Network Modernization Way Forward

Version 1.0

February 2021

Shared Services Canada
Services partagés Canada
Canada

Table of Contents

Preamble

This document presents way-forward strategies for Network Modernization within the Government of Canada. This document is the current way forward for Network Modernization and is released for any feedback from external parties.

If you have specific input on this document, please provide your name, contact information and comments to SSC Network Modernization by Friday March 19, 2021.

1. The Need for Change

To realize the vision of a digital government, the Government of Canada must deliver end-to-end digital services to public servants and Canadians. A high-performing and resilient enterprise network is a key underpinning enabler of a digital government.

Shared Services Canada (SSC) is responsible for providing infrastructure, including network services, to more than 400,000 users across government departments and agencies. Network security is more important than ever as Canadians access more and more programs and services online. Protecting the government's information technology (IT) infrastructure from vulnerabilities and responding to cyber-security-related attacks is critical to the safety and security of Canadians' data and services provided by the Government of Canada.

To effectively deliver services to Canadians, government users depend on fast, appropriately-secured and reliable networks, and expect to access services from anywhere, at any time, regardless of the demand and circumstances. With the growth of cloud-based services throughout the Government of Canada, ubiquitous access to appropriately-secured and high-quality network services has become even more important.

The current digital landscape resides on a highly complex system of network infrastructure that SSC inherited from departments and agencies (referred to as SSC's partners) when it was created 10 years ago. This infrastructure was aging, costly to maintain and unable to support modern services such as cloud, video and voice services. SSC has been investing to modernize the network through the development of standards, IT infrastructure and contracts consolidation, and technology simplification and standardization.

The recent COVID-19 pandemic resulted in a dramatic shift in the Government of Canada's network landscape, with the vast majority of government employees suddenly being forced to work from home. It is expected that employees will continue to work from home, or adopt a hybrid office/home work environment in the future. These factors—coupled with the migration toward software-defined networking and improved wireless technology (e.g., 5G)—have caused SSC to reassess how it delivers and secures its network services. A modernized approach, leveraging software-defined infrastructure and artificial intelligence (AI), provides both improved manageability and performance to enable the Government of Canada's cloud-first strategy. Now is the time to re-imagine the vision for the future of Enterprise Network Services.

What are partners asking for?

- **Network Access:** Users want a better user experience. To improve their experience, more network speed and capacity will enable them to perform their work more quickly and efficiently—SSC needs to provide users with an upgraded and modern network.

- **Cloud Access:** Partners want to accelerate the transition of applications to the cloud—SSC needs to provide more capacity for appropriately-secured cloud connectivity.

- **Mobility:** Users want to seamlessly connect to the network both at work and outside the office—SSC needs to ramp-up the delivery of wireless connectivity and improve the user experience of secure remote access (SRA) services.

- **Agility:** Partners want simpler processes and faster turnaround times to meet emerging requirements—SSC and partners need to plan ahead and automate and simplify the provisioning of new services.

2. A Vision for the Future

The digital vision of the Government of Canada requires a simple, agile, robust, efficient, reliable and appropriately-secured network infrastructure as a foundation to satisfy the expectations of both employee and Canadians.

SSC must implement and support a modern and appropriately-secured digital network to enable a positive user experience and Government of Canada enterprise-wide connectivity for multimedia communications and collaboration. SSC must also simplify governance, funding, project delivery and business intake processes to where Enterprise Network Services are viewed as a "utility" that can be quickly scaled up or down, on demand, with minimal administrative burden.

What are Enterprise Network Services?

In the simplest of terms, Enterprise Network Services are defined as a common set of services delivered to all partners, rather than customized services specific to a single partner. Key attributes of Enterprise Network Services include the following:

- **Consumption Standards**
  - ✓ Common service standards defined for different types of users in the government (e.g., scientists may be entitled to higher network speeds and bandwidth than administrators).
  - ✓ Standard service-level options available to meet specific circumstances (e.g., network speed uplifts for a disaster response).

- **Shared Infrastructure**
  - ✓ A shared infrastructure where multiple partners share the same hardware, software and physical network, but are separated logically in an appropriately-secure manner.

- **Product Standardization**
  - ✓ Limit the number of makes and models to realize large-volume purchase discounts, lower support costs and complexity, and ensure SSC support teams are knowledgeable and trained.
    - Standardize, typically, on one or two different vendor products for a specific component of the solution.

