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

Évaluation de la résilience et de la fiabilité du réseau de Rogers liée à la panne du 8 juillet 2022 – Sommaire exécutif

Le 12 Décembre 2023

RAPPORT SOUMIS PAR : Xona Partners Inc.

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

ISBN : 978-0-660-69965-3
Catalogue No. : BC92-130/2-2024F-PDF

Évaluation de la résilience et de la fiabilité du réseau de Rogers liée à la panne du 8 juillet 2022

Un rapport de Xona Partners Inc

Décembre 2023

Résumé

Aperçu

Au petit matin du 8 juillet 2022, Rogers Communications Inc. (Rogers) a connu une panne de service majeure dans son réseau central de protocole Internet (IP) qui a touché ses services sans fil et filaires partout au Canada (panne de juillet 2022). La panne de juillet 2022 a duré du 8 juillet 2022 à 4 h 58 HAE au 9 juillet 2022 à 7 h HAE, lorsque les services ont été progressivement rétablis. Plus de 12 millions de clients ont perdu des services sans fil et filaires, notamment des abonnés mobiles, des utilisateurs d'Internet à domicile, des entreprises et des clients institutionnels qui fournissent des services essentiels (p. ex., Interac e-Transfer et des services de paiement électronique).

Ce rapport présente en détail les résultats d'une évaluation indépendante de la fiabilité et de la résilience de l'architecture du réseau de Rogers[1], ainsi que les processus en place chez Rogers pour gérer les changements de réseau (processus de gestion des changements[2]) et répondre aux incidents de réseau tels que les pannes (processus de gestion des incidents[3]), car ces processus ont joué un rôle central dans la panne de juillet 2022.

Dans ce rapport, nous présentons en détail les résultats obtenus avant et pendant la panne et nous décrivons les mesures que Rogers a mises en œuvre depuis lors pour remédier aux lacunes dans la conception de son réseau et dans ses processus. Ce rapport est principalement basé sur un examen indépendant approfondi des

[1]La fiabilité est une mesure de la capacité du réseau à fournir des services conformément aux spécifications prévues. La résilience est une mesure de la manière dont le réseau réagit pour réduire l'incidence des défaillances et de la vitesse à laquelle il se remet des perturbations.

[2]Le processus de gestion du changement est une approche systématique de la gestion des modifications de l'infrastructure et des services du réseau. Il s'agit d'un processus conçu pour réduire le risque d'interruption des services et pour garantir que les changements sont contrôlés et mis en œuvre de manière efficace.

[3]Le processus de gestion des incidents est une approche systématique du recensement, de la réponse et de la résolution des incidents qui touchent les services du réseau. Il est conçu pour réduire l'effet des incidents sur les utilisateurs en rétablissant le service normal aussi rapidement que possible.

réponses de Rogers à plusieurs séries de questions et de réunions avec le personnel technique et de gestion de Rogers au cours de cette évaluation, ainsi que sur les renseignements fournis par Rogers en réponse à la demande de renseignements (DDR) du CRTC après la panne.

Description de la panne

Contexte. Pour situer le contexte, Rogers exploite des réseaux sans fil et filaires qui partagent un réseau central IP commun, comme le montre, sous une forme simplifiée, le tableau ci-dessous Figure 1. Le réseau central est une partie du réseau de télécommunication qui est responsable de l'agrégation et de l'acheminement du trafic de données à la fois en interne au sein du réseau de Rogers et en externe avec l'Internet et d'autres fournisseurs de services. Ainsi, pour Rogers, le trafic de données sans fil et filaire est traité par le même réseau central IP. Dans les semaines qui ont précédé le jour de la panne, le 8 juillet 2022, Rogers a mis en œuvre un processus en sept phases pour moderniser son réseau central IP. La panne s'est produite au cours de la sixième phase de ce processus de mise à niveau.

