

// Amreesh Phokeer (AFRINIC)
// Kevin Chege (Internet Society)
// Josiah Chavula (University of Cape Town)
// Ahmed Elmokashfi (Simula Research Lab)
// Assane Gueye (CMU-Africa)



Abril de 2021 (v1.0)

Medición de la Resiliencia de Internet en África (MIRA)

Descripción general del proyecto





Resumen

Internet desempeña un papel fundamental en la sociedad actual. La pandemia de la COVID-19 ha resaltado aún más la importancia de un acceso a Internet confiable para todas las personas. Desafortunadamente, no todos los países han alcanzado la madurez suficiente en términos de contar con una infraestructura de Internet confiable. En particular, los países de bajos ingresos suelen tener redes infraaprovisionadas y carecer de una infraestructura de cable adecuada o de sistemas de interconexión redundantes. En estos países (o regiones), se producen cortes importantes de Internet cuando hay una rotura de cable o un corte de energía. Esto impacta en todo el ecosistema de Internet, lo que puede resultar en una importante pérdida de ingresos para la economía digital. Además, muchos países de bajos ingresos no tiene la capacidad de auditar a fondo su infraestructura de Internet y, en muchos casos, no han desarrollado o adoptado las mejores prácticas para construir una infraestructura de Internet resiliente. El proyecto Medición de la Resiliencia de Internet en África (MIRA) es una iniciativa conjunta entre el Centro de Información de Red Africano (AfrINIC) e Internet Society, con el objetivo de evaluar la capacidad de un país para proporcionar un medio estable y confiable de acceso a Internet en todo momento. Basándonos en los resultados, brindaremos recomendaciones en forma de mejores prácticas que podrían ayudar a las redes o países a lograr una mayor resiliencia de Internet.

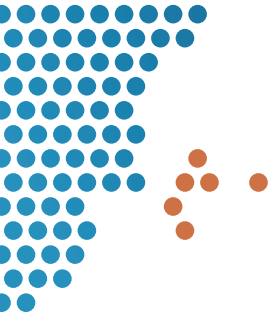
1 Introducción

Uno de los 13 principios de la Declaración Africana de los derechos y la libertad de Internet¹ es la seguridad, estabilidad y resiliencia de Internet. Este principio implica que todas las personas tienen el derecho de disfrutar de un acceso a Internet seguro y confiable, independientemente del tamaño y la ubicación de su red. La pandemia de la COVID-19 ha mostrado la importancia de Internet y de los servicios habilitados mediante Internet para la sociedad y además ha demostrado lo crucial que es construir redes que sean resilientes. Sin embargo, muchas redes africanas están sujetas con frecuencia a muchas formas de interrupción, como cortes de energía, roturas de cables, apagones (no) intencionales y otros incidentes de seguridad [1]. En algunos casos, las interrupciones se deben a un accidente, ya sea debido a una ingeniería deficiente o a la falta de infraestructura redundante. En algunos casos, las interrupciones se deben a bloqueos patrocinados por el estado, especialmente durante períodos electorales [2]. En algunos casos, los apagones se producen porque no se considera a los operadores responsables y, por lo tanto, no se les incentiva a invertir en su infraestructura para hacerla resiliente. Ya sean intencionalmente o no, las interrupciones de Internet pueden tener un impacto considerable en la sociedad y la economía [3].

Estudios recientes han destacado la diversa calidad del acceso a Internet entre y dentro de los países africanos [4]–[6]

Sin embargo, muchos de los desafíos de Internet en África siguen sin investigarse. Las afirmaciones se basan principalmente en conocimientos anecdóticos no escritos que se comparten informalmente entre las comunidades operativas, como en la Cumbre de África sobre Internet (AIS) y el Foro Africano de Peering e Interconexión (AfPIF). Esta deficiencia dificulta la formulación de soluciones basadas en evidencia o la evaluación del éxito de las interconexiones y esquemas de inversión recientemente implementados. Una

¹ <https://africaninternetrights.org>



encuesta realizada por AfriNIC en 2019 [7] mostró que la medición de Internet no es una práctica común en África. La falta de mediciones suficientes en los países africanos hace que sea muy difícil determinar con precisión las áreas problemáticas que deben atenderse para mejorar la confiabilidad y la resiliencia de Internet en África.