- **Security by Design**
  - ✓ The network is designed to be appropriately secured from the ground up and built to minimize flaws that could compromise security.
  - ✓ Networks designed in alignment with Communications Security Establishment Canada's Top 10 Security Mitigations to build and protect Government of Canada information and assets.

What do we mean by "Network as a Utility"?

The following are user-centric attributes that SSC has used to define "Network as a Utility":

- **Seamless Network Access**
  - ✓ Users should be able to connect securely, seamlessly and simply to their departmental network, the Internet or the Cloud at any time (e.g., a resilient, highly available network).
  - ✓ Users should be able to connect to the network via wireless connectivity in government locations.
  - ✓ Users should have adequate in-building coverage for cellular services wherever possible.
  - ✓ Network services must be scalable to meet time-sensitive increases and decreases in demand.

- **Anywhere, anytime, any government-approved device**
  - ✓ Users should be able to connect to applications in Enterprise Data Centres and "cloud-as-a-service" offerings in an appropriately-secure manner from home, while on the move (locally, nationally and internationally), or from a Government of Canada Workplace, at any time, from any government-approved device.

- **Access to Government of Canada Co-Working locations**
  - ✓ Users from any department should be able to go to a designated Government of Canada Co-Working location and connect to a network for security-controlled access to cloud applications, and departmental and government Enterprise IT resources.

- **Ability to use real time collaboration tools**
  - ✓ Users should be able to access and adequately use modern collaboration tools (e.g., Microsoft Office 365) to communicate and share information.

What key technologies will enable SSC to realize the Vision?

SSC has defined a Network and Security Vision (the Vision) for the future. The Vision identifies key technology enablers to modernize the current networking environment to support a digital government. The foundations of this Vision are based on software-defined networks (SDN), Zero Trust network architecture (ZTNA), next-generation wireless, Long Term Evolution (LTE) and 5G technologies, AI and continuous network monitoring.

SSC has developed the "Future GC Network and Security Vision" document which includes a technical overview of the foundations. The Vision will be available online in the near future.

A Network Strategy (the Strategy), which takes the Vision to the next level of detail, has also been drafted and will be available online in the near future. This Strategy is being updated as SSC consults with partners, central agencies and advisory firms. The Strategy will also evolve as SSC works with industry vendors as part of a collaborative procurement process to establish long-term contracting vehicles to implement new Enterprise Network Services.

3. Guiding Principles to Get There

To guide solutioning and procurement activities moving forward, the following principles have been developed.

- **Enterprise**—In alignment with SSC 3.0, a modern Government of Canada Enterprise Network will be based on enterprise standards and simple, common services delivered to all SSC partners.
- **Secure and Shared Infrastructure**—Implement a robust single physical network, with logical separation to meet partner data security requirements.
- **Automate and Simplify**—Implement automation, orchestration and self-service provisioning tools to remotely monitor and manage networks with enhanced visibility.
- **Incremental**—Network Modernization will be an evolution, starting small, using pathfinder approaches and agile procurement strategies to scale and at speed.

- **Standardization**—Limit the number of products to be integrated and supported to one or a very small number of vendors, depending on the underlying service or function. For each component of the network, a trade-off must be continually assessed:
  - ✓ Standardize to reduce interoperability costs and deliver maximum product capabilities such as automation, orchestration and remote management.
  - ✓ Ensure ongoing competition for better pricing and to mitigate the risk of vendor lock-in.
- **Technology Standards and Interoperability**—All solution components should strive to use a small number of supported makes and models, integrated together using interoperability standards to enable efficient and effective delivery of services to users. SSC will evolve more to this approach as industry publishes open, interoperability standards for emerging technologies.
- **Enterprise Procurement Vehicles**—As network services are modernized, new supporting enterprise procurement vehicles are to be established via competitive processes.
- **Exceptions**—There will be situations where an urgent solution is required to meet a critical business need of a partner. Standard escalation and governance processes must be followed in these situations, including independent third-party reviews when applicable.
- **Commercial Networks**—Whenever possible, commercial networks (e.g., the Internet) should be leveraged for government network traffic.
- **Talent Management**—To deliver on Network Modernization, SSC must develop appropriate talent management strategies to deliver, manage and support the future-state network.

