Canadian Radio-television and Telecommunications Commission
Conseil de la radiodiffusion et des télécommunications canadiennes
Canada

Assessment of Rogers Networks for Resiliency and Reliability Following the 8 July 2022 Outage – Executive Summary

December 12, 2023

REPORT SUBMITTED BY: Xona Partners Inc.

Xona Partners Inc.
2969 Sable Ridge Drive, Ottawa, Ontario K1T 3S3, Canada
www.xonapartners.com

ISBN: 978-0-660-69963-9
Catalogue number: BC92-130/2-2024E-PDF

Assessment of Rogers Networks for Resiliency and Reliability Following the 8 July 2022 Outage

A report by Xona Partners Inc.

December 2023

Executive Summary

Overview

In the early morning of 8 July 2022, Rogers Communications Inc. (Rogers) experienced a major service outage in its Internet Protocol (IP) core network that affected its wireless and wireline services across Canada (July 2022 outage). The July 2022 outage lasted from 4:58 EDT on 8 July 2022 to 7:00 EDT on 9 July 2022 as services were gradually restored. More than 12 million customers lost wireless and wireline services, including mobile subscribers, home Internet users, corporate customers, and institutional customers that provide critical services (e.g., Interac e-Transfer and electronic payment services).

This report details the results of an independent assessment of the Rogers network architecture for reliability and resiliency[1], as well as the processes in place at Rogers to manage network changes (change management process[2]) and respond to network incidents like outages (incident management process[3]) as these processes were central to the July 2022 outage.

In this report we detail the findings for the period before and during the outage and outline the measures that Rogers has since implemented to address deficiencies in its network design and processes. This report is primarily based on an extensive independent review of the Rogers responses to multiple rounds of questions and meetings with the Rogers technical and management staff during this assessment, as well as information Rogers provided in response to the CRTC's request for information (RFI) after the outage.

[1] Reliability is a measure of the ability of the network to deliver services according to their design specifications. Resiliency is a measure of how the network responds to minimize the impact of failures and the speed at which it recovers from disruptions.
[2] Change management process is a systematic approach to managing network infrastructure and service changes. It is a process that is designed to minimize the risk of service disruptions and to ensure that changes are controlled and implemented efficiently.
[3] Incident management process is a systematic approach to identifying, responding to, and resolving incidents that affect network services. It is designed to minimize the impact of incidents on users by restoring normal service as quickly as possible.

Description of the outage

Background. For context, Rogers operates wireless and wireline networks that share a common IP core network, as shown in a simplified form in Figure 1. The core network is part of the telecommunications network that is responsible for aggregating and routing data traffic both internally within the Rogers network and externally with the Internet and other service providers. Hence, for Rogers, both wireless and wireline data traffic is processed by the same IP core network. In the weeks leading to the day of the outage on 8 July 2022, Rogers was executing on a seven-phase process to upgrade its IP core network. The outage occurred during the sixth phase of this upgrade process.