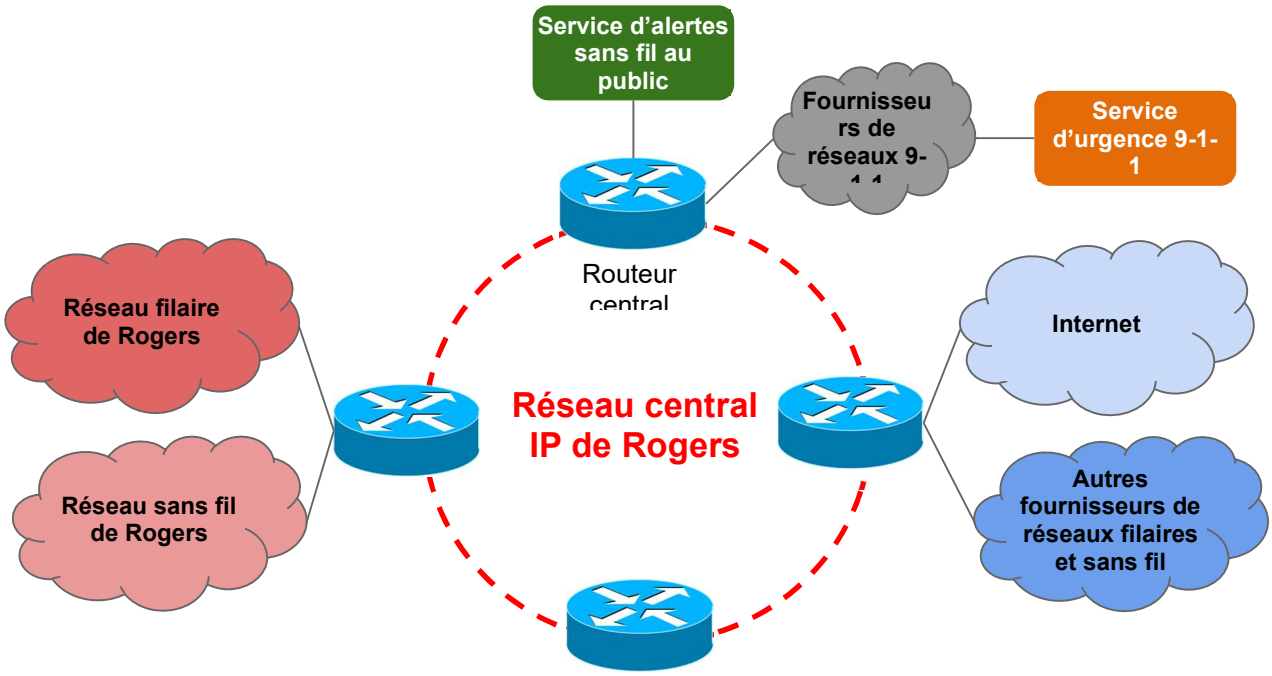

Figure 1 Topologie simplifiée de l'architecture du réseau de Rogers.

Cause première de la défaillance du réseau. La panne de juillet 2022 est attribuée à une erreur de configuration des routeurs de distribution[4] au sein du

[4]Un routeur de distribution est un routeur qui dirige le trafic entre la couche d'accès, qui connecte les utilisateurs au réseau, et le réseau central, qui regroupe tout le trafic du réseau.

réseau IP de Rogers. Le personnel de Rogers a supprimé le filtre de gestion de la liste de contrôle d'accès[5] de la configuration des routeurs de distribution. Il en est résulté un afflux d'informations de routage IP dans les routeurs du réseau central, ce qui a déclenché la panne. Les routeurs du réseau central permettent aux clients des services filaires et sans fil de Rogers d'accéder à des services comme la voix et les données. L'afflux de données de routage IP des routeurs de distribution vers les routeurs centraux a dépassé leur capacité de traitement de l'information[6]. Les routeurs principaux sont tombés en panne dans les minutes qui ont suivi la suppression du filtre de gestion de la configuration des routeurs de distribution. Lorsque les routeurs du réseau central sont tombés en panne, le trafic des utilisateurs ne pouvait plus être acheminé vers la destination appropriée. En conséquence, des services comme la téléphonie mobile, la téléphonie résidentielle, l'Internet, la connectivité filaire des entreprises et les appels au 9-1-1 ont cessé de fonctionner.

Absence de protection contre les surcharges du routeur. La panne de juillet 2022 a mis en évidence l'absence de protection contre les surcharges des routeurs du réseau central. La panne du réseau aurait pu être évitée si les routeurs du réseau central avaient été configurés avec une limite de surcharge qui spécifie le nombre maximum acceptable de données de routage IP que le routeur peut prendre en charge. Cependant, les routeurs du réseau central de Rogers n'ont pas été configurés avec de tels mécanismes de protection contre les surcharges. Par conséquent, lorsque le filtre de gestion a été supprimé du routeur de distribution, une quantité excessive de données de routage a inondé les routeurs principaux, ce qui les a fait tomber en panne.