4. The Solution Components Defined

The delivery of Government of Canada Enterprise Network Services can be broken down into multiple sets of products and services, each with its own procurement and service delivery strategy. This approach lowers overall risk to the government by delivering incremental changes in a managed and coordinated manner.

The Government of Canada Enterprise Network is defined by the components below. Refer to Annex A for a graphical representation of the network, aligned to the numbering scheme below.

<u>Networking Equipment and Support Services</u>

1A) In-Building Networks—Network Services for government buildings and other places of work for GC users. These services include local area networks (LAN) (i.e. LAN / software-defined wide area networks [SD-WAN] / Wi-Fi) and other network access services (e.g., wired or wireless LTE/5G access to the nearest point of presence or core network interface point).

1B) WAN / SD-WAN—Network Services to connect government buildings with Government of Canada data centres, the cloud and the Internet. This also includes the infrastructure and toolsets required to enable SSC to remotely monitor and manage the end to end network using automation, orchestration, and artificial intelligence. SD-WAN will also enable SSC to logically separate departmental networks on the same physical network infrastructure.

1C) Remote Access—Virtual Private Network (VPN) infrastructure and services to provide remote access services to government users (e.g., to work from home in an appropriately secure fashion).

2) GC Backbone (Optical Services)—The GC Backbone is an SSC-owned and managed high-speed network connecting departmental networks, Government of Canada data centres, the cloud and the Internet. High-speed optical network services include components such as fibre optic cable, optical switches, optical multiplexers/demultiplexers, optical amplifiers and optical splitters.

3) Internet Connectivity—These are appropriately-secured, high-speed connections between the GC Backbone and the Internet.

4) Cloud Connectivity—These are highly secure connections between the GC Backbone and the cloud. All government data and applications connect to the "outside world" through these appropriately-secured and closely monitored access points.

5) Data Centre Network (DCN) —DCN is high speed networking infrastructure used within Government of Canada data centres—analogous to a LAN in a building, but with much faster speeds, more reliability and greater functionality.

Connectivity and Networking Bandwidth Services

These services connect the equipment described above. The following are examples:

Core Network Services—WAN services that interconnect In-Building Networks and/or other Core Network Services. These services are delivered by large Canadian Telecommunications Providers (Telco). Multiprotocol Label Switching (MPLS) is an example of a Core Network Service.

Dark Fibre—"Unlit" fibre optic cables.

Satellite Services—Services that connect users in remote locations to government networks in an appropriately-secure manner using commercially-available satellite services.

5. The Strategy Moving Forward

SSC is currently designing the future state solution and establishing corresponding contracting vehicles, including the five streams of the recently launched Government of Canada Network Services (GCNS) procurement process. SSC will establish technology standards through open, competitive procurements, and will provide boundaries for these standards that encourage competition while keeping operational burden in check. The standards will be put in place for the useful life of the equipment purchased.

Given that many technology foundations in the Vision are new to the government, and must be integrated into the existing networking infrastructure, various industry engagements are planned as SSC develops these strategies. As part of this process, SSC will define standards for various segments of the network, leveraging the best practices from other peer-size enterprises.

In the meantime, SSC continues to procure products and services to maintain current network services. For short term requirements, procurements must be aligned to the vision, and the following product selection approach is being followed:

- If there is no interoperability requirement then SSC will complete a competitive procurement (often referred to as a generic procurement).
- If there is an interoperability requirement, then SSC will procure a like-for-like solution that is competed among resellers. These exceptions must have technology constraints and quantified business impacts documented, and be reviewed and approved on a case-by-case basis.

The solution's component-specific strategies are described at a high level in the following table, and are aligned with the guiding principles described in the previous section. For each component, the following is provided:

- What products and contracts were inherited from partners 10 years ago when SSC was created?
- What key solution development and procurement activities have occurred in the past 10 years since SSC has taken over service delivery?
- What is the installed base? Refer to Annex B for additional information on the historical and current installed base.
- Where are we going with the service from a solution-development and procurement perspective?