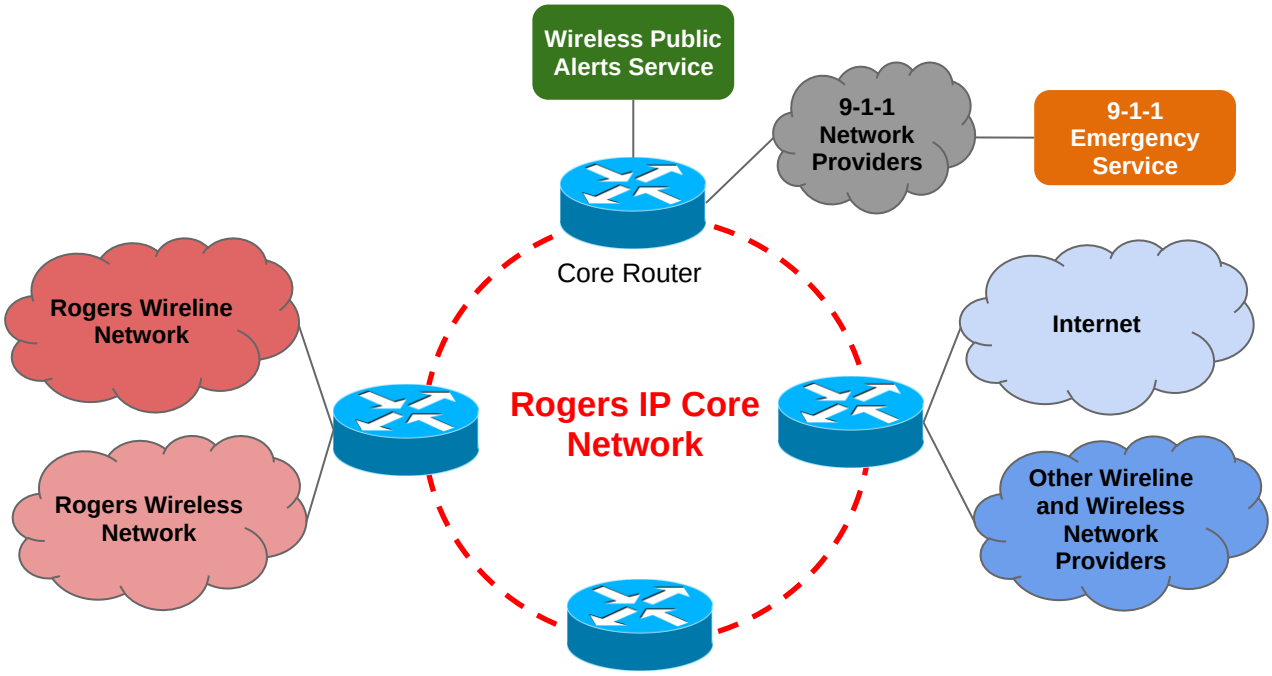

Figure 1 A simplified topology of Rogers' network architecture.

Root cause of the network failure. The July 2022 outage is attributed to an error in configuring the distribution routers[4] within the Rogers IP network. Rogers staff removed the Access Control List[5] policy filter from the configuration of the distribution routers. This consequently resulted in a flood of IP routing information into the core network routers, which triggered the outage. The core network routers

[4] A distribution router is a router that directs traffic between the access layer which connects users to the network, and the core network which aggregates all the network traffic.

[5] An Access Control List in a router is a table that provides the rules on how the router ought to manage the packet traffic. The Access Control List is described as a policy filter because it defines what traffic will pass through the router and how it will be directed based on the set of rules (filters).

allow Rogers wireline and wireless customers to access services such as voice and data. The flood of IP routing data from the distribution routers into the core routers exceeded their capacity to process the information[6]. The core routers crashed within minutes from the time the policy filter was removed from the distribution routers configuration. When the core network routers crashed, user traffic could no longer be routed to the appropriate destination. Consequently, services such as mobile, home phone, Internet, business wireline connectivity, and 9-1-1 calling ceased functioning.

Absence of router overload protection. The July 2022 outage exposed the absence of overload protection on the core network routers. The network failure could have been prevented had the core network routers been configured with an overload limit that specifies the maximum acceptable number of IP routing data the router can support. However, the Rogers core network routers were not configured with such overload protection mechanisms. Hence, when the policy filter was removed from the distribution router, an excessive amount of routing data flooded the core routers, which led them to crash.

Deficiency in the change management process. The configuration error, which led to the removal of the policy filter from the configuration of the distribution routers, is the result of a change management oversight by Rogers staff. Rogers staff deleted the policy filter that prevented IP route flooding in an effort to clean up the configuration files of the distribution routers. The change management process, which includes audits of change parameters, failed to flag the erroneous configuration change.

As stated above, this configuration change was the sixth phase of a seven-phase network upgrade process that had begun weeks earlier. Before this sixth phase configuration update, the previous configuration updates were completed successfully without any issue. Rogers had initially assessed the risk of this seven-phased process as "High." However, as changes in prior phases were completed successfully, the risk assessment algorithm downgraded the risk level for the sixth phase of the configuration change to "Low" risk, including the change that caused the July 2022 outage. The Low risk assessment resulted in Rogers staff not being required to conduct additional scrutiny, go through higher levels of approvals, and conduct laboratory testing for this configuration change. Downgrading the risk assessment to "Low" for changing the Access Control List filter in a routing policy contravenes industry norms, which require high scrutiny for such configuration changes, including laboratory testing before deploying in the production network.