Déficience dans le processus de gestion du changement. L'erreur de configuration, qui a conduit à la suppression du filtre de gestion de la configuration des routeurs de distribution, est le résultat d'un oubli de gestion des changements par le personnel de Rogers. Le personnel de Rogers a supprimé le filtre de gestion qui empêchait l'inondation des routes IP afin de nettoyer les fichiers de configuration des routeurs de distribution. Le processus de gestion des changements, qui comprend des vérifications des paramètres de changement, n'a pas permis de détecter la modification erronée de la configuration.

Comme indiqué plus haut, ce changement de configuration constituait la sixième phase d'un processus de mise à niveau du réseau en sept phases qui avait débuté quelques semaines auparavant. Avant cette sixième phase de mise à jour de la

[5]Une liste de contrôle d'accès dans un routeur est une table qui fournit les règles sur la façon dont le routeur doit gérer le trafic de paquets. La liste de contrôle d'accès est décrite comme un filtre de politique parce qu'elle définit le trafic qui passera par le routeur et comment il sera dirigé en fonction de l'ensemble des règles (filtres).

[6]Rogers a déclaré qu'environ 10 000 routes sont annoncées dans le routeur principal lorsque le filtre de gestion de la liste de contrôle d'accès est présent sur le routeur de distribution. Lorsque ce filtre a été supprimé, un seul routeur de distribution a transmis plus de 900 000 données d'itinéraires aux routeurs principaux.

configuration, les précédentes mises à jour de la configuration ont été effectuées avec succès, sans aucun problème. Rogers avait initialement évalué le risque de ce processus en sept phases comme étant « élevé ». Toutefois, comme les modifications des phases précédentes ont été menées à bien, l'algorithme d'évaluation des risques a ramené le niveau de risque de la sixième phase du changement de configuration à un risque « faible », notamment la modification à l'origine de la panne de juillet 2022. L'évaluation des risques étant faible, le personnel de Rogers n'a pas été tenu de procéder à un examen plus approfondi, de passer par des niveaux d'approbation plus élevés et d'effectuer des tests en laboratoire pour ce changement de configuration. L'abaissement de l'évaluation du risque à « faible » pour la modification du filtre de gestion de la liste de contrôle d'accès dans une politique de routage est contraire aux normes de l'industrie, qui exigent un examen minutieux pour de tels changements de configuration, notamment des tests en laboratoire avant le déploiement dans le réseau de production.

Fiabilité de l'architecture du réseau de Rogers

Le réseau de Rogers est un réseau national de niveau 1 dont l'architecture est conçue pour être fiable; il est typique de ce que l'on attendrait d'un tel réseau de fournisseur de services de niveau 1. La panne de juillet 2022 n'était pas due à un défaut de conception dans l'architecture du réseau central de Rogers. Cependant, les réseaux sans fil et filaires partageant un réseau central IP commun, l'ampleur de la panne a été extrême, puisqu'elle a entraîné une perte catastrophique de tous les services. Une telle architecture de réseau est commune à de nombreux fournisseurs de services et constitue un exemple de la tendance à la convergence des réseaux de télécommunications filaires et sans fil. Il s'agit d'un choix de conception des fournisseurs de services, notamment Rogers, qui cherche à équilibrer le coût et le rendement.

Facteurs touchant la restauration du réseau

Infrastructure de gestion de réseau. Un réseau de gestion permet d'accéder aux sites d'infrastructures critiques ou aux équipements d'un réseau afin d'en permettre le dépannage et la réparation. Au moment de la panne de juillet 2022, Rogers disposait d'un réseau de gestion qui s'appuyait sur le réseau central IP de Rogers. Lorsque le réseau central IP est tombé en panne pendant l'interruption, les employés de Rogers qui travaillent à distance n'ont pas pu accéder au réseau de gestion. En outre, Rogers n'a pas fourni à son centre d'exploitation du réseau et à d'autres sites d'infrastructure critiques qui se trouvent à distance une connectivité redondante provenant de fournisseurs de services de rechange pour la gestion du réseau. Cela a limité l'accès aux équipements critiques du réseau pendant la panne de juillet 2022 pour effectuer le dépannage et l'analyse des causes profondes. Rogers a dû envoyer du personnel sur des sites situés à distance pour accéder physiquement aux routeurs concernés, ce qui a retardé les efforts de rétablissement du réseau. Selon notre évaluation, la résilience du réseau exige que

les exploitants de réseaux de télécommunications disposent d'un accès de rechange sécurisé à des éléments de réseau essentiels situés à distance qui ne dépendent pas du réseau de données. L'incapacité du personnel de Rogers qui travaille à distance à accéder au réseau de gestion et l'absence de connectivité de secours provenant de fournisseurs de services de rechange vers le centre d'exploitation du réseau et d'autres sites critiques situés à distance ont contribué à prolonger la panne de juillet 2022.