Component	What did SSC inherit?	What has SSC done for the past 10 years?	Where is SSC going? (Notional procurement approach)
In-Building Networks	LAN—SSC inherited a range of LAN switches and router brands from vendors, with Cisco making up the majority of the installed base.	LAN—SSC typically replaced LAN equipment on a like-for-like basis as part of the equipment refresh process. Over the past few years, SSC ran competitive procurements for large Real Property (RP) projects, such as Lester B Pearson Refit, Carling Campus and MPLS routers for Employment and Social Development Canada. SSC currently has equipment from Cisco, Juniper, Extreme Networks, Ruckus Networks and Hewlett Packard Enterprise (HPE).	SSC has recently completed a generic LAN inventory procurement that was openly competed last fiscal year and awarded to Ruckus Networks. The current platform based on Ruckus will be implemented for approximately 3 years for smaller RP re-fit initiatives. For any new, large-scale RP initiatives, SSC will compete the in-building LAN requirements as a generic product procurement. SSC is just completed a generic LAN inventory procurement to replace existing, aging LAN equipment. Juniper Networks is the winning original equipment manufacturer.
	Wi-Fi—There were limited Wi-Fi deployments 10 years ago. There were some early implementations of Cisco and Motorola that SSC inherited.	Wi-Fi—Using a competitive procurement process, SSC has standardized on the HPE Aruba platform.	Wi-Fi—Transition period to start summer 2021 from the current WLAN contract to the Network Solutions Supply Chain (NSSC) procurement vehicle for future procurements.
	WAN Optimizers—SSC inherited only Riverbed WAN Optimizers.	WAN Optimizers—SSC continued to use the Riverbed product suite for compatibility purposes, completed among resellers.	The long term procurement strategy for Enterprise Network Services is to establish a standing offer for In-Building Network Services with multiple suppliers and/or a supply arrangement for combined Network Access and LAN services. A competitive procurement (under GCNS) will occur over the next 6-12 months.

