal with the segmentation of any flows interacting with external nodes in relation to the City. This obviously includes the Internet, 3<sup>rd</sup> party VPNs and other extranets. These are assisted by the Internet routers which deal only with Internet bound traffic.
- The DMZ switch is physically and logically an independent connectivity point for Platform and network elements that are exposed to third parties.
- The network management zone includes many elements that do not handle user traffic directly. Instead, these elements are focused on the actual operation and resources needed for the network operations team.

- Finally, the out-of-band network provides a totally independent solution to connect to all key network nodes. This applies for normal and 'rescue' use cases.

## 3.1 DC Core and Campus Layer 3 switching

The Data Centre and Campus layer 3 core is the main place where routes are being exchanged between all components in the DC and MAN. It forwards traffic to reach the local switching fabric, the Internet and DMZ and the MAN links reaching the remote city locations.

The DC Layer 3 Core is a critical part of any Network this size. It is the gateway to all external Services or Networks that need to leave the DC. It is a clear dividing line from the DC Switching Fabric and an isolation point in the Network which helps in Operational support. This Core Layer needs to be very stable and once set-up should rarely need to be changed. Failover routing decisions would occur here in the event of a MAN link outage.

### 3.1.1 Requirements for the Layer 3 core design element

The following list shows what is expected from this block. As can be seen, this integration block owns functionality that cannot be consolidated into other existing elements (central routing table, firewall and WAN connectivity).

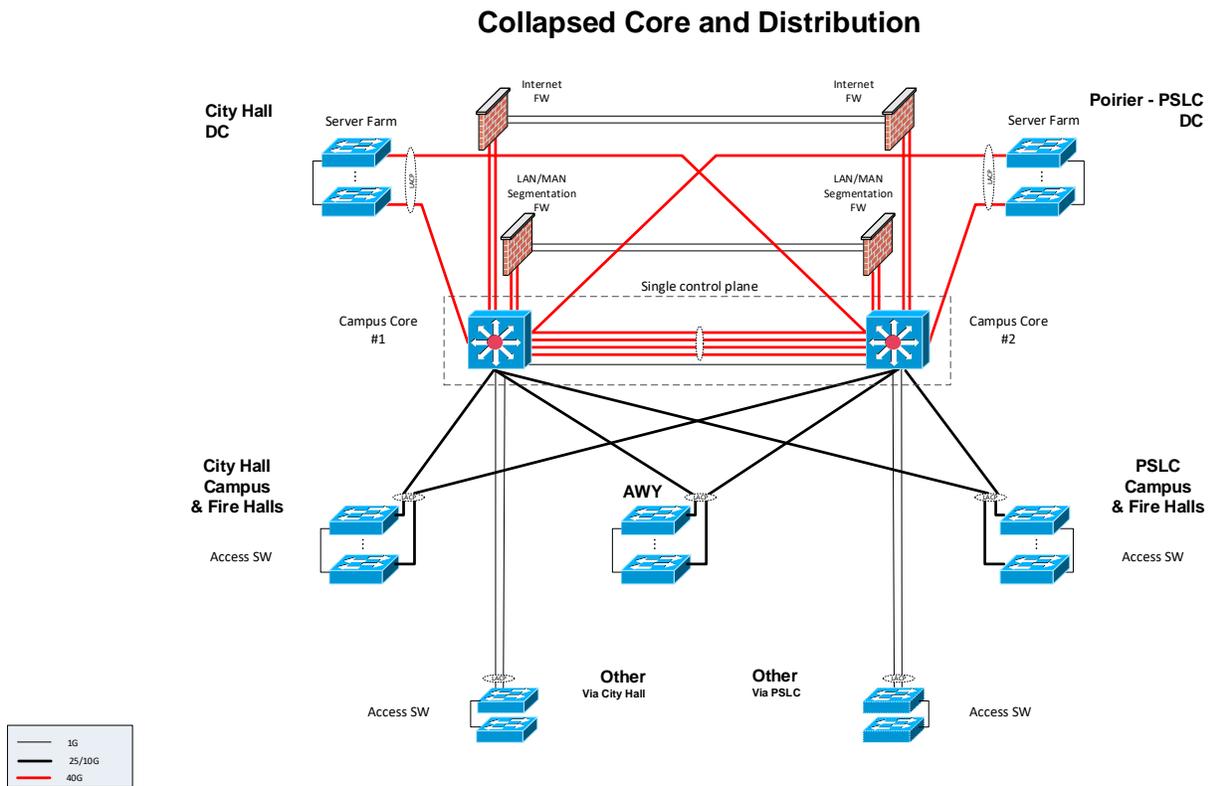
- Interface with MAN links. Add the option for each MAN link to have two alternate connections from the edge device into the DC and campus layer 3 core.
- Interface at high speed with the switching fabric. Even if the Internet access and WAN access blocks interface into “slow” capacity links (WAN @ 1 / 10 Gbps), there is still need to reach the DMZs at higher capacity for server-to-server flows. 10G or even 40G connectivity is highly desirable. Switching/Routing capacity allows link-speed connectivity with no oversubscription.
- If required, use OSPF as the internal DC routing protocol to aggregate all internal routes.
- Interface with the Internet access block for layer 3 traffic routing into DMZs, VPNs, and the Internet. This is also a place to offer layer 2 interconnectivity for the Edge / Internet Firewalls (HA-pair) that provides access to that block (an alternative to avoid having separate layer 2 switches just to “glue” blocks).
- Offers potential software tapping points (SPAN) for packet capture and analysis (IDS, DLP, Sniffer).
- Include HA redundancy for this block physical elements.
- Keep the number of physical elements in this block to a minimum number.
- Software Defined provisioning. State of the art APIs that could be used to automate tasks and at some point, be part of a private cloud overall approach. Nevertheless, the core of the network is not a place for many changes and this is mainly a nice to have requirement.
- Having a multitenant approach is not a current requirement.
- Redundant power supplies fed by C14 outlets.
- Include optics needed to interconnect core switches using single mode fibre (10 Km or less).