Communication limitée au sein du personnel de Rogers. Le personnel de Rogers s'appuyait sur les services mobiles et Internet de l'entreprise pour communiquer entre eux. Lorsque les réseaux sans fil et filaires sont tombés en panne, le personnel de Rogers, en particulier le personnel chargé de la gestion des incidents critiques, n'a pas été en mesure de communiquer efficacement pendant les premières heures de la panne. Rogers a dû envoyer des cartes SIM (module d'identité d'abonné) d'autres exploitants de réseaux mobiles à ses sites situés à distance pour permettre à son personnel disposant d'une connexion sans fil de communiquer entre eux. L'absence de moyens de communication de rechange suffisants a ralenti la réaction de Rogers à la panne de juillet 2022.

Accès rapide à l'information critique pour le rétablissement du réseau. Le manque de renseignements a entravé le processus de gestion des incidents de Rogers. Le personnel de Rogers n'avait pas accès aux journaux d'erreurs des routeurs défaillants et ne pouvait pas déterminer la cause première de la panne pendant environ 14 heures après le début de la panne. De plus, Rogers avait effectué de multiples changements de configuration pendant la fenêtre de maintenance le jour de la panne. Cela a eu une incidence négative sur les efforts de rétablissement des pannes, et il a été difficile de décider quel ticket de changement de réseau devait être annulé. Ces deux facteurs ont contribué à un mauvais diagnostic de la cause première de la défaillance du réseau dans les premières heures de la panne de juillet 2022. Cependant, une fois la cause première déterminée, les activités de restauration du réseau ont commencé méthodiquement et les services ont été progressivement rétablis.

Mesures prises par Rogers pour améliorer la fiabilité et la résilience de son réseau

Traiter la cause première de la panne et les déficiences de l'architecture du réseau de gestion. Dans les mois qui ont suivi la panne de juillet 2022, Rogers a pris une série de mesures et d'initiatives pour remédier aux déficiences critiques révélées par la panne. Plus important encore, Rogers a mis en place des mesures de protection dans la configuration des routeurs de son réseau central afin d'empêcher l'inondation des données de routage IP, ce qui permet d'éviter qu'une panne similaire ne se reproduise à l'avenir. Rogers a également mis en place un réseau de gestion physique et logique distinct pour accéder aux éléments du réseau à des fins de dépannage et d'analyse des causes profondes. En outre, Rogers a déployé une connectivité de secours auprès de fournisseurs de services tiers pour

son centre d'exploitation du réseau et d'autres sites d'infrastructure critiques situés à distance, et a investi dans des outils qui aideraient à valider les changements de configuration des routeurs.

Noyau IP séparé pour les réseaux sans fil et filaires. À la suite de cette panne, Rogers a annoncé qu'il avait décidé de séparer le réseau central IP pour ses réseaux sans fil et filaires. Cette décision implique le déploiement d'un nouveau noyau IP pour le réseau sans fil, tandis que le noyau IP existant resterait en place pour desservir le réseau filaire. Par conséquent, si un réseau central IP était touché par une panne, l'autre réseau central IP resterait intact et opérationnel.

Rogers n'a pas encore terminé de mettre en œuvre la séparation du réseau central IP, qui reste un travail en cours. Lorsqu'ils seront mis en œuvre, les réseaux IP centraux distincts pour les réseaux sans fil et filaires permettront de limiter une panne à leur réseau d'accès respectif et, par conséquent, d'éviter le type de panne de réseau catastrophique que l'on a connu lors de la panne de juillet 2022, où les services sans fil et filaires n'étaient pas disponibles en raison d'une panne du réseau central IP commun. La séparation du réseau central IP améliorerait la résilience globale des réseaux sans fil et filaires de Rogers.