El proyecto MIRA establecerá un marco llamado el “Marco de resiliencia de Internet” que evalúa la capacidad de una red (y por añadidura, un país) para proporcionar medios estables y confiables de acceso a Internet. El marco estará basado en el análisis de datos empíricos (tanto primarios como secundarios) recopilados de redes y países de África. Con base en estos resultados, planeamos identificar y describir las mejores prácticas necesarias para crear un sistema de interconexión nacional y regional más resiliente que, si los proveedores de servicios de Internet (ISP) y los operadores de red lo implementan, podría fortalecer y salvaguardar la infraestructura de Internet de las interrupciones.

1.1 // Contexto

Este proyecto es una iniciativa conjunta del Centro de Información de Red Africano (AFRINIC) e Internet Society. Este proyecto se enmarca en el programa AfriNIC AIM (Medición de Internet en África, Africa Internet Measurement)² y en el proyecto “Medición de Internet” de Internet Society³. AfriNIC e Internet Society colaborarán con otros investigadores como se describe en la Sección 6.4 para Medir la Resiliencia de Internet en África (MIRA). En resumen, queremos:

1. Recopilar y analizar datos empíricos para determinar los niveles actuales de resiliencia de Internet en los países africanos.
2. Desarrollar aún más la infraestructura de medición de Internet en África aumentando el número de puntos de observación de medición activos en África.
3. Presentar los datos a los usuarios en todos los niveles (legisladores, ingenieros, operadores de redes, responsables políticos, usuarios de Internet, etc.).

1.2 // Público destinatario

El resultado de este proyecto se utilizará para informar a los responsables políticos en dos categorías principales:

- Operadores de redes y proveedores de servicios de Internet (ISP) que buscan mejorar la resiliencia de su infraestructura.
- Autoridades reguladoras nacionales (ANR) que definen los entornos legales y operativos de los ecosistemas de Internet en sus respectivos países.

Este proyecto y sus hallazgos tendrán una aplicabilidad más amplia y pueden ser de interés para una mayor audiencia, incluidos los grupos de consumidores e industriales, laboratorios de investigación académicos e industriales, así como organismos de estandarización.

1.3 // Definición y alcance

A lo largo de este proyecto, nuestro objetivo es investigar las amenazas y los obstáculos (tanto internos como externos) que afectan la infraestructura de Internet y los mecanismos

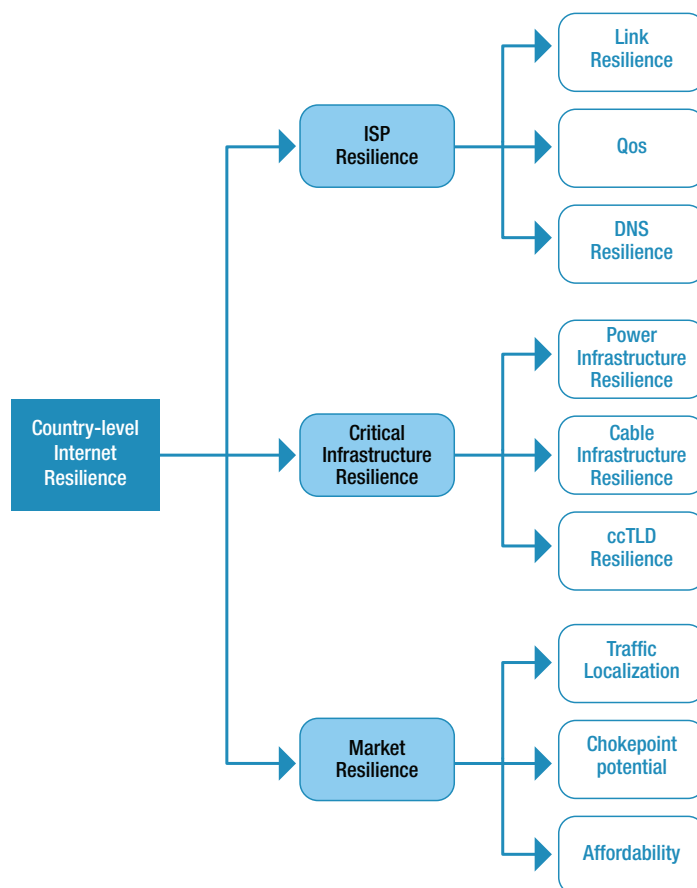
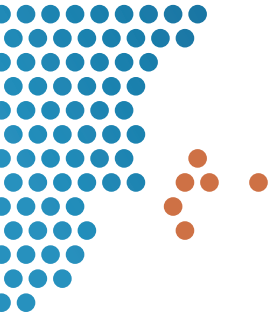


