Transnet Group ICT

PROCUREMENT OF REDUNDANCY AND BACKUP CONNECTIVITY FOR SD-WAN TRAFFIC: SCOPE OF WORK AND REQUIREMENTS

Title	Procurement Of Redundancy and Backup Connectivity for SD-WAN Traffic: Scope Of Work and Requirements
Functional Area	Network Engineering
Executive Sponsor	Pandelani Munyai
Service Owner	Lindiwe Sibidi
Authors	Louis Nel
Version	1
Date Compiled	2024-05-13

I TABLE OF CONTENTS

IILIST OF FIGURES

III LIST OF TABLES

IV DOCUMENT CHANGE HISTORY

ISSUE NUMBER	DATE ISSUED	ISSUED BY	HISTORY DESCRIPTION
1.00	September 24	GICT/Network Engineering	This is the original version

V ABBREVIATIONS, ACRONYMS AND DEFINITIONS

Acronym/ Abbreviation	Description
CMO	Current Mode of Operation
FEL	Front End Loading
FMO	Future Mode of Operation
FY	Financial Year
IOS	Internetwork Operating System
LAN	Local Area Network
LTE	Long-Term Evolution
MPLS	Multiprotocol Label Switching
NEC	Network Enterprise Connectivity
NERSA	National Energy Regulator of South Africa
PFMA	Public Finance Management Act
POPI	Protection of Personal Information
PPM	Procurement Process Manual
SCADA	Supervisory Control and Data Acquisition
SDN	Software Defined Networking
UPS	Uninterruptible Power Supply
UTP	Unshielded Twisted Pair
VC	Video Conference
VLAN	Virtual LAN
WACC	Weighted Average Cost of Capital
WAN	Wide Area Network
WiFi	Wireless Fidelity
SDWAN	Software Defined Wide Area Network
IP	Internet Protocol
PMO	Project Management Office
PLP	Project Lifecycle Process

1. DOCUMENT PURPOSE

This document defines the scope of work and requirements for sourcing a secondary service provider through an open request for proposal (RFP) for provisioning and maintenance of redundancy and backup connectivity for 47 SD-WAN campus sites nationally, the SD-WAN traffic should be routed through the secondary service provider network for failover and high availability and redundancy for a three (3) year period. The current fibre and transmission service provider (TFR) has provisioned the primary connectivity for the 47 SD-WAN Campus sites nationally.

2. BUSINESS CONTEXT AND CHALLENGES

2.1. BUSINESS CONTEXT

Transnet is transforming its business to a digital enterprise that will make use of digitization to improve digital processes and digitalization to realize innovative disruptions as depicted in Figure 1 below in order to enable the organization to grow the business core.

Figure 1: Digitization and digitalization required to accelerate digital business transformation

2.2. As Transnet prepares to embark on a new strategic journey to embrace digital growth and transformation to deliver on its mandate as a state owned entity, it will be enabled through the network connectivity that is stable, scalable and reliable.

2.3. TFR owns, operates, manages telecommunications network infrastructure which is key to safe and reliable rail operations.

2.4. TFR's Layer 1 network consists of 24 – core, 36 – core, and 48 – core fibre cables. The network is supported by over 140 network equipment rooms with approximately 159 Huawei Dense Wavelength Division Multiplexers (DWDM) nodes used for transmitting digital signals.

2.5. Transnet has 9 575km of optic fibre cable ("Layer 1") under Transnet Freight Rail (TFR) and nearly 680km under Transnet Pipelines (TPL), totalling approximately 10 255km of fibre. To activate its fibre, TFR deployed 159 optical switches based on Huawei Dense-Wavelength Division Multiplexing (DWDM) technology. The TPL fibre (48-core) activation will require optical switches. TPL's optical network switches are deployed on the TPL 24-core fibre, dedicated to supporting the TPL Process Control Network (PCN) on the New Multi-Product Pipeline (NMPP) which is excluded from the PSP scope (see next section)

2.6. The Transnet installed fibre cable in some areas consist of 12, 24, 36, or 48 fibre strands bundled into six or eight core fibre bundles . This network covers most of the country and touches most of the campuses on Transnet's operation. This vast fibre infrastructure is used for the rail network signalling and rail infrastructure asset monitoring as well as !eased out to third (3rd) parties for broadband requirements.

- TFR (24-, 36- and 48-core) optical fibre cable (Layer 1)
- TFR optical transport network (Layer 2)
- TPL (48-core) optical fibre cable (Layer 1)

2.7. iv. Resources and tools of trade dedicated to supporting and maintaining the above-listed elements

2.8. Transnet also has a significant amount of campus fibre which is installed on various Operating Divisions (OD's) buildings and yards, and some has reached end of life, i.e. it needs to be replaced and upgraded to meet the business demands including network technology enhancement opportunities such as Software Defined Networking (SDN).