Améliorer le processus de gestion du changement. Après la panne de juillet 2022, Rogers a apporté plusieurs améliorations à son processus de gestion du changement. Ces améliorations comprennent un nouvel algorithme d'évaluation des risques, des changements organisationnels visant à améliorer la collaboration entre les équipes d'exploitation et d'ingénierie du réseau, un processus amélioré pour l'introduction de nouveaux équipements et de nouvelles technologies, des améliorations dans la mise en œuvre des modifications du réseau, comme l'introduction de l'automatisation pour rationaliser le processus de gestion des changements, et des tests de laboratoire supplémentaires pour les modifications prévues de la configuration du réseau.

Améliorer le processus de gestion des incidents. Après la panne de juillet 2022, Rogers a apporté des améliorations à son processus de gestion des incidents, notamment en renforçant ses lignes directrices en matière de gestion des incidents afin d'englober divers scénarios de panne; en rationalisant sa réponse aux incidents grâce à des rôles de leadership bien définis; en mettant en œuvre une solution pour hiérarchiser les alarmes pendant la panne; en améliorant les retours automatisés aux configurations précédentes lorsque les nouveaux changements ne réussissent pas; en mettant en œuvre des mesures supplémentaires afin d'améliorer ses protocoles de communication. Rogers a également équipé tous les membres de l'équipe de réponse aux incidents et de gestion de crise de moyens de communication de secours provenant de fournisseurs de services tiers afin de maintenir les capacités de communication pendant les pannes.

Évaluation et recommandations à Rogers

Notre évaluation globale est que la combinaison des mesures prises par Rogers après la panne de juillet 2022 est satisfaisante pour améliorer la résilience et la fiabilité du réseau de Rogers ainsi que pour traiter la cause fondamentale de la panne de juillet 2022.

La diligence dans la mise en œuvre des processus améliorés de gestion du changement serait le moyen le plus efficace d'éviter qu'une panne similaire ne se produise à l'avenir. L'amélioration des processus de réponse aux incidents permettrait à Rogers de réagir plus rapidement en cas de défaillance du réseau. Nous avons formulé plusieurs recommandations concernant des mesures supplémentaires que Rogers pourrait prendre pour améliorer la résilience de son réseau. Ces recommandations sont les suivantes :

1. Tester l'itinérance d'urgence avec d'autres exploitants de réseaux mobiles et l'étendre à un ensemble plus complet de scénarios d'essai. Rogers a signé le protocole d'accord sur la fiabilité des télécommunications, qui prévoit l'itinérance d'urgence avec d'autres exploitants de réseaux mobiles afin de permettre aux clients de Rogers d'accéder aux services d'urgence (p. ex., les appels 9-1-1) lors d'une panne majeure. Ces essais supplémentaires permettraient de s'assurer que l'itinérance d'urgence est possible dans différents scénarios de défaillance du réseau, en particulier le scénario observé lors de la panne de juillet 2022 (où le réseau radio était en service et le réseau central en panne).
2. Élaborer une analyse détaillée des causes profondes des futures pannes majeures. Cela faciliterait le processus d'évaluation d'une panne et de son incidence, ainsi que la détermination des mesures d'atténuation appropriées.
3. Assurer une large couverture et une grande rigueur dans les tests des changements de configuration. Cela permettrait d'éviter les erreurs susceptibles d'entraîner des pannes. Rogers devra exploiter de nouveaux outils de test pour modéliser des scénarios de test qui reproduisent le réseau de production et pour tenir compte de l'évolution des technologies de réseau.
4. Élargir la portée des exercices de gestion des incidents. Cela permettrait d'améliorer la préparation du personnel et du réseau aux situations d'urgence et de découvrir les faiblesses de manière proactive.
5. Institutionnaliser l'apprentissage à partir de ses propres défaillances de réseau et de celles d'autres fournisseurs de services afin de mettre en œuvre des mesures préventives, de réduire l'incidence des pannes de réseau et d'améliorer la qualité du service.
6. Informer les clients sur la manière de joindre les services 9-1-1 pendant une panne.

7. Faire connaître les causes profondes des pannes et les stratégies d'atténuation à l'ensemble de la communauté Internet (représentée par des organismes comme le North American Network Operator's Group), afin d'aider les autres exploitants de réseaux de télécommunication à prévenir des pannes similaires.