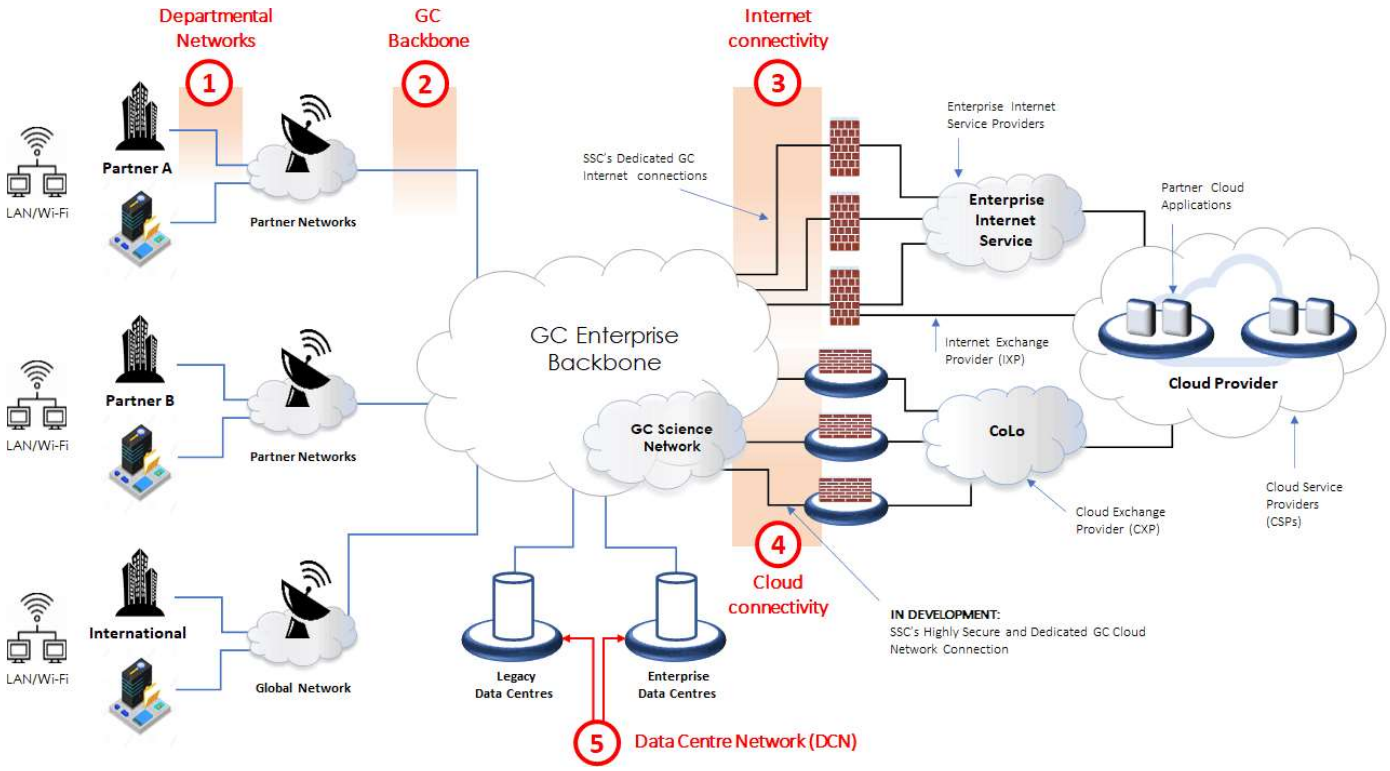
Component	What did SSC inherit?	What has SSC done for the past 10 years?	Where is SSC going? (Notional procurement approach)
WAN / SD-WAN	SSC inherited Cisco customer edge (CE) WAN routers from partners. SD-WAN was not in use when SSC was created.	SSC typically replaced WAN routers on a like-for-like basis for compatibility purposes. In recent years, SSC has completed lab tests and pilots using WAN equipment from other vendors (e.g., Juniper). SSC is researching and piloting a range of SD-WAN products and technologies as this will be a foundational component of a modern network for the government.	SSC currently in open competition for a generic CE WAN router procurement to replace existing, aging CE routers. The winning vendor(s) must provide products that are interoperable with the current installed base. The long-term procurement strategy is to establish an enterprise contract with a service provider through a competitive procurement to occur over the next 6-12 months (under GCNS). Software-defined network services will gradually be incorporated to increase network visibility, flexibility, reliability, security and cost effectiveness.
SRA	SSC inherited a wide range of department-specific remote access products and services, leveraging equipment from multiple vendors, but primarily from Cisco.	SSC retired many legacy solutions, and moved a number of departments to a managed Remote Access Service (GCSRA), a competitively-procured managed service through Bell Canada (Bell selected Cisco equipment to provide the service). The SSC-managed solution for non-GCSRA departments is based on Cisco and Fortinet products, as was inherited by SSC.	The SRA service will be replaced with a new enterprise service, through the Secure Remote Access Migration (SRAM) project. An active procurement for equipment and services is currently in progress for SRAM. Implementation will be carried out over the next 1-3 years.

Component	What did SSC inherit?	What has SSC done for the past 10 years?	Where is SSC going? (Notional procurement approach)
GC Backbone	SSC inherited primarily Cisco and Ciena equipment from partners.	In the early years of SSC, there was limited investment in this space, and as such SSC typically replaced equipment on a like-for-like basis for compatibility purposes. In recent years there has been increased demand for these services given requirements for workload modernization. SSC has been researching and piloting alternative options in this space to define long term requirements and develop the solution and procurement strategy. In the meantime, to keep up with key business imperatives, SSC has continued to procure Cisco.	The long term procurement strategy is to establish supply arrangement(s) with multiple qualified vendors. Competitive procurement (under GCNS) to occur over the next 12-18 months.