### 3.1.2 Layer 3 Core design

We prefer the core design to be implemented with a single chassis per DC to offer high density of high-speed 40G/100G ports and at the same time slow speed 1G/10G/25G interfaces. Another very important feature is the option to aggregate two physical chassis into a single logical entity.

This may not sound as resilient as having two independent devices. On the other hand, it makes the operation very simple, which is a top priority in this design.

The following diagram shows the layer 3 core being in between all access switches, and also all core devices in the DC.



## 3.2 Server Farm or DC Switching Fabric

The Data Centre switching fabric provides very high speed, low latency, and great connectivity to aggregate all **Platform** elements (servers and storage via IP). It obviously allows “vertical” traffic to reach other layers (WAN, Internet). Nevertheless, as happens in current DC designs it also moves large amount of “horizontal” traffic in between Platform elements. Grouping servers in tiers or security zones is part of this design. This increases this type of traffic.

All modern platform elements require high interface speeds. Offering 40G and 10G Ethernet connectivity is already a requirement. In the future some servers could require even more. There is also a requirement to connect slower ports at 1Gbps (management and few potential legacy devices that could be temporarily needed at the DC).

We should also remember the requirement to follow a very conservative / low-risk approach and at the same time open the option to offer a Software Defined Network (SDN) alternative.

Note: At this point, it is not in the scope of this design to satisfy storage Fiber Channel connectivity. This is implemented by independent FC switches (not covered here). FCoE is not a requirement to consider. Still, there could be storage flows using the IP/Ethernet network in the future (ISCSI, NFS, CIFS volumes) but not in scope in the short and medium term. All access to storage is done via the VMs and hypervisors.

### 3.2.1 Switching Fabric Design Approach

The DC fabric can provide the option to centralize all connections into a single central pair of switches providing line cards that feed servers and storage directly. Nevertheless, this architecture becomes “stiff” or difficult to expand (if needed). Also, in a DC, it is easier to provide local switching in each cabinet/rack without extending a lot of cables to a central location.