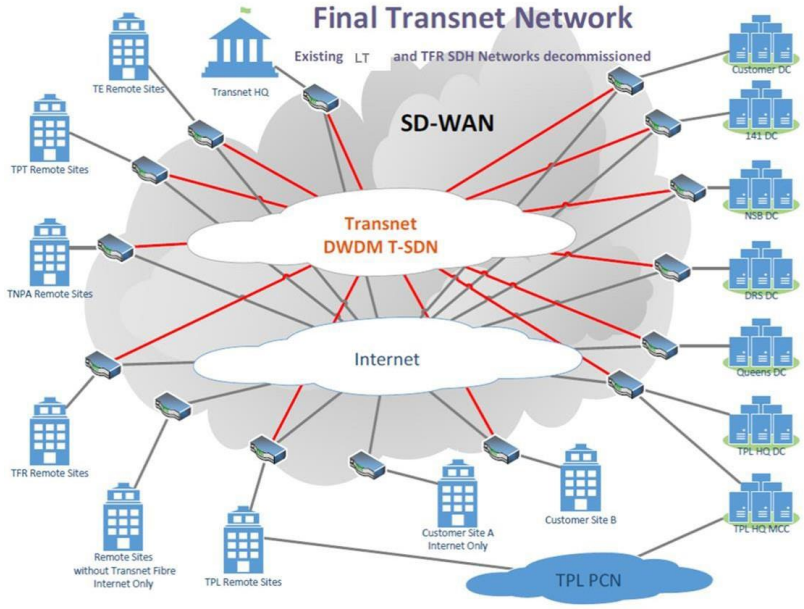
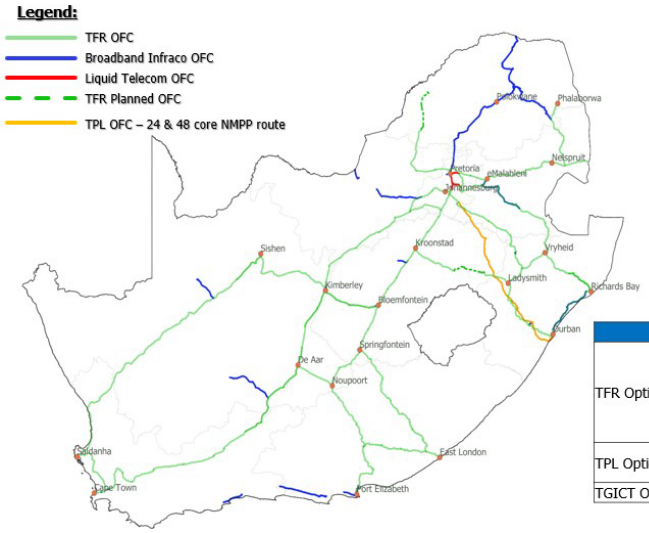


Figure 2: The high level envisaged TO-BE state (90% complete) of the Transnet network



Asset	Optical Fibre Cable Cores	Distance
TFR Optical Fibre Cables (OFC)	24 Cores (12 Pairs)	7555
	36 Cores (18 Pairs)	1623
	48 Cores (24 Pairs)	200
TPL Optical Fibre Cables	24 Cores (12 Pairs)	680
TGICT Optical Fibre Cables	48 Cores (24 Pairs)	680
	Total Distance OFC	**10738**

Figure 3: Transnet Fibre Network Overview

3. CURRENT ENTERPRISE NETWORK STATE

3.1. FIBRE CONNECTIVITY

3.1.1. Transnet has over 12 000km of fibre deployed through-out the country covering the long haul (National Long Distance, [NLD]) as well as the campuses where there are Transnet offices.

3.1.2. Transnet is currently deploying a 100Gb/s nationwide DWDM/OTN system in order to provide a robust Ethernet backbone network.

3.1.3. Transnet has layer 2 (Ethernet) connectivity on major data centres in the country which include Teraco (Isando, Durban and Rondebosch) as well as 141 Sivewright and Megawatt Park. Transnet has finalized IP Peering at Teraco on NAPAFRICA and Teraco Cloud Exchange

3.1.4. Point of Presence has also been established on the Cable undersea landing stations (Mtunzini Seacom, Mtunzini Telkom, Yzerfontein). As part of Transnet's Network strategy, self-provisioning is a critical aspect to ensure sustainability of network services.

3.2. INTERNET SERVICES STATE

3.2.1. Transnet has procured Internet Breakout services as a managed service from a third party provider and these services are provisioned on the Service Providers MPLS Network.

3.2.2. Due to the cost of last mile links for the internet break-out, Transnet has invested on point of presence at three Teraco's in the country; Isando(JHB), Brackenfell (CPT) and Durban(DBN).

3.2.3. The current Managed Services Service Provider (DCX has interconnected the layer 2 presence at all three the Teraco Data Centres,Cape Town(CPT), Durban (DBN) & Johannesburg (JHB).

3.2.4. The service is operating in a redundant and automatic fail-over configuration, in the event of failure of one of the breakout points entire load must be provided for on the remaining breakout areas for full capacity of the service.

3.3. WAN SERVICES STATE

3.3.1. Transnet has procured the WAN services as a managed service through a third-party provider and these services are provisioned on Transnet Enterprise Network.

3.3.2. Transnet has an estimate of 483 customer edge routers nationwide which form the access layer network. Transnet has an estimate of 6 Nexus Switches on the SD-WAN environment deployed at the three Teraco data centres.

3.3.3. There are areas inside the borders of South Africa where Transnet operates where there is no physical infrastructure to provide services and these sites are also connected by VSAT. Transnet WAN sites have varying capacities from 128kb/s to 1Gb/s.

3.3.4. Transnet has awarded DCX a contract to build and commission Transnet private, secure and dedicated SD-WAN network, utilizing where possible, the Transnet existing network backbone owned and operated by Transnet. To provision a new Architecture and Network redesign focusing on digital transformation within Transnet campus site. To provision, manage integrate (with invested infrastructure), secure, administrate, maintain and support the WAN Network infrastructure limited to layer 3 and above.

3.3.5. DCX has transformed multiple sites and they are in process of completing the transformation on the remaining campus sites, by migrating services from MPLS to SDWAN. The current fibre and transmission service provider (TFR) has provisioned the primary connectivity for the 47 SD-WAN Campus sites nationally.