Component	What did SSC inherit?	What has SSC done for the past 10 years?	Where is SSC going? (Notional procurement approach)
Cloud / Internet Connectivity	Each Partner invested in their own Internet Connectivity solutions before SSC was created. Typically, Cisco or McAfee equipment was used. For Perimeter Services (firewall, web filtering and load balancers), a range of solutions from Cisco, Citrix, Radware, McAfee, BlueCoat, Forcepoint and Trend Micro were inherited by SSC.	SSC typically replaced equipment on a like-for-like basis for compatibility purposes. In 2015–2016, SSC completed a competitive procurement to replace the department-specific firewall equipment through the IT Refresh project. A contract was awarded to Fortinet, and most firewalls were migrated to this technology as they reached end of support. More recently, Juniper has been awarded contracts for Internet and cloud connectivity solutions. The Enterprise Perimeter Services (EPS) project recently ran a competitive procurement. The Fortinet and A10 platform was selected.	Firewalls—Complete a generic product procurement via a competitive process in summer 2021. Enterprise Perimeter—Leverage the competitive contract awarded to Fortinet and A10. Cloud and Internet Connectivity—Leverage existing contracts and compete new ones as necessary.
DCN	SSC inherited a range of makes and models of DCN switches from 2-3 vendors, with Cisco making up the majority of the installed base. SSC inherited a range of data centre Load Balancers from 4-5 vendors, with F5 making up the majority of the installed based.	SSC developed a strategy to reduce the data centre's footprint in the Government of Canada to a small number of Enterprise Data Centres (EDC). For compatibility and ease-of-integration purposes, SSC determined that a single DCN solution would be used in the overall EDC blueprint. Cisco and F5 were selected given the investments already made in equipment, training and solution integration.	The strategy is to continue to leverage Cisco and F5 products given the investments made to date, and for interoperability and service operations requirements. For the refresh of existing EDCs, or for net-new EDCs, by pair (active and back-up), SSC will complete a competitive procurement process. This strategy is being reviewed by independent analysts and will be updated as applicable.

Component	What did SSC inherit?	What has SSC done for the past 10 years?	Where is SSC going? (Notional procurement approach)
Core Network Services	Several department-specific contracts were inherited, the largest, and longest running were GENS (Employment and Social Development Canada) and GDNS (Department of National Defence).	SSC consolidated contracts where possible, and awarded multiple contracts to different providers for Core Network Services throughout the country and around the world.	Long-term contract(s) with multiple suppliers, with little-to-no minimum commitment. Competitive procurement to occur over the next 12-18 months.
Dark Fibre Services	A small number of departmental Leased Dark Fibre contracts were inherited.	SSC consolidated the contracts, and established a long term Leased Dark Fibre Services contract for the government. This contract is expiring in the near future.	Long-term contract(s) to be established. Competitive procurement to occur over the next 6-12 months.
Satellite Services	A small number of enterprise and departmental satellite services contracts were inherited by SSC.	SSC consolidated the contracts, and established a series of Enterprise Satellite Services contracting vehicles (one for each type of satellite service).	Enterprise contracting vehicles for specific satellite services will continue to be re-competed at the appropriate time (e.g., to enable timely migration of services to the new contracts).

Annex A—Conceptual Architecture of the Government of Canada Network



1 – Departmental Networks—WAN, LAN (Wi-Fi, routers, switches, hubs) and SRA systems specific to a department. Includes network management tools to manage, monitor, automate, remediate and provision networking capabilities (e.g., SD-WAN).

2 – GC Backbone—Network infrastructure that connects departmental networks to data centres, the cloud and the Internet.

3 – Internet Connectivity—Secure, monitored connections to the Internet.

4 – Cloud Connectivity—Secure, monitored connections to Cloud Service Providers.

5 – Data Centre Network—Network that connects users to applications, servers and storage within a data centre, and also interconnects data centres for availability and disaster recovery purposes.

Annex B—Installed Base Metrics (approximations based on historical purchases)

Component	What did SSC Inherit?	What is the current installed base?
In-Building Network—LAN	Cisco Avaya HPE	Cisco Extreme Networks (previously Avaya) Ruckus Juniper HPE
In-Building Network—Wi-Fi	Cisco Motorola (Note: there was a small install base at that time)	HPE Extreme Networks (previously Motorola) Cisco
In-Building Network—WAN Optimizers	Riverbed	Riverbed
WAN—CE Routers	Cisco	Cisco Juniper
SRA	Bell Managed Service Cisco Fortinet	Bell Managed Service Cisco (SSC managed) Fortinet (SSC managed)
GC Backbone Optical	Cisco Ciena	Cisco Ciena/Nortel-Optera
Cloud / Internet Connectivity—Network Connectivity	Cisco (IIS) Miscellaneous vendors	Cisco Juniper A10
Cloud / Internet Connectivity—Perimeter Services	Cisco Miscellaneous vendors	Fortinet Cisco Symantec Others
DCN Switches	Cisco Avaya	Cisco Juniper Extreme Networks (previously Avaya)
DCN Load Balancers	F5 Radware Citrix Cisco Barracuda	F5 Citrix A10