We could follow instead a hierarchical design. Core fabric switches and distribution / top-of-rack (ToR) switches. Instead of connecting all platform resources to a single central set of switches, these are connected instead to switches that behave as the “edge” of the fabric. These can be considered as *distribution* switches in a traditional topology or *leaf* switches in a new spine/leaf topology.

#### 3.2.1.1 Spine-Leaf

For big deployments, a two-tier spine-leaf fabric provides any-to-any connectivity with predictable bandwidth, increased throughput, and consistent low latency. Every leaf switch is connected to every spine switch, providing equidistant behavior. Traffic with the source and destination on the same leaf is handled locally, and all other traffic travels from the ingress leaf to the egress leaf through a spine switch. This is specifically important to meet the new trend of lots of horizontal traffic in between elements in the DC.

For a bigger DC with lots of cabinets and servers and the option for a drastic gradual expansion, this would be the recommended solution. Still, the Coquitlam DC **requirements are very limited**. A controller-based spine-leaf fabric represents a very steep learning curve, and it is **not** recommended

### 3.2.1.2 *Traditional hierarchical design*

We consider if we create the server farm with very similar switches compared to those in the rest of the design will make the Operations process simpler to follow for the network administrators. These switches can provide connectivity to many server chassis via 40G interfaces.

The server farm can be implemented with a pair of high-speed physical (1U) switches. It only includes 40G/100G interfaces, and it is stretched to exist in both DCs. This is however a single logical switch managed as a unique entity.

Server chassis are directly connected at 40G. If possible, each chassis can be fed from different switches to create location and device diversity. If existing chassis only operate at 10G speeds before being refreshed to newer platforms, connectivity can still be provided via the server farm switches using QSFP to SFP+ adapters (QSA). Alternatively, if many 10G devices still need connectivity, that can be accomplished via an additional server farm access or top-of-rack switch.

One or multiple of these access top-of-rack or middle-of-row can be added to satisfy the geography of the DC. Some may only need to provide 1G connectivity; some can be engineered to provide 10G aggregation.

### 3.2.1.3 *Partial or total collapse into Campus Core*

This can also be considered as an option (to compare cost with previous). In this case, if high-speed server connectivity requirements are very low, they can simply use few ports in the campus core. This can apply specially for few high-speed 40G interfaces (one or maximum two chassis per DC requiring 2 to 4 uplinks each). 1G and 10G connections can still be done using a hierarchical approach with top-of-rack or middle-of-the-row switches.

Yes, this can be counterintuitive and bring us back 15 years into the past when the campus core used to be the place to connect servers as well. Nowadays with high density server chassis and hypervisors, we feel we can go back to follow this approach as an option.

### 3.3 Internet, Edge Networks and DMZ access

The main purpose of this building block is to provide access from networks that are **external** to the City. In few words this considers connectivity, routing, and security to other networks. This building block is intentionally decoupled from the campus core. This happens both in a physical and logical way. This is mainly a security requirement that will aim to isolate external traffic to never be routed or switched by the internal network.

We consider the following as external networks:

- The Internet.
- Any City customers that could use it as an ISP.
- DMZ are included here. In this design we consider a DMZ as a security zone with resources directly exposed to external connections.
- Encrypted VPNs over the internet originated by a trusted third party or person. Among these we have:
  - Point-to-point VPNs from remote locations or organizations with multiples nodes and routes.
  - Dynamic single node VPNs originated from corporate owned devices and subject to two-factor authentication.

Among the requirements this building block needs to satisfy we have:

- Internet Traffic capacity. Be able to offer the same Internet access capacity of 1 Gbps in production before this migration. Also, be able to **migrate to higher speeds** without needing a physical interface or equipment change. This considers interconnecting with service providers using higher speed interfaces like 5 or 10 Gbps (copper or fibre; to agree with each service provider about available options).
- Connectivity to diverse Internet access providers. Be able to peer with these providers using BGP and potentially receive the **full** Internet routing table. By doing this, we can reach each Internet destination by using the best peering point (based on BGP metrics). It is important in case the City as it is hosting critical Internet facing services used by vendors and customers distributed all over across the municipality.
- Offer local network equipment and link redundancy per location into the service provider on-site edge device(s).
- Offer location diversity. Corporate Internet access will not depend only on the City Hall DC being the single alternative. If this is unavailable, other locations must have an alternate way to reach the Internet. PSLC is considered as the main alternative to introduce this level of redundancy.
- Provide routing preferences based on geographic location in the corporate network with the option to failover to an alternate Internet access peering point in case the preferred one is not available.
- Introduce a firewall layer into all flows originating from external networks. The specific requirements these firewalls need to satisfy are covered in a different section.