4. BACKGROUND

4.1. Transnet relies heavily on its current SD-WAN infrastructure network to support critical business operations, including data exchange between multiple locations, access to cloud services, and communication with external stakeholders. However, the current SD-WAN design lacks redundancy, making it vulnerable to single points of failure and potential network outages.

4.2. The requirement is for a redundancy and backup connectivity solution for an SD-WAN (Software-Defined Wide Area Network) infrastructure. This entails acquiring additional network connectivity services to ensure uninterrupted operation of the SD-WAN in case of primary link failure on the TFR Telecom's fibre network. Redundancy and backup connectivity are crucial for maintaining seamless communication and business continuity, especially in scenarios where the primary network link encounters issues such as outages or degradation in performance.

4.3. The proposed acquisition aims to mitigate the risks associated with single points of failure in the network infrastructure, enhancing reliability and resilience. By investing in redundant connectivity options, the organization can safeguard against potential disruptions to critical operations, maintain productivity, and uphold service level agreements (SLAs) with customers and stakeholders. This acquisition aligns with the strategic goal of ensuring robust and reliable network connectivity to support business objectives and mitigate risks associated with network downtime.

5. CURRENT FIBRE NETWORK CHALLENGES

5.1. As Transnet prepares to embark on a new strategic journey to embrace digital growth and transformation to deliver on its mandate as a state-owned entity, it will be enabled through the network connectivity that is stable, scalable and reliable.

5.2. Transnet's obsolete fibre infrastructure, however, introduces several challenges and issues, hindering the network performance, security, and scalability. These challenges are further elaborated below:

5.3. Lack of Fibre Redundancy and Device Redundancy on Transnet owned Transmission Network. Single Points of Failure: Without redundant fibre connections, a single fibre cut or failure disrupts connectivity and result in prolonged downtime for affected network segments. This vulnerability increases the risk of service interruptions and impacts business continuity and affect business operations.

5.4. Limited Bandwidth Capacity: Obsolete fibre infrastructure has limited bandwidth capacity compared to modern fibre-optic technologies and this limitation causes constrain data transfer speeds and throughput, leading to slower network performance and decreased productivity for users.

5.5. Data Transmission Errors: Aging fibre infrastructure may experience higher rates of data transmission errors, signal degradation, and latency issues, these results in packet loss, retransmissions, and disruptions to network services, impacting user experience and application performance.

5.6. Security Vulnerabilities: Outdated fibre infrastructure lacks advanced security features and encryption protocols, making it more susceptible to interception, eavesdropping, and cyberattacks. Hackers may exploit vulnerabilities in obsolete fibre equipment to gain unauthorized access to sensitive data and compromise network integrity.

5.7. Interoperability Challenges: Legacy fibre infrastructure may not be compatible with newer networking technologies, protocols, or devices, and this leads to interoperability issues, connectivity problems, and integration challenges when trying to incorporate new equipment or systems into the network.

5.8. Maintenance and Reliability Concerns: As fibre infrastructure ages, it may become more prone to physical wear and tear, environmental factors, and equipment failures. Maintenance costs may increase as Transnet struggle to source replacement parts, troubleshoot issues, and ensure uptime for critical network services. Users experience extended network downtime due to network outages resulting in potential revenue loss due to unavailability of redundant links and switches.

5.9. Scalability Limitations: Obsolete fibre infrastructure may lack the scalability and flexibility needed to accommodate growing data volumes, expanding user bases, and emerging technology trends and this can hinder Transnet's growth, innovation, and adaptability to changing business requirements.

5.10. Compliance and Regulatory Risks: Aging fibre infrastructure may no longer comply with industry standards, regulatory requirements, or data protection laws. Non-compliance can expose Transnet to legal liabilities, fines, and reputational damage if found in violation during audits or inspections.

5.11. Fibre optic cables are a critical component of Transnet Network infrastructures, providing high-speed, reliable data transmission, however, the absence of fibre redundancy leads to several challenges and issues that impact network reliability, performance, and resilience. Challenges caused by the lack of fibre redundancy:

5.12. Limited Fault Tolerance: Transnet network has no fibre redundancy, lacking fault tolerance, making them susceptible to disruptions caused by environmental factors, construction activities, or accidental damage to fibre cables. Even minor incidents can lead to significant downtime and service outages.

5.13. Reduced Reliability: In the absence of fibre redundancy, network reliability is compromised as there is no backup path for data transmission in case of fibre failures. This increases the likelihood of service disruptions and impacts user experience, particularly for mission-critical applications and services.

5.14. Increased Recovery Time: When fibre cuts occur in non-redundant networks, the time required to identify and repair the fault is prolonged, leading to extended downtime and longer recovery times. Without redundant fibre routes, restoring connectivity becomes a time-consuming process, affecting business operations and productivity.

5.15. Risk of Data Loss: Network disruptions caused by fibre failures can result in data loss or corruption, particularly if critical data is being transmitted at the time of the outage. Without redundant fibre links, there is no alternative path for data transmission, increasing the risk of data loss and compromising data integrity.

5.16. Inadequate Configuration and Optimization: Without skilled resources, network configurations may be suboptimal, leading to inefficiencies, performance bottlenecks, and security vulnerabilities. Poorly configured networks may struggle to meet the demands of modern applications and services.

5.17. Increased Downtime and Service Disruptions: The lack of skilled personnel can result in longer response times to network issues and outages. Without timely resolution, downtime can disrupt business operations, impact productivity, and lead to revenue losses.