Recommandations aux exploitants de réseaux de télécommunications

Leçons tirées de la panne de juillet 2022. Voici un résumé des principales leçons tirées de la panne de juillet 2022 :

1. Mettre en œuvre une protection contre la surcharge des routeurs dans les réseaux IP centraux et de distribution.
2. Séparer physiquement et logiquement la couche de gestion du réseau du réseau de données.
3. Fournir au centre d'exploitation du réseau et à d'autres sites distants critiques une connectivité de secours sécurisée provenant d'exploitants de réseaux de télécommunications tiers.
4. Veiller à ce que le processus de vérification des changements de configuration du réseau soit efficace et implique différentes équipes au sein de l'organisation, comme l'ingénierie, les opérations et la gestion de projet. Il est également conseillé d'impliquer les fournisseurs d'équipement lorsque les changements de configuration concernent des infrastructures critiques, comme le réseau central IP.
5. Effectuer des tests en laboratoire des changements de configuration prévus et s'assurer que l'équipement de laboratoire et les scénarios de test reflètent fidèlement le réseau de production.
6. Gérer avec soin le nombre de changements de configuration effectués au cours d'une seule fenêtre de maintenance et tirer parti des outils et des processus pour le retour automatisé des paramètres de configuration.
7. Mettre en œuvre une solution automatisée de hiérarchisation des alarmes afin de supprimer les alarmes inutiles pour chaque type de changement et de permettre au personnel de se concentrer sur les alarmes importantes.
8. Fournir au personnel critique des moyens de communication secondaires, tels que des cartes SIM d'exploitants de réseaux tiers.
9. Simuler et pratiquer des scénarios de défaillance et de panne du réseau afin de mettre en évidence les lacunes de l'architecture du réseau et du processus de gestion des incidents.

Évolution des tendances des réseaux de télécommunications. Les tendances évolutives des réseaux de télécommunications ont une incidence sur la fiabilité et la

résilience des réseaux. Il s'agit notamment de l'évolution vers des plateformes publiques de télécommunications en nuage, de la logiciellisation et de la virtualisation des réseaux, de l'utilisation accrue de l'intelligence artificielle dans l'automatisation des réseaux, de la préparation à la cybersécurité post-quantique et de la convergence des réseaux terrestres et non terrestres. Les fournisseurs canadiens de services de télécommunications sont en train d'intégrer certaines de ces tendances dans l'évolution de leur réseau. Nous soulignons quelques recommandations technologiques et de processus qui permettraient de renforcer la résilience des réseaux face à ces tendances évolutives. Ces recommandations comprennent :

1. Recommandations technologiques :

    A. Tirer parti des nouvelles constellations de satellites en orbite non géostationnaire (p. ex., les constellations de satellites en orbite basse) pour fournir aux sites éloignés une connectivité de secours et envisager les nouvelles constellations à liaison directe pour les appels d'urgence 9-1-1.

    B. Suivre et préparer la mise en œuvre des normes d'itinérance en cas de catastrophe qui sont en cours de planification au sein de l'organisme de normalisation du 3rd Generation Partnership Project (3GPP).

    C. Envisager l'utilisation d'applications de messagerie en ligne comme méthode de communication de rechange, notamment pour les services d'urgence. Cela serait utile en cas de défaillance de certains systèmes critiques, tels que le système multimédia IP.

    D. Exploiter les technologies SIM dynamiques basées sur des logiciels, qui offrent différents niveaux de programmabilité et permettent de nouveaux modèles d'itinérance vers d'autres fournisseurs en cas de pannes majeures.

    E. Étudier l'applicabilité des techniques de partage du spectre et de la capacité d'urgence pour atténuer l'incidence des défaillances du réseau et œuvrer en ce sens. Ces techniques augmentent temporairement et dynamiquement la capacité du réseau pour répondre aux besoins des utilisateurs itinérants.

    F. Envisager de collaborer avec les réseaux de diffusion de contenu et les fournisseurs d'applications en ligne pour définir des modèles d'interaction précis en cas d'urgence. Par exemple, la gestion dynamique du trafic permet aux fournisseurs de contenu d'adapter leur comportement en fonction des renseignements fournis par les exploitants de télécommunications.

G. Envisager d’offrir aux fournisseurs de services d’infrastructures critiques des options secondaires pour des services de connectivité redondants.

2. Recommandations relatives au processus :

   A. Mettre en œuvre des formations et des exercices de réponse aux incidents afin de découvrir les faiblesses de l’architecture, des opérations et des processus opérationnels qui ont une incidence négative sur les efforts de rétablissement des pannes.

   B. Mettre en place des indicateurs de rendement clés pour la réponse à la gestion des incidents afin d’évaluer l’effort de réponse aux incidents et d’en améliorer l’efficacité.