- Provide connectivity to servers and other nodes that exist in the various DMZs. The specific requirements for the DMZ switches are covered in a different section. PSLC is an symmetric and alternate location in relation to the City Hall DC for DMZ services.
- Provide connectivity and traffic replication for any security traffic analysis tool that requires this (IDS, DLP).
- Some flows in a DMZ need to reach the equivalent DMZ at the alternate location (for example for DNS replication). The solution needs to allow this level of communication without exposing each security zone to others with less security level. In a similar way, Internet routers at different locations should be allowed to establish an I-BGP peering session by tunneling through the DMZ switch.
- Optionally, support IPv6 in case the City may plan to start running a dual stack facing the Internet and other networks.
- Include optics to reach the local and remote core via single mode fibre (10 Km or less).

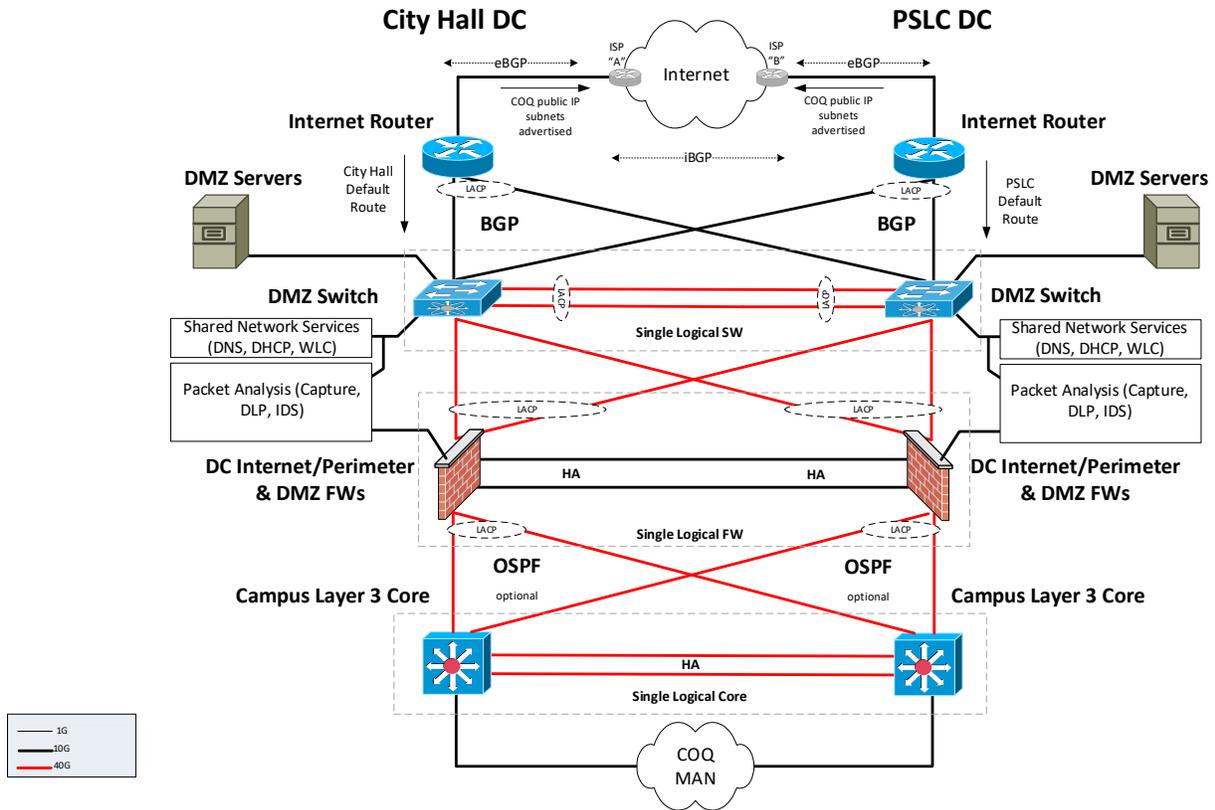
### 3.3.1 Internet, Edge and DMZ access design