5.18. Limited Innovation and Adaptability: A lack of skilled resources can hinder innovation and the adoption of emerging technologies. Transnet may miss out on opportunities to leverage advancements such as cloud computing, software-defined networking (SDN), and Internet of Things (IoT) due to the inability to deploy and manage these technologies effectively.

5.19. A directive was issued by Transnet Corporate to insource telecommunication services that were previously provided by LIT, TFR telecoms was subsequently "Appointed" to fulfil the maintenance of the fibre across the campuses.

5.20. Due to the unavailability of "As-Built" documents of the current fibre layout and the unavailability of maintenance funding, there has been an increase in the meantime to repair at the campus networks as technicians must spend a significant amount of time locating the fibre before any repairs can be carried out, and this has drastically affected business operation due to prolonged fibre network outages and lack of redundancy.

6. INTRODUCTION: REDUNDANCY AND BACKUP CONNECTIVITY FOR SD-WAN

6.1. Transnet is sourcing a secondary service provider through an open request for proposal (RFP) for provisioning, Implementing and maintenance of redundancy and backup connectivity for 47 SD-WAN campus sites nationally, to enhance the reliability, availability, and resilience of Transnet's software defined wide area network (SD-WAN) connectivity. The SD-WAN traffic should be routed through the secondary service provider network for failover and high availability and redundancy for a three (3) year period.

6.2. Transnet seeks the provision and implementation of redundancy and backup connectivity for the 47 SD-WAN campus sites, as per the table provided in Addendum A. The bidders are invited to propose a redundancy and backup connectivity solution for SD-WAN traffic, i.e either Layer 2 Managed Service, Dedicated internet Access (DIA), alternative fibre connection (preferred) etc. For managed capacity in cases where there is no fibre available a site-to-site IPsec tunnel via microwave or other wireless mediums would be considered as an alternative.

6.3. The current fibre and transmission service provider (TFR) has provisioned the primary connectivity for the 47 SD-WAN Campus sites nationally and provided primary connectivity at the three Teraco Data centres.

7. TECHNICAL REQUIREMENTS: REDUNDANCY AND BACKUP CONNECTIVITY FOR SD-WAN

Redundancy and Backup Connectivity for SD-WAN and Backup Connectivity for Transnet Enterprise Network is crucial for ensuring continuous connectivity and minimizing downtime in case of link failures.

The following are the key requirements which Transnet expects the service provider to implement when provisioning WAN redundancy and backup connectivity for the 47 SD-WAN campus sites:

7.1. The service provider must conduct an initial assessment for infrastructure and connectivity for the existing 49 SD-WAN campus sites requirements.

7.2. The service provider must design and propose the redundancy and backup connectivity solutions based on gathered requirements and analysis that will ensure scalability to accommodate future growth and expansion.

7.3. The service provider must procure necessary fibre optic cables, hardware, software, licenses, and services for redundancy and backup connectivity implementation for the 49 SD-WAN campus sites.

7.4. The service provider must procure, provision, deploy and implement the redundancy and backup connectivity for the 49 SD-WAN campus site and complete configuration of the interconnect network devices to support redundancy mechanisms.

7.5. The service provider must procure and provision inter-connects, cross-connects and NNI (Network-to-network interface) cables to terminate into the existing secondary SD-WAN router for provisioning and implementation of the secondary SD-WAN link though a service provider other than the existing primary SD-WAN fibre service provider (TFR).

7.6. The service provider must implement last mile connectivity for the provision of the redundancy and backup connectivity for all SD-WAN campus sites.

7.7. The service provider must Implement an automatic failover mechanism (including self-healing) that can quickly switch traffic to the redundancy and backup connectivity in case of primary link failure, to ensure high availability and reliability, with minimal failover time and downtime resulting minimal disruption to network services.

7.8. The service provider must implement multiple WAN links from different providers or using different technologies (e.g., fiber optic, Dedicated internet Access, 4G/5G, Microwave) to provide redundancy. This diversification reduces the risk of simultaneous failures. A key requirement is for the alternative transmission technologies to be interference and contention free.

7.9. The service provider must deploy resilient networking equipment to integrate with the existing secondary SD-WAN equipment on all of the 49 SD-WAN campus sites, including routers capable of handling redundancy and backup connectivity for SD-WAN and seamless failover.

7.10. The service provider must utilize load balancing techniques to distribute traffic across multiple WAN links efficiently. This optimizes bandwidth utilization and enhances overall network performance.

7.11. The Service provider must implement robust monitoring tools to continuously monitor the status and performance of the redundancy and backup connectivity for the SD-WAN links. Alerts need to be configured to notify network administrators of any link failures or performance degradation on the secondary WAN redundant links.

7.12. Make use of dynamic routing protocols such as Border Gateway Protocol (BGP) or Open Shortest Path First (OSPF) to automatically reroute traffic in case of link failures. These protocols enable routers to dynamically adjust routing tables based on link availability.

7.13. The service provide must Implement Quality of Service (QoS) policies to prioritize critical traffic over the redundant and backup connectivity, ensuring that important applications receive adequate bandwidth and sufficiently low latency, even during failover scenarios. Implement load balancing and QoS mechanisms to optimize traffic distribution and prioritize critical applications.

7.14. The service provider must regularly test failover mechanisms and redundancy configurations to ensure they function as expected. Conduct simulated failure scenarios to validate the effectiveness of redundancy measures.

7.15. The service provider must offer cost-effectiveness and competitive pricing for fibre optic cables, hardware, software for redundancy and backup connectivity solution for the SD-WAN campus sites.