   C. Définir clairement les rôles et les responsabilités du personnel afin de mieux répondre aux pannes de réseau.

   D. Envisager de calculer l’incidence financière d’une panne de réseau afin d’atténuer les conséquences des incidents en prenant des décisions sur l’affectation des ressources et en communiquant avec les intervenants pour préserver l’image de marque et la stabilité financière.

   E. Pendant une panne, il est conseillé aux fournisseurs de services de rappeler au public comment accéder aux services d’appels d’urgence et d’alertes au public.

Glossaire

Fournisseur de réseau 9-1-1	Le fournisseur de réseau 9-1-1 est l'exploitant local historique qui fournit le service d'intervention d'urgence 9-1-1 à l'autorité locale conformément à un tarif ou à un accord. Le tarif ou l'accord du fournisseur du réseau 9-1-1 met l'accès aux appels d'urgence 9-1-1 à la disposition des utilisateurs finaux situés dans la zone de desserte.
Filtre de gestion de la liste de contrôle d'accès	Un filtre de gestion de la liste de contrôle d'accès dans un routeur est une table qui fournit les règles sur la façon dont le routeur doit gérer le trafic de paquets. La liste de contrôle d'accès est décrite comme un filtre de gestion parce qu'elle définit le trafic qui passera par le routeur et comment il sera dirigé en fonction de l'ensemble des règles (filtres).
Protocole BGP	Le protocole BGP est un protocole de routage de passerelle extérieure qui permet l'échange d'informations sur les itinéraires entre les routeurs de différents systèmes autonomes, dans le but de sélectionner le meilleur chemin pour les paquets de données.
Routeur central	Un routeur central est un routeur situé dans le réseau central, ou couche, d'un réseau IP.
Processus de gestion du changement	Le processus de gestion du changement est une approche systématique de la gestion des modifications de l'infrastructure et des services du réseau. Il s'agit d'un processus conçu pour réduire le risque d'interruption des services et pour garantir que les changements sont contrôlés et mis en œuvre de manière efficace.
Routeur de distribution	Un routeur de distribution est un routeur de la couche de distribution du réseau IP d'un fournisseur de services de télécommunication. Il se situe entre la couche d'accès qui connecte les utilisateurs finaux au réseau et la couche centrale qui regroupe tout le trafic du réseau.
Serveur de noms de	Un serveur de noms de domaine est comme un carnet d'adresses pour l'Internet. Un serveur de noms de domaine

domaine	traduit les adresses Web conviviales (comme www.rogers.com) en adresses numériques de protocole Internet.
Processus de gestion des incidents	Le processus de gestion des incidents est une approche systématique du recensement, de la réponse et de la résolution des incidents qui touchent les services du réseau. Il est conçu pour réduire l'effet des incidents sur les utilisateurs en rétablissant le service normal aussi rapidement que possible.
Entreprise de services locaux titulaire (ESLT)	L'entreprise de services locaux titulaire est le fournisseur du réseau 9-1-1 dans le cadre de ce rapport.
Intermediate System to Intermediate System	Intermediate System to Intermediate System est un protocole de routage par passerelle intérieure qui permet l'échange d'informations sur les itinéraires entre les routeurs au sein du réseau d'un exploitant afin de sélectionner le meilleur chemin pour les paquets de données. Il s'agit d'un type de protocole similaire à Open Shortest Path First (OSPF).
Système d'agrégation et de dissémination national d'alertes (système ADNA)	Le Système d'agrégation et de dissémination national d'alertes reçoit les alertes d'urgence des agences gouvernementales autorisées. Ces alertes sont ensuite mises à la disposition des radiodiffuseurs et autres distributeurs de médias qui les diffusent volontairement au public canadien. Pelmorex Communications Inc. est désigné comme regroupeur et distributeur national de messages d'alerte en cas d'urgence.
Système national d'alertes au public (SNAP)	Le Système national d'alertes du public est un système fédéral, provincial et territorial qui permet aux organisations de gestion des urgences de partout au Canada d'avertir le public des dangers imminents ou en cours.
Open Shortest Path First (OSPF)	Open Shortest Path First est un protocole de routage par passerelle intérieure qui permet l'échange d'informations sur les itinéraires entre les routeurs du réseau d'un exploitant afin de sélectionner le meilleur chemin pour l'acheminement des paquets de données.