This is the proposed solution: We consider two Internet peering points: The City Hall and PSLC. These deal with city nodes creating flows that interact with the Internet. This applies for both incoming and outgoing flows. City traffic can originate from City Hall as the main contributor but can also originate from the other locations in the MAN.

Each one of the two Internet peering points includes one router. Each router originates an internal Internet default route that is propagated via BGP into the Internet / Edge firewalls and then from there to the rest of the LAN and City MAN. Each route includes BGP attributes that allows all consumers decide what the preferred option to reach the Internet is. In case one route becomes unavailable, the alternate route becomes active and all outgoing Internet traffic starts routing through the other peering point.

There is no Policy Based Routing in place that routes outgoing traffic based on source IP addresses. All routing is done by configuring BGP and all it associated metrics to prefer on route on top of the other.

The following diagram describes the solution in a graphical format:



As all DMZ servers live at the City Hall and PSLC DCs (those offering a public service open to receive an incoming connection), in a normal situation BGP will advertise this entry point as the preferred option to receive traffic; PSLC will advertise these with a lower preference. In case of an Internet access failure at the main DC, these same routes will still be advertised from PSLC and all public traffic will ingress through that point.

## 3.4 Access and Distribution Switches

At the City some switches behave only as access switches providing connectivity to end-devices (user workstations, Wi-Fi APs, VoIP phones & IoT devices). Other switches do this and in addition, because of the fibre local topology, also work as distribution switches. These distribution switches include uplinks to the core and downlinks to other access switches they feed.

The main requirements for these switches are:

- Connect end user devices at 100 Mbps and 1 Gbps. In some cases, using existing legacy Cat5e copper cabling. In other cases, using newer Cat6 or Cat6a cabling.
- Some devices (like Wi-Fi APs offering 802.11ac & ax) do require higher speeds in copper. Access switches will require offering several multi-gigabit interfaces able to operate at 2.5 or 5 Gbps (via Cat6a as the desired cabling).
- Be able to provide PoE+ (30 Watts). There are no requirements at this point for UPoE (60 Watts) and beyond.
- Be able to provide redundant power supplies. Some locations include alternate power circuits and PDUs feeding switches. In other locations having at least power supply diversity is desirable, even if connected to the same circuit and PDU.
- The solution should be able to allow switch stacking. This will allow a dynamic growth depending on the site requirements. It is desirable not to restrict the design to chassis-based solutions that could limit an expansion or, alternatively, become very expensive and never be totally used.
- Provide the right performance and capacity while stacking switches and in their uplinks to the core. We know end-user activity typically works in bursts and it is normal to oversubscribe the overall capacity. We expect normal users to only be active 5% of the time consuming network capacity. With this in mind, uplinks will still allow 50% of spare capacity. Different uplinks can be aggregated via LACP to reach the right capacity (either adding more 1G, 10G or 25G interfaces).
- Offer QoS at the edge. Trusting DSCP marking by end devices or remarking this as needed. Then, having multiple queues with the right priority in the uplink to the core.
- No layer 3 functionality is required for these devices.
- Add basic security features to protect the network against loops and intruders (filters and detection for BPDU, ARP, DHCP, or general broadcast storms).
- Satisfy our management and surveillance requirements using the same tools used for all other Campus and MAN switches.
- It is desirable for fibre uplinks to be fed by interchangeable modules. Include optics/SFPs for these to use single mode fibre (10Km or less) at 10 or 25 Gbps.