7.16. The service provider must provide 24/7 maintenance, support and management of the redundancy and backup connectivity solution, including service support, redundancy infrastructure maintenance and support, fibre maintenance and support software updates, patches, fault investigations, troubleshooting and resolution of outages and faults for the redundancy and backup connectivity solution.

8. BENEFITS

8.1. High Availability**:** Redundant and backup connectivity ensures continuous network availability by providing alternative pathways for data traffic in the event of primary link failures or disruptions. This minimizes downtime and ensures uninterrupted access to critical applications and services, thereby maximizing productivity and user satisfaction.

8.2. Geographic Redundancy: Redundant connectivity options allow Transnet to establish geographic redundancy by deploying backup links through diverse network paths, service providers, or physical locations. This geographic diversity further enhances resilience and reduces the risk of single points of failure, ensuring robust connectivity and disaster recovery capabilities across distributed networks and remote sites.

8.3. Improved Reliability: By deploying multiple connectivity options and failover mechanisms, SD-WAN networks become more resilient to link failures, congestion, and other network issues. Redundancy ensures that even if one link experiences problems, traffic can seamlessly reroute to alternative paths, maintaining connectivity and preserving service continuity.

8.4. Business Continuity: Redundancy and backup connectivity solutions are essential for ensuring business continuity and disaster recovery preparedness. By minimizing the impact of network outages and disruptions, Transnet can maintain operational continuity, meet service level agreements (SLAs), and safeguard revenue streams, customer relationships, and brand reputation.

8.5. Enhanced Performance: Backup connectivity options enable load balancing and dynamic path selection mechanisms, allowing SD-WAN controllers to optimize traffic routing based on real-time network conditions and link performance. This ensures efficient utilization of available bandwidth and minimizes latency, jitter, and packet loss, thereby improving application performance and user experience.

8.6. Flexibility and Scalability: Redundant connectivity options provide flexibility for Transnet to adapt to changing network requirements and scale their SD-WAN infrastructure as needed. With the ability to easily add or switch between different types of backup links, Transnet can effectively respond to evolving business demands, geographic expansions, or technology advancements without compromising network reliability or performance.

8.7. Cost Optimization: While redundancy and backup connectivity solutions involve additional infrastructure investments, they can ultimately result in cost savings by preventing costly network downtime, service disruptions, and associated business losses. The proactive approach to network resilience and availability helps minimize the financial impact of outages and disruptions, making it a worthwhile investment in the long run.

8.8. Regulatory Compliance and Risk Mitigation: Redundancy and backup connectivity solutions help Transnet meet regulatory compliance requirements related to data availability, confidentiality, and privacy and National key points requirements. By ensuring continuous access to critical data and applications, Transnet can mitigate the risk of non-compliance penalties, data breaches, and legal liabilities associated with network downtime or data loss.

8.9. Redundancy and backup connectivity are essential components of a robust SD-WAN network architecture, providing Transnet with the resilience, reliability, and performance required to support mission-critical operations, drive business growth, and maintain a competitive edge with the current digital landscape.

9. RISKS AND CHALLENGES

The disadvantages of not implementing redundancy and backup connectivity for an SD-WAN campus network are significant and far-reaching, impacting business continuity, revenue generation, customer satisfaction, regulatory compliance, and brand reputation and will also leave the network vulnerable to various risks and challenges.
The following are some challenges and risks which have been identified due to lack of redundancy within the network:

9.1. Single Point of Failure: Without redundancy, the network relies solely on a single primary link for connectivity. Any disruption or failure in this link, whether it is due to hardware failure, network outage, or maintenance, it can result in a complete loss of connectivity. This single point of failure increases the risk of extended downtime and service interruptions, impacting business operations and productivity.

9.2. Increased Downtime: In the absence of backup connectivity options, network downtime can be prolonged as there are no alternative pathways for data traffic to reroute in the event of primary link failure. Extended downtime can lead to significant financial losses, missed opportunities, and damage to reputation, especially in industries where continuous connectivity is critical, such as finance, healthcare, and e-commerce.

9.3. Loss of Revenue and Productivity: Network outages and downtime directly impact revenue generation and employee productivity. Without redundant links, Transnet may lose revenue from online transactions, suffer disruptions in customer service operations, and experience delays in business-critical processes such as order processing, inventory management, and supply chain operations.

9.4. Operational Disruptions: Network outages and downtime disrupt day-to-day operations, causing delays in business processes, communication breakdowns, and inefficiencies in workflow management. IT teams are tasked with troubleshooting and resolving network issues, diverting resources and attention away from strategic initiatives and core business activities.

9.5. Limited Scalability and Growth: Lack of redundancy hampers the scalability and growth potential of the network infrastructure. Without backup connectivity options, Transnet may face challenges in expanding their network footprint, adding new sites or users, and accommodating increased traffic demands. This limits agility and flexibility in responding to evolving business needs and market dynamics.

9.6. Negative Impact on Customer Experience: Network disruptions can adversely affect the customer experience, leading to dissatisfaction, loss of trust, and potential churn. Operating divisions expect seamless access to online services and applications, and any interruption or degradation in service quality can result in frustration and dissatisfaction, damaging brand reputation and customer loyalty.

9.7. Reputational Damage: Network downtime and service interruptions can tarnish the organization's reputation and credibility in the eyes of customers, partners, and stakeholders. Negative publicity, social media backlash, and word-of-mouth referrals can erode trust and undermine brand equity, making it difficult to regain customer confidence and market trust.

9.8. Investing in redundancy and backup connectivity solutions is essential for mitigating these risks and ensuring the resilience, reliability, and availability of network services.