[6] Rogers stated that about 10,000 routes are advertised into the core router when the Access Control List policy filter is present on the distribution router. When this policy filter was removed, a single distribution router released over 900,000 route data into the core routers.

Reliability of Rogers network architecture

The Rogers network is a national Tier 1 network and is architecturally designed for reliability; it is typical of what would be expected of such a Tier 1 service provider network. The July 2022 outage was not the result of a design flaw in the Rogers core network architecture. However, with both the wireless and wireline networks sharing a common IP core network, the scope of the outage was extreme in that it resulted in a catastrophic loss of all services. Such a network architecture is common to many service providers and is an example of the trend of converged wireline and wireless telecom networks. It is a design choice by service providers, including Rogers, that seeks to balance cost with performance.

Factors affecting network restoration

Network management infrastructure. A management network provides access to critical infrastructure sites or equipment in a network to enable troubleshooting and repair. At the time of the July 2022 outage, Rogers had a management network that relied on the Rogers IP core network. When the IP core network failed during the outage, remote Rogers employees were unable to access the management network. Moreover, Rogers did not provision its network operation centre and other critical remote infrastructure sites with redundant connectivity from alternative service providers for network management. This limited access to critical network equipment during the July 2022 outage for troubleshooting and root cause analysis. Rogers had to dispatch staff to remote sites to physically access the affected routers, which delayed network recovery efforts. In our assessment, network resiliency demands that telecom network operators have secure alternative access to crucial remote network elements that is not dependent on the data network. Both the inability of Rogers remote staff to access the management network and the absence of backup connectivity from alternative service providers to the network operation centre and other critical remote sites contributed to prolonging the July 2022 outage.

Limited communication among Rogers staff. Rogers staff relied on the company's own mobile and Internet services for connectivity to communicate among themselves. When both the wireless and wireline networks failed, Rogers staff, especially critical incident management staff, were not able to communicate effectively during the early hours of the outage. Rogers had to send Subscriber Identity Module (SIM) cards from other mobile network operators to its remote sites to enable its staff with wireless connectivity to communicate with each other. The absence of sufficient alternative means of communication slowed the Rogers response to the July 2022 outage.

Timely access to critical information for network recovery. A lack of information hampered the Rogers incident management process. Rogers staff did not initially have access to the error logs from the failed routers and could not pinpoint the root cause for about 14 hours from the start of the outage. Additionally, Rogers had completed multiple configuration changes during the

maintenance window on the day of the outage. This adversely impacted outage recovery efforts, making it difficult to decide which network change ticket to roll back. These two factors contributed to misdiagnosing the root cause of the network failure in the initial hours of the July 2022 outage. However, once the root cause was identified, network restoration activities commenced methodically, and services were gradually restored.

Measures taken by Rogers to improve its network reliability and resiliency

Addressing the outage root cause and deficiencies in the management network architecture. In the months following the July 2022 outage, Rogers undertook a series of measures and initiatives to address the critical deficiencies that the outage exposed. Most importantly, Rogers implemented safeguards in the configuration of the routers in its core network to prevent the flooding of IP routing data, thus preventing a similar outage from happening in the future. Rogers also implemented a separate physical and logical management network to access network elements for troubleshooting and root cause analysis. Additionally, Rogers deployed backup connectivity from third party service providers to its network operation centre and other critical remote infrastructure sites, and invested in tools that would help validate router configuration changes.

Separate IP core for the wireless and wireline networks. Following the outage, Rogers announced it had decided to separate the IP core network for its wireless and wireline networks. This decision entails deploying a new IP core for the wireless network, while the existing IP core would remain to serve the wireline network. Therefore, if one IP core network were affected by an outage, the other IP core network would remain unaffected and operational.