## 3.5 Network Management and Surveillance

Included with all new network gear, the technical proposal also needs to include a system able to cover the following network management tasks:

### 3.5.1 Typical requirements needed for a Network Operations team

This list represents typical elements, tools and processes we consider a network operations team should have access to as a result of this deployment:

- Backup and restore of all network nodes configuration.
- Configuration change accounting - keeping track of who and what was changed at different points in time.
- Configuration & image deployment automation - Able to build configuration templates with configuration sections that are deployed to all similar nodes at once – track successful and failed deployments; to be able to apply general commands globally (i.e. configuration save; reboot).
- Configuration consistency and integrity verification - measurements for correctness and unexpected changes; verify all devices include a consistent configuration (especially in those areas that are general to all devices).
- OS image integrity and Common Vulnerabilities and Exposures (CVE). Validate that each OS image has not been tampered and is not vulnerable to a known threat.
- HW & OS version advisor - security alerts; contract coverage and end-of-life status.
- Network device inventory. List of all devices, models, serial numbers and locations.
- General surveillance and availability – ping and periodic polling with SNMP or any other agent. Notifications and real time display of overall and specific network device health.
- Environmental surveillance - Temperature, Fans, Power, CPU, Memory. UPS surveillance will also be included here (if one is present).
- It is desirable to offer capacity management based on telemetry rather than periodic polling.
- Centralized network authentication. If possible, independent to other Platform resources (AD, LDAP).
- DC diversity as an option.
- The solution can run as a collection of VMs in a hypervisor (desired approach) or as a dedicated appliance.

### 3.5.2 Integration to other external systems

The new network will be able to interface with other existing or independent systems able to:

- Perform event and log management – SNMP traps / Syslog – alerting, indexing, querying historical. Access to a SIEM that can be mined with complex queries.
- Flow management – Netflow – exporters and collectors.
- Time synchronization for the network and in general for all infrastructure and application elements.
- Network visibility, capture and analysis – Able to have multiple tapping points that allow the integration of security, application and network traffic analyzers and potential detailed flow storage.

- Collaboration QoS and assurance management – WAN latency, packet loss, jitter.
  - In this last case, it can be interesting to host software agents running in a container environment hosted inside one of the new network devices (no need to have a hypervisor at all locations).

## **Appendix B – Non Disclosure Agreement**

# **NON-DISCLOSURE AGREEMENT**

In consideration of participating in an RFP process conducted by the City of Coquitlam (the “City”) as a Proponent, **XXXXXX** (the “Proponent”) agrees as follows:

1. The Proponent acknowledges that during the RFP evaluation process he/she may have access to certain trade secrets and confidential information of the City, its contractors, suppliers or residents (the “Information”). Information includes but is not limited to any of the following:
  - i. business methods, practices, and strategies;
  - ii. compilations of data, information, or other documents concerning business, methods, practices, and strategies;
  - iii. information deemed sensitive or private under the laws of British Columbia;
  - iv. information about residents of the City;
  - v. confidential, proprietary or trade secret information submitted by suppliers, consultants or co-venturers to the City for study, evaluation or use; and
  - vi. any other information not generally known to the public (including but not limited to information about operations, products or services) which, if misused or disclosed, could adversely affect the reputation and/or business of the City.
2. The Proponent recognizes that disclosure of the Information to any unauthorized person may expose the City to substantial and irreparable harm, and agrees that, except as directed by the City, he/she will not at any time, whether during the RFP process or after an award as a result of the RFP process, his/her involvement as a Proponent, disclose any Information to any person or permit any person to examine and/or make copies of any documents which contain or are derived from the Information.
3. The Proponent acknowledges that disclosure of any confidential information will give rise to irreparable injury to the City, inadequately compensable to damages. Accordingly, the City may seek and obtain injunctive relief against any breach or threatened breach of this Agreement, in addition to any other legal remedies which may be available.
4. The provisions of this Agreement shall be enforceable notwithstanding the existence of any claim or cause of action of by either party against the other whether predicted on this Agreement or otherwise, and shall survive the conclusion of the RFP process and subsequent contract award.
5. This Agreement shall be enforceable in and construed in accordance with the laws of the Province of British Columbia, Canada.