10. EXPECTED OUTPUT

Transnet is sourcing the service provider to implement redundancy and backup connectivity for the SD-WAN campus network.

The following are the key expected outputs from the service provider:

10.1. Network Assessment and Design Documentation Phase:

10.1.1. Detailed documentation outlining the current network infrastructure, including topology, hardware, and configurations.

10.1.2. Network assessment reports highlighting areas for improvement, potential single points of failure, and recommendations for redundancy and backup connectivity enhancements.

10.1.3. Network design documents specifying the proposed redundancy architecture, backup connectivity options, failover mechanisms, and routing policies.

10.2. Solution Proposal and Implementation Plan:

10.2.1. Proposal documents outlining the proposed redundancy and backup connectivity solution, including hardware, software, licensing, and professional services.

10.2.2. Implementation plan detailing the phased approach for deploying redundancy and backup connectivity features, including timelines, milestones, and resource requirements.

10.2.3. Project kick-off meetings and workshops to align stakeholders, define project objectives, and establish communication channels.

10.3. Fibre cables, Hardware and Software Procurement:

10.3.1. Procurement of Fibre optic and hardware components, such as routers and SD-WAN edge devices, where required for implementing redundancy and backup connectivity.

10.3.2. Acquisition of software licenses, subscriptions, and maintenance agreements for SD-WAN controllers, management platforms, and security appliances.

10.4. Configuration and Deployment:

10.4.1. Deployment of backup links, failover mechanisms on SD-WAN campus sites, and dynamic routing policies to ensure seamless failover and optimal traffic routing across primary and backup links.

10.4.2. Configuration and implementation scripts for deploying redundancy and backup connectivity features on network devices, SD-WAN controllers, and edge devices.

10.4.3. Testing and validation procedures to verify the functionality and effectiveness of redundancy and backup connectivity features under various scenarios and conditions.

10.5. Training and Knowledge Transfer:

10.5.1. Training sessions and workshops for IT staff and network administrators on the operation, management, and troubleshooting of redundancy and backup connectivity features.

10.5.2. Documentation and knowledge base materials covering best practices, troubleshooting guidelines, and operational procedures for maintaining and supporting the implemented solution.

10.6. Monitoring and Management Tools:

10.6.1. Deployment of monitoring and management tools for real-time visibility into network performance, link utilization, status of primary and backup connectivity options and objective measurement and tracking of contracted Service Levels.

10.6.2. Integration with existing network management systems (NMS) and security information and event management (SIEM) platforms for centralized monitoring and alerting.

10.7. Documentation and Reporting:

10.7.1. Comprehensive documentation packages covering configuration details, network diagrams, change and service management procedures, and post-implementation recommendations.

10.7.2. Regular status updates, progress reports, and project documentation throughout the implementation process to track milestones, identify risks, and address issues.

10.8. Post-Implementation Support and Maintenance:

10.8.1. Close-out report confirming no Priority 1 and 2 issues remaining, lessons learned and roadmap of recommended improvements.

10.8.2. Post-implementation support services to address any issues, concerns, or optimization opportunities identified during the deployment phase.

10.8.3. Governance structure for service, change and escalation meetings including account management interface(s) to ODs.

10.8.4. Ongoing maintenance and support agreements for managing and maintaining the redundancy and backup connectivity solution, including software updates, patches, and troubleshooting assistance.

11. PERFORMANCE MANAGEMENT: SLAS

Key Performance Indicators (KPIs) for WAN redundancy measure the effectiveness and performance of redundant WAN links and failover mechanisms. These KPIs assist in assessing the reliability, availability, and resilience of WAN redundancy and backup connectivity.

These are the key essential WAN redundancy KPIs which the service provider needs to achieve and report on daily/weekly, Monthly, quarterly and yearly basis:

11.1. Link Availability:

11.1.1. Measure the percentage of time that WAN links are available and operational. High availability indicates robust redundancy and failover capabilities:

11.1.2. Target: Achieve 99.99% uptime for all SD-WAN Links.

11.1.3. Measure: Calculate link availability as (Total uptime / Total time) * 100%.

11.2. Failover Time:

11.2.1. Assess the time it takes for traffic to be rerouted to alternative paths after a WAN link failure. Lower failover times indicate faster recovery and minimal disruption to network services.

11.2.2. Target: Ensure failover within 100 milliseconds of link failure.

11.2.3. Measure: Measure the time taken for traffic to switch to redundant links after a failure event.

11.3. Redundancy Utilization:

11.3.1. Monitor the utilization of redundant WAN links to ensure efficient use of available bandwidth. Balanced utilization across redundant links optimizes network performance and avoids overloading individual links. A key requirement is for any redundant route to be capable to carry the maximum network traffic load at any given time.

11.3.2. Target: Maintain balanced utilization across redundant links, with no single link exceeding 70% capacity.

11.3.3. Measure: Monitor bandwidth utilization for each SD-WAN link and adjust traffic distribution as needed.

11.4. **Packet Loss**:

11.4.1. Evaluate the percentage of packets lost during transmission over redundant WAN links. Low packet loss rates indicate reliable connectivity and effective failover mechanisms.

11.4.2. Target: Keep packet loss below 0.1% for all SD-WAN links.

11.4.3. Measure: Measure the percentage of lost packets during transmission over redundant links.

11.5. **Latency**:

11.5.1. Measure the delay in data transmission over redundant WAN links. Low latency ensures responsive network performance, especially for real-time applications (e.g. Voice over IP) and services.