Rogers has not yet finalized the implementation of the IP core network separation, which remains a work in progress. When implemented, separate IP core networks for the wireless and wireline networks will help to contain a failure to its respective access network and, therefore, avoid the type of catastrophic network failure experienced in the July 2022 outage, where both wireless and wireline services were unavailable due to the outage in the common core IP network. IP core network separation would improve the overall resiliency of the Rogers wireless and wireline networks.

Improving the change management process. Following the July 2022 outage, Rogers made several improvements to its change management process. These improvements included a new risk assessment algorithm; organizational changes to improve collaboration between network operations and engineering teams; an enhanced process for introducing new equipment and technology; improvements in implementing network changes such as introducing automation to streamline the change management process; and additional lab testing of planned network configuration changes.

Improving the incident management process. Following the July 2022 outage, Rogers made improvements to its incident management process, to include bolstering its incident management guidelines to encompass various outage scenarios; streamlining its incident response with well-defined leadership roles; implementing a solution for prioritization of alarms during outage; enhancing automated rollbacks to previous configurations when new changes are not successful; and implementing additional measures to improve its communication protocols. Rogers has also equipped all incident response and crisis management team members with backup communications from third party service providers to maintain communication capabilities during outages.

Assessment and recommendations to Rogers

Our overall assessment is that the combination of measures that Rogers undertook after the July 2022 outage are satisfactory to improve the Rogers network resiliency and reliability as well as to address the root cause of the July 2022 outage.

Diligence in implementing the improved change management processes would be the most effective way to avoid a similar outage from occurring in the future. Enhancements to the incident response processes would improve the Rogers response to enable a faster service recovery if network failure occurs. We have several recommendations for additional measures that Rogers could undertake to further improve its network resiliency. These recommendations are:

1. Test emergency roaming with other mobile network operators and expand it to include a more comprehensive set of test scenarios. Rogers has signed the Memorandum of Understanding on Telecommunications Reliability, which includes emergency roaming with other mobile network operators to enable Rogers customers to access emergency services (e.g., 9-1-1 calls) during a major outage. This additional testing would ensure that emergency roaming is feasible under different network failure scenarios; specifically, the scenario observed during the July 2022 outage (wherein the radio network was up and the core network was down).

2. Develop a detailed root cause analysis for future major outages. This would benefit the process of assessing an outage and its impact, as well as identifying the appropriate mitigation measures.

3. Ensure wide coverage and rigor in testing configuration changes. This would help avoid errors leading to potential outages. Rogers would need to leverage new test tools for modeling test scenarios that replicate the production network, and to address the evolution of networking technologies.

4. Expand the scope of incident management drills. This would enhance staff and network’s emergency preparedness and proactively uncover weaknesses.

5. Institutionalize learning from its own and other service providers' network failures to implement preventive actions, minimize the impact of network outages, and enhance quality of service.
6. Inform customers how to reach 9-1-1 services during an outage.
7. Share outage root cause and mitigation strategies with the broader Internet community (represented by bodies such as the North American Network Operator's Group), to help other telecom network operators prevent similar network failures.

Recommendations to telecom network operators

Lessons learned from the July 2022 outage. A summary of the important lessons learned from the July 2022 outage includes:

1. Implement router overload protection in the IP core and distribution networks.
2. Separate the network management layer physically and logically from the data network.
3. Provide the network operation centre and other critical remote sites with a secure backup connectivity from third-party telecom network operators.
4. Ensure that the audit process for network configuration changes is effective and involves different teams within the organization, such as engineering, operations, and project management. It is also advisable to involve equipment vendors where the configuration changes pertain to critical infrastructure, such as the IP core network.
5. Conduct lab tests of planned configuration changes and ensure that the lab equipment and test scenarios accurately reflect the production network.
6. Carefully manage the number of configuration changes completed in a single maintenance window and leverage tools and processes for automatic rollback of configuration parameters.
7. Implement an automated alarm prioritization solution to suppress unnecessary alarms for every type of change and to allow staff to focus on the important alarms.
8. Provide critical staff with secondary means to communicate, such as SIM cards from third-party network operators.
9. Simulate and practice network failure and outage scenarios to uncover deficiencies in the network architecture and the incident management process.