6. This Agreement contains the entire agreement of the parties relating to the Information. This Agreement may be modified only by an instrument in writing signed by both parties hereto.

IN WITNESS WHEREOF, the Consultant has executed and delivered this Agreement as of the \_\_\_\_ day of \_\_\_\_\_, 2021.

Witnessed by: \_\_\_\_\_

\_\_\_\_\_  
Print Name

Signed: \_\_\_\_\_

Name of Proponent/Contractor

Signed on behalf of the City of Coquitlam:

Witnessed by: \_\_\_\_\_

\_\_\_\_\_  
Print Name

By: \_\_\_\_\_

**Manager  
City of Coquitlam**

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_



City of Coquitlam

## REQUEST FOR PROPOSALS

RFP No. 21-070

# Local Area Network (LAN) / Metropolitan Area Network (MAN) Replacement

Proposals will be received on or before 2:00 pm local time on

Wednesday, October 13, 2021

(Closing Date and Time)

### INSTRUCTIONS FOR PROPOSAL SUBMISSION

Proposal submissions are to be consolidated into one PDF file and uploaded through QFile, the City’s file transfer service accessed at website: [qfile.coquitlam.ca/bid](http://qfile.coquitlam.ca/bid)

1. In the “Subject Field” enter: RFP Number and Name

2. Add files in .pdf format and “Send”

(Ensure your web browser remains open until you receive 2 emails from QFile to confirm upload is complete.)

Proponents are responsible to allow ample time to complete the Proposal Submission process. If assistance is required phone 604-927-3037.

## PROPOSAL SUBMISSION FORM

Submitted By: \_\_\_\_\_

(Company Name)

Proponents are to provide as much information as possible when replying to each point throughout the Proposal.

**1. PRICE**

Prices proposed are to be all inclusive; therefore, include all labour, material, tools, equipment, transportation, fuel, supervision, disposal fees, permit fees and any other items required for provision of the services (exclude GST). Provide below or provide as an attached:

1.1. Equipment Prices

A full list and description of equipment offered to be stated below:

	<b>Equipment Type</b>	<b>Part Number</b>	<b>Model</b>	<b>Unit Price</b>	<b>Quantity</b>	<b>Total Price (Exclude GST)</b>
1.				\$		\$
2.				\$		\$
3.				\$		\$
4.				\$		\$
5.				\$		\$
6.				\$		\$
7.				\$		\$
8.				\$		\$
9.				\$		\$
<b>Total Price (Excluding GST)</b>						<b>\$</b>

1.2. Additional Rates

<b>Description</b>	<b>Unit of Measure</b>	<b>Price</b>
Rate to assist and teach installation procedures	Hourly	\$
Project Management Plan	Each	\$
Design (low level design and updated documentation)	Each	\$
Documentation and Training Plan	Each	\$
Completion criteria: equipment functional and staff trained	Each	\$

1.3. Maintenance and Support

Term	Price
Equipment 3 year maintenance and support option	\$
Equipment 5 year maintenance and support option	\$

**2. REQUESTED DEPARTURES – CONTRACT**

The Proponent has reviewed the City’s Contract and the [Standard Terms and Conditions - Purchase of Goods and Services](#). I/We would be prepared to enter into that Contract, amended by the following departures (list, if any):

**3. VALUE ADDED**

Provide information on what makes your firm innovative, what is your competitive advantage, and what other services your firm provides that would assist or be of benefit to the City:

**4. SUSTAINABLE BENEFITS AND SOCIAL RESPONSIBILITY**

4.1. Sustainable Benefits

Describe all initiatives, policies, programs and product choices that illustrate your firm’s efforts towards sustainable practices and environment responsibility in providing the services that would benefit the City:

4.2. Social Responsibility

a) What policies does your organization have for hiring apprentices, indigenous peoples, recent immigrants, veterans, young people, women, and people with disabilities:

b) What policies does your organization have for the procurement of goods and services from local small and medium sized business or social enterprises:

**5. EXPERIENCE, CAPABILITIES AND CAPACITY**

- a) Proponent's relevant experience and qualifications in delivering Goods and Services similar to those required by the RFP

--

- b) Proponent is to provide a narrative as to their experience and capabilities in delivering goods and Services similar to those requested in this RFP:

--

**6. EXPERIENCE AND REFERENCES**

Proponents shall be competent and capable of performing the services requested and successfully delivered service contracts of similar size, scope and complexity. Provide current references that the City may contact to verify successful performance of the Services.