11.5.2. Target: Maintain latency below 50 milliseconds for all SD-WAN links.

11.5.3. Measure: Measure the round-trip time for data transmission over redundant links.

11.6. Jitter (Variation in timing, or time of arrival, of received packets):

11.6.1. Assess the variation in latency over time across the SD-WAN links. Consistent jitter levels indicate stable network performance, while high jitter can lead to quality issues for voice and video applications.

11.6.2. Target: Ensure jitter remains below 5 milliseconds for all SD-WAN links.

11.6.3. Measure: Calculate the variance in latency over time to assess jitter levels.

11.7. Redundancy Testing Frequency:

11.7.1. Target: Conduct redundancy testing and failover simulations at least once per quarter.

11.7.2. Measure: Document the frequency of testing and ensure that failover mechanisms are functioning correctly.

11.8. Incident Response Time:

11.8.1. Target: Maintain an average incident response time of less than 15 minutes for WAN link failures.

11.8.2. Measure: Track the time taken to detect, diagnose, and resolve incidents related to WAN link failures.

11.9. Incident Resolution Time:

11.9.1. Target: Maintain an average incident resolution time of less than 4 hours for WAN link failures.

11.9.2. Measure: Track the time taken to investigate, localization, repair and restoration of services and incidents related to WAN link failures.

11.10. SERVICE LEVEL Excused performance

The following tables provide a list of events that should they occur will not impact on the measurement of the service level requirements.

Number	Service Level Measurement Excused performance
1.	Force Majeure events to be defined in the Master Service Agreement.
2.	Power failures that are extended going beyond the designed power backup facilities where additional remediation action is not available/possible e.g. load shedding
3.	A delay by Transnet and or its 3rd parties pertaining to site facilities readiness delaying the installation.
4.	Any Transnet 3rd party initiated installation\ provisioned where records of equipment are not provided then these will be excluded from the CMDB.

Table 1: Service Level Requirement Measurement Exclusions

Number	Clock Stopping Events
1.	The clock will stop outside of the SCW applicable to an Incident or Request. This will be managed automatically by the SM call logging tool.
2.	Information required to fulfil a Request or resolve an Incident is incomplete or incorrect.
3.	Access to site or location is required and the Service Provider or its 3rd parties are unable to gain access after prior arrangement has been agreed
4.	In the event where construction or provisioning of additional facilities is required to the Transnet site or location which are the responsibility of Customer
5.	In the event where Transnet provisioned services or components of services are the cause of the Service Provider logged incident then the clock will stop on this incident until such time as the Transnet dependent incident(s) has been resolved.
6.	Awaiting Customer approval of a Change Requested by the Service Provider required to remediate the incident
7.	A site contact is unavailable to arrange access.
8.	A site contact is unavailable to confirm if site has power.

Table 2: Events that will stop the Clock for Incidents and Service Requests

12. SERVICE CREDIT METHODOLOGY

The Service Provider shall implement measurement and monitoring tools and produce the metrics and reports necessary to measure its performance against the Service Levels. Upon request in connection with an audit or other Transnet requirement, and at no additional charge to Transnet, Service Provider shall provide Transnet or its designees with information and access to the tools and procedures used to produce such metrics.

12.1. DEFINITIONS

Total Monthly Fee - relating to the month in which a Service Level Failure occurs, the total service fees payable by Transnet to the Service Provider for that month.

At-Risk Percentage - 15% (fifteen percent) of the **Total Monthly Fee.**

Weighting Factor - for a particular Service Level Requirement (SLR), the proportion of the At-Risk Percentage used to calculate the Service Credit payable to Transnet in the event of a Service Level Failure with respect to that SLR.
Service Level Failure - occurs whenever the Service Provider's actual level of performance for a specific Service Level Requirement is worse than the Performance Target.
Performance Target - minimum required level of performance as set out in the SLR table.
Service Credit - has the same meaning as assigned thereto in Attachment A and for purposes of this Annexure means a Rand value calculated based on the applicable Weighting Factor of the Service Level Requirement failed, the Total Monthly Fee, and the At-Risk Percentage.
Service Level Requirement Categories - SLRs are allocated the following categories:
Primary Category: Has a direct impact on Transnet business. Service Credits will be applied.
Secondary Category: Has some direct impact on Transnet business, no service credits

12.2. CALCULATING SERVICE CREDITS

For each Primary Service Level Failure, the Service Provider shall pay or credit to Transnet a Service Credit that will be calculated by multiplying (a) the Weighting Factor Allocation for such Service Level by (b) the At-Risk Percentage and (c) the Total Monthly Fee.

For example, and for purposes of illustration only, assume that:

- the Service Provider fails to meet a Service Level with a Weighting Factor of 10% (ten percent), and
- the Total Monthly Fees in that month are R100 000 (one hundred thousand rand) and
- the At-Risk Amount is 15% (fifteen percent),

Then the Service Credit due to Transnet would be: 10% x (R100 000 x 15%) = R1 500.

12.3. SERVICE CREDITS CAP

The aggregate amount of Service Credits credited or paid to Transnet with respect to all Service Level Failures occurring in a specific month will not exceed the At-Risk Percentage x the Total Monthly Fee.

12.4. NON-EXCLUSIVE REMEDY

The Service Provider acknowledges and agrees that the Service Credits shall not be deemed or construed to be liquidated damages or a sole and exclusive remedy or in lieu of any other rights and remedies Transnet has under the Agreement or in law.

12.5. SLR WEIGHTING TABLE

Below is a listing of the SLRs, with their corresponding Weighting Factor for Service Credit calculations.