Evolving telecom network trends. There are evolving telecom network trends that impact network reliability and resiliency. These include the evolutions towards

telecom public cloud platforms, network softwarization and virtualization, the increased use of Artificial Intelligence in network automation, readiness for post-quantum cybersecurity, and the convergence of terrestrial and non-terrestrial networks. Canadian telecom service providers are in the process of incorporating some of these trends into their network evolution. We highlight a few technological and process recommendations that would strengthen network resiliency in the face of such evolutionary network trends. These recommendations include:

1. Technological recommendations:

    A. Leverage emerging non-geostationary orbit satellite constellations (e.g., low earth orbit satellite constellations) to provide remote sites with backup connectivity and consider emerging direct-to-cell constellations for emergency 9-1-1 calling.

    B. Track and prepare to implement disaster roaming standards that are currently being planned in the 3rd Generation Partnership Project (3GPP) standard setting body.

    C. Consider using over-the-top messaging applications as an alternative communication method, including emergency services. This would be useful in case of failures in some critical systems, such as the IP Multimedia System.

    D. Leverage dynamic software-based SIM technologies, which provide various levels of programmability and allow new roaming models to alternative providers in case of major outages.

    E. Consider and work towards the applicability of emergency spectrum and capacity-sharing techniques to mitigate the impact of network failures. These techniques temporarily and dynamically increase network capacity to accommodate roaming users.

    F. Consider collaborating with content delivery networks and over-the-top application providers to define specific interaction models during emergencies. For example, dynamic traffic management allows content providers to adapt their behaviour based on feedback from telecom operators.

    G. Consider offering critical infrastructure service providers secondary options for redundant connectivity services.

2. Process recommendations:

    A. Implement incident response training and drills to uncover weaknesses in architecture, operations, and business processes that adversely impact outage recovery efforts.

B. Implement incident management response key performance indicators to benchmark the incident response effort and improve its effectiveness.

C. Designate clear roles and responsibilities for personnel to better respond to network outages.

D. Consider calculating the cost impact of a network outage to help mitigate the consequences of incidents through decision-making on resource allocation and communication with stakeholders to preserve brand-image and financial stability.

E. During an outage, service providers are advised to remind and inform the public on how to access emergency calling and public alerts services.

Glossary

9-1-1 Network Provider	The 9-1-1 Network Provider is the incumbent local exchange carrier that provides 9-1-1 emergency response service to the local authority pursuant to a tariff and/or agreement. The 9-1-1 network provider's tariff and/or agreement makes access to 9-1-1 emergency calling available to the end-users located within the serving area.
Access Control List policy filter	An Access Control List policy filter in a router is a table that provides the rules on how the router ought to manage the packet traffic. The Access Control List is described as a policy filter because it defines what traffic will pass through the router and how it will be directed based on the set of rules (filters).
Border Gateway Protocol (BGP)	Border Gateway Protocol is an exterior gateway routing protocol that enables the exchange of route information among routers in different autonomous systems, for the purpose of selecting the best path for data packets.
Core router	A core router is a router in the core network, or layer, of an IP network.
Change management process	Change management process is a systematic approach to managing network infrastructure and service changes. It is a process that is designed to minimize the risk of service disruptions and to ensure that changes are controlled and implemented efficiently.
Distribution router	A distribution router is a router in the distribution layer of a telecommunications service provider’s IP network. It sits between the access layer that connects end users to the network and the core layer that aggregates all the network traffic.
Domain name server	A domain name server is like an address book for the Internet. A domain name server translates user-friendly web addresses (like www.rogers.com) into numerical Internet Protocol addresses.