<b>Description of Contract</b>	
<b>Year Started</b>	
<b>Year Completed</b>	
<b>Company</b>	
<b>Contact Person</b>	
<b>Telephone and Email</b>	
<b>Contract Value</b>	

<b>Description of Contract</b>	
<b>Year Started</b>	
<b>Year Completed</b>	
<b>Company</b>	
<b>Contact Person</b>	
<b>Telephone and Email</b>	
<b>Contract Value</b>	

<b>Description of Contract</b>	
<b>Year Started</b>	
<b>Year Completed</b>	
<b>Company</b>	
<b>Contact Person</b>	
<b>Telephone and Email</b>	
<b>Contract Value</b>	

## 7. APPROACH & METHODOLOGY

Summarize the key features of your Proposal and the Technical Approach to be used. Provide a brief description the various components required for successful completion of the work.

**Delivery, set-up and execution of the work** – Proposals should address the plan for the delivery, set up and execution of the work; as well as the disposal, recycle or reuse for the surplus materials. Include any safety and pedestrian control measures.

**Support Services** - include an in-depth view of support services including online resources (forums, support groups, etc.) and emphasis on availability of local resources who are highly qualified to support the product.

**Quality Assurance** – Provide the measures the Proponent will use to maintain quality control for the Services being performed.

**Risk Factors** – Describe the risk factors anticipated and how the Proponent intends to mitigate these.

**Safety** – Proposal is to provide how the Proponent would address safety on the work site.

<b>Delivery, set-up and execution</b>
<b>Support Services</b>
<b>Quality Assurance</b>
<b>Risk Factors</b>
<b>Safety</b>

## 8. MANUFACTURER

State manufacturer you represent:

--

**9. MANUFACTURE AUTHORIZATION**

Provide as an attachment a letter from the manufacturer that you are an authorized dealer for resale.

Yes  No

**10. TRAINING AND MANUALS**

10.1. Training

Describe types of training that will be provided by Proponent’s professional Technicians:

<b>Installation</b> – State duration of training, training material used/provided.	
<b>Operators</b> – state duration of training, number of attendees.	

10.2. Manuals

a) <b>Manuals</b> (online/web based/DVD/paper manuals) included:	State Format available:
b) <b>Training Materials:</b> Access to online/web based or DVD training	Confirm: State format available:

**11. CONFLICT OF INTEREST DECLARATION**

Proponents shall disclose any actual or potential conflicts of interest and existing business relationships it may have with the Cities, their elected or appointed officials or employees:

**12. NON-COMPLIANCE**

Proponents shall fully disclose any requirements they are unable to comply with:

**13. ADDENDA**

We acknowledge receipt of the following Addenda related to this Request for Proposals and have incorporated the information received in preparing this Proposal:

Addendum No.	Date Issued

**14. AUTHORIZATION**

We hereby submit our Proposal for the supply and services as specified and undertake to carry out the work in accordance with all Regulations and Codes, applicable to this RFP.

We agree to the rules of participation outlined in the [Instructions to Proponents](#) and should our Proposal be selected, will accept the City’s Contract: [Standard Terms and Conditions - Purchase of Goods and Services](#)

The signature is an authorized person of the organization and declares the statements made in their submission are true and accurate.

For the purpose of this RFP submission, electronic signatures will be accepted.

<b>Company Name:</b>	
<b>Address:</b>	
<b>Phone:</b>	
<b>GST Registration No.:</b>	
<b>Project Contact:</b> Name and Title of Individual <i>for communication related to this RFP</i> (please print)	
<b>Contact Email:</b>	
<b>Name &amp; Title of Authorized Signatory:</b> (please print)	
<b>Signature:</b>	
<b>Date:</b>	