Section	Service Level Requirement (SLR)	WEIGHTING FACTOR (%)
11.1	Link Availability	30%
11.2	Failover time	10%
11.3	Redundancy Utililsation	5%
11.4	Packet loss	5%
11.5	Latency	10%
11.6	Jitter	5%
11.7	Redundancy Testing Frequency	10%
11.8	Incident Response Time	5%
11.9	Incident Resolution Time	20%
	TOTAL	**100%**

Table 3: SLR weightings

ANNEXURE A: Redundancy + Backup Connectivity for SD-WAN Campus sites: 1 Gbps

Site #	SD-WAN Campus Sites Name	PHYSICAL ADDRESS
1	Newcastle	8 CTC Building, Madadeni Road, Newcastle
2	Springs	1 Appel Ave, Geduld, Springs
3	Sentrarand	1 Du Randt Rd, Sentrarand, Benoni
4	Ermelo	CTC Ermelo - Infra Telecoms Workshop
5	Vryheid	Side East CTC Building, Hlobane Road Number 2, Vryheid
6	Ogies	No 1 Main Road, Transnet Building
7	Standerton	Room 1 Walter Sisulu Road, Standerton Station
8	Empangeni	1 Station Rd, Empangeni Rail, Empangeni
9	Richards Bay	Nsezi CTC, Nsezi Rd, Richards Bay
10	Pietermaritzburg	16 Devenshire Road, Pietermaritzburg
11	Ladysmith	7 Albert Str, Ladysmith
12	Durban	Transnet Durban CTC, Stamford Hill, Durban
13	Bayhead	Loliwe House, 151 South Coast Rd, Rossburgh
14	Isando	114 Pretoria Rd, Kempton Park
15	Heidelberg	10 Van Zyl Street, Heidelberg
16	Vooruitsig	Unnamed road, R23, Volksrust
17	Empangeni	1 Station Rd, Empangeni Rail, Empangeni
18	Queens Warehouse	237 Mahatma Gandhi Rd, Point, Durban, 4001
19	Esselen Park	Essellen Server Rm, 1st Flr, Church St, Tembisa
20	Kroonstad	01 Sterley St, Kroonstad, 9501, South Africa
21	Bethlehem	101 Joubert St, Bethlehem, 9701, South Africa
22	Bloemfontein	2 Harvey Rd, Bloemfontein, Free State
23	Klerksdorp	Golden Way, Klerksdorp Industrial, Klerksdorp comms building
24	Potchefstroom	Stasie Road, Potchefstroom, 2520, South Africa
25	Langslaagte	103 Pomeroy Ave, Johannesburg, 2092, South Africa
26	Krugersdorp	29 Kruger Rd, Luipaardsvlei, Krugersdorp, 1743
27	Vereeniging	56C Union St, Vereeniging, 1936, South Africa
28	Germiston	4 Railway Str, Georgetown, Germiston
29	Johannesburg(NSB)	JCC, Rissik St, Johannesburg, 2000, South Africa
30	Kimberley	35 Knight St, Kimberley, 8300, South Africa
31	Bellville	01 Caledon St, Transnet, Cape Town
32	Worcester	18 Bains St, Worcester, 6850, South Africa
33	Saldanha	Fisheagle Rd, Durban, South Africa
34	Beaufort West	Kerk St, Beaufort West, 6970, South Africa
35	Cape Town	McDonald Rd, Transnet, Cape Town, 7505, South Africa
36	Witbank	2 Langermann St, Emalahleni, 1035, South Africa
37	Middelburg	Connect via Witbank

38	Rustenburg	Kock Street, Rustenburg,
39	Polokwane	Forssman St, Modimolle, 0510, South Africa
40	Pretoria North	Ou Warmbadpad Rd, Pretoria, 0110, South Africa
41	Nelspruit	1 Andrew Str, Nelspruit
42	Hoedspruit	Klaserie Rd, Hoedspruit, 1380, South Africa
43	Nzasm	2677 Skietpoort Ave, Pretoria, 0002, South Africa
44	Koedoespoort	313 Moreleta St, Pretoria, 0184, South Africa
45	East London	1A Cambridge St, East London
46	PE North End	Broad Serv Rd, North End, Gqeberha
47	Noupoort	18 Shaw St, Noupoort, 5950, South Africa
48	Mossel Bay	40 Bland St, Mossel Bay, 6500, South Africa
49	Tarlton	Tarlton
50	North Station	North Station, Johannesburg

Annexure B: LEASE OF MANAGED SERVICES (BANDWIDTH) INTER-TERACO DATA CENTRE LINKS

10 Gbps Links to the Teraco's in Metro areas
Note: all distances are track distances, not optical

LEASE OF TFR 10Gbps TO TGICT Tariff (R / capacity / km / month)					
No	Site A	Site B	Length (km)	Capacity (total)	GICT only
1	Teraco Data Environments (Pty) Ltd., Teraco Campus, 5 Brewery St, Isando, Johannesburg, 1600	Teraco - DB1, Durban, Riverhorse Cl, Newlands East, 4037	937.00	10Gbps	1
2	Teraco Data Environments (Pty) Ltd., Teraco Campus, 5 Brewery St, Isando, Johannesburg, 1600	Teraco - CT1, Cape Town, 240 Main Rd, Rondebosch, Cape Town, 7701	1 676.00	10Gbps	1
3	Teraco - DB1, Durban, Riverhorse Cl, Newlands East, 4037	Teraco - CT1, Cape Town, 240 Main Rd, Rondebosch, Cape Town, 7701	2 386.00	10Gbps	1