Fournisseurs de réseau d'origine	Le réseau à l'origine d'un appel 9-1-1. Il comprend le réseau d'accès et le réseau d'appel. Il est Généralement exploité par des entreprises ou d'autres fournisseurs de services.
Messagerie par contournement	La messagerie par contournement est un service de messagerie offert par une application qui n'est généralement pas liée au fournisseur de services de télécommunication et qui fonctionne indépendamment de lui. Par exemple, des services comme WhatsApp, Signal, Telegram, WeChat et d'autres sont des services de messagerie par contournement, contrairement au service de messages courts et au service de messagerie multimédia, qui sont des technologies intégrées à la technologie cellulaire (p. ex., GSM, 3G ou LTE).
Réseau de production	Le réseau de production est un terme couramment utilisé par les fournisseurs de services pour distinguer les éléments de réseau actifs de ceux utilisés dans un environnement de laboratoire. Dans ce contexte, la production consiste à traiter le trafic des clients dans un environnement réel.
Centre d'appels de la sécurité publique (CASP)	Lieu de réponse aux appels 9-1-1 provenant d'une zone donnée. Un CASP peut être conçu comme primaire ou secondaire, ce qui fait référence à l'ordre dans lequel les appels sont acheminés pour y répondre. Les CASP primaires interviennent en premier. Il s'agit d'une installation de communication ouverte 24 heures sur 24, 365 jours par année, chargée de rediriger ou de transférer les appels d'urgence vers des CASP secondaires qui reçoivent les appels sur la base d'un transfert uniquement et qui servent généralement de lieu de réponse centralisé pour un type particulier d'appel d'urgence. Les employés des CASP secondaires proviennent d'organismes de services comme la police, les pompiers ou les agences médicales d'urgence, ou d'un bureau commun desservant un groupe d'entités de ce type.
Routeurs	Les routeurs sont des dispositifs de mise en réseau qui reçoivent et transmettent des paquets de données dans les réseaux IP. Les routeurs dirigent le trafic au sein des réseaux ou entre eux.
Protocole de	Un protocole de routage spécifie comment les routeurs transmettent les paquets d'une source à une destination. Les

routage	protocoles de routage sont regroupés en deux grandes catégories : les protocoles de passerelle intérieure et les protocoles de passerelle extérieure. Les protocoles de passerelle intérieure sont conçus pour fonctionner au sein d'un système autonome, c.-à-d. un réseau contrôlé par voie administrative par une seule organisation. Les protocoles de passerelle externe sont conçus pour gérer le transfert d'informations entre les systèmes autonomes.

Acronymes :

API	Interface de programmation d'applications
BGP	Protocole BGP
BRI	Indice de risque de base
SSE	Systèmes de soutien aux entreprises
CRMS	Capacité, fiabilité, sécurité obligatoire et service (réseau d'accès)
CRTC	Conseil de la radiodiffusion et des télécommunications canadiennes
CCCST	Comité consultatif canadien pour la sécurité des télécommunications
PD	Passerelle de distribution
DNS	Système de nom de domaine
DOCSIS	Spécifications d'interface du service de données sur câble
HAE	Heure avancée de l'Est
FCC	Commission fédérale des communications des États-Unis
IETF	Internet Engineering Task Force
PPI	Protocole de passerelle intérieure
ESLT	Entreprise de services locaux titulaire
IP	Protocole Internet
IPv4	IP version 4
IPv6	IP version 6
Innovation, Sciences et Développement économique Canada (ISDE)	Innovation, Sciences et Développement économique Canada (Ministère d')
FSI	Fournisseurs de services Internet
IRC	Indicateur de rendement clé
LTE	Technologie d'évolution à long terme
MPLS	Commutation multiprotocole par étiquette
RPVM	Réseau privé virtuel multidiffusion
ADNA	Système d'agrégation et de dissémination national d'alertes
TCR	Ticket de changement de réseau
NIST	National Institute of Standards and Technology
CER	Centre d'exploitation du réseau
SNAP	Système national d'alertes au public
LNP	Lancement d'un nouveau produit

LNT	Lancement d’une nouvelle technologie
OSPF	Open Shortest Path First
SSO	Systèmes de soutien opérationnel
ICP	Infrastructure à clés publiques
CASP	Centre d’appels de la sécurité publique
RCMIN	Réseau IP de gestion de Rogers Communications
RFC	Demande de commentaires
DDR	Demande de renseignements
SD-WAN	Réseau étendu défini par logiciel
SIM	Module d’identité d’abonné
ANS	Accord sur les niveaux de service
FST	Fournisseur de services de télécommunication
RPV	Réseau privé virtuel