Incident management process	Incident management process is a systematic approach to identifying, responding to, and resolving incidents that affect network services. It is designed to minimize the impact of incidents on users by restoring normal service as quickly as possible.
Incumbent Local Exchange Carrier (ILEC)	The Incumbent Local Exchange Carrier is the 9-1-1 network provider in the context of this report.
Intermediate System to Intermediate System	Intermediate System to Intermediate System is an interior gateway routing protocol that enables the exchange of route information among routers within an operator's network for the purpose of selecting the best path for data packets. It is a similar type of protocol to OSPF.
National Alert Aggregation and Dissemination (NAAD) System	The National Alert Aggregation and Dissemination System accepts emergency alerts from authorized government agencies which are then made available to broadcasters and other media distributors who voluntarily distribute them to the Canadian public. Pelmorex Communications Inc. is designated as Canada's aggregator and disseminator of emergency public alert messages.
National Public Alerting System (NPAS)	The National Public Alerting System is a Federal, Provincial, and Territorial system that provides emergency management organizations throughout Canada with the capability to warn the public about imminent or unfolding hazards.
Open Shortest Path First (OSPF)	Open Shortest Path First is an interior gateway routing protocol that enables the exchange of route information among routers within an operator's network for the purpose of selecting the best path for forwarding data packets.
Originating Network Provider	The network which originates a 9-1-1 call. Includes the access network and the calling network. Typically operated by carriers or other service providers.
Over-the-top	Over-the-top messaging is a messaging service offered by an application that is typically agnostic to the telecom service

messaging	provider and runs independently from it. For example, services such as WhatsApp, Signal, Telegram, WeChat, and others are over-the-top messaging services, unlike short message service and multimedia messaging service, which are technologies built into the cellular technology (e.g., GSM, 3G, or LTE).
Production network	Production network is a common term used by service providers to distinguish active network elements from those used in a laboratory environment. Production, in this context, means processing customer traffic in a live environment.
Public Safety Answering Point (PSAP)	An answering location for 9-1-1 calls originating in a given area. A PSAP may be designed as Primary or Secondary, which refers to the order in which calls are directed for answering. Primary PSAPs respond first. This is a communications facility that is open 24 hours a day, 365 days a year, and is responsible for redirecting or transferring emergency calls to Secondary PSAPs that receive calls on a transfer basis only, and generally serve as a centralized answering location for a particular type of emergency call. Secondary PSAPs are staffed by employees of service agencies such as police, fire, or emergency medical agencies or by employees of a common bureau serving a group of such entities.
Routers	Routers are networking devices that receive and forward data packets in IP networks. Routers direct traffic within networks or between networks.
Routing protocol	A routing protocol specifies how routers forward packets from a source to a destination. Routing protocols are grouped into two major categories: interior gateway protocols and exterior gateway protocols. Interior gateway protocols are designed to work within an autonomous system—a network administratively controlled by a single organization. External gateway protocols are designed to manage the transfer of information between autonomous systems.

Acronyms

API	Application Programming Interface
BGP	Border Gateway Protocol
BRI	Base Risk Index
BSS	Business Support Systems
CRMS	Capacity, Reliability, Mandatory Safety and Service (Access Network)
CRTC	Canadian Radio-television and Telecommunications Commission
CSTAC	Canadian Security Telecommunications Advisory Committee
DGW	Distribution Gateway
DNS	Domain Name System
DOCSIS	Data Over Cable Service Interface Specifications
EDT	Eastern Daylight Time
FCC	Federal Communications Commission
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
IPv4	IP Version 4
IPv6	IP Version 6
ISED	Innovation Science and Economic Development (Ministry of)
ISP	Internet service providers
KPI	Key Performance Indicator
LTE	Long Term Evolution
MPLS	Multiprotocol Label Switching
MVPN	Multicast Virtual Private Network
NAAD	National Alert Aggregation and Dissemination System
NCT	Network Change Ticket
NIST	National Institute of Standards and Technology
NOC	Network Operation Centre
NPAS	National Public Alerting System
NPI	New Product Introduction
NTI	New Technology Introduction
OSPF	Open Shortest Path First
OSS	Operational Support Systems
PKI	Public Key Infrastructure

PSAP	Public Safety Answering Point
RCMIN	Rogers Communications Management IP Network
RFC	Request for Comments
RFI	Request for Information
SD-WAN	Software-Defined Wide Area Network
SIM	Subscriber Identity Module
SLA	Service Level Agreement
TSP	Telecommunications Service Provider
VPN	Virtual Private Network