Figura 1: Taxonomía de los componentes de la resiliencia

² <https://afrinic.net/research/programmes/aim>

³ <https://www.internetsociety.org/issues/measurement>



para aumentar la resiliencia general de los servicios de Internet. Es decir, la capacidad de una red para mantener un nivel de servicio aceptable en caso de interrupción o durante crisis [8]–[13]. El mismo principio se aplica a la resiliencia de Internet de un país y este proyecto evaluará la capacidad de cada país para continuar brindando el mejor servicio posible durante una crisis.

Como se muestra en la Figura 1, la “resiliencia de Internet” abarca muchos componentes subyacentes⁴, que van desde la resiliencia de la infraestructura física y de energía de Internet hasta la resiliencia del mercado y la calidad de servicio (QoS), es decir, desempeño, disponibilidad, ancho de banda disponible, etc.

Definiciones:

- Resiliencia de Internet a nivel de país: la capacidad del ecosistema de Internet nacional de un país (los ISP, regulaciones, infraestructura física, estructura de mercado) para proporcionar servicios de Internet a sus ciudadanos a un nivel de servicio aceptable frente a fallas y desafíos para las operaciones normales.
- Resiliencia de la infraestructura crítica: la resiliencia de la infraestructura de energía, la infraestructura de cable de Internet (tanto terrestre como submarina), así como la infraestructura de dominio de nivel superior con código de país (ccTLD).
- Resiliencia del mercado: la disponibilidad y eficiencia de los puntos de intercambio de Internet (IXP) y la capacidad de mantener local el tráfico local, la capacidad del mercado para autorregularse y ofrecer precios asequibles a los usuarios finales manteniendo un mercado diverso y competitivo.
- Resiliencia de la red/ISP: la capacidad de una red para continuar brindando un nivel aceptable de servicio en caso de una interrupción o durante una crisis. Este componente de resiliencia se compone de varios componentes, como la resiliencia de los enlaces físicos, los enlaces lógicos/de peering, el desempeño, la calidad de servicio y el DNS.

Alcance y objetivos:

En nuestro marco de evaluación, consideraremos los siguientes aspectos:

1. La disponibilidad y estabilidad de la infraestructura física, que incluye centrales eléctricas, fibra submarina o terrestre, estaciones terrestres y redes de acceso de última milla.
2. La calidad de servicio (QoS) de la red desde la perspectiva del usuario final y la estabilidad de la red en términos de accesibilidad, desempeño y latencia a los servidores de destino seleccionados.
3. La disponibilidad y el rendimiento del ecosistema del sistema de nombres de dominio (DNS).
4. La disponibilidad y eficiencia del tejido de emparejamiento local, así como la capacidad del país para mantener local el tráfico local.
5. La resiliencia del mercado de ISP, es decir, el nivel de concentración hacia Sistemas Autónomos (AS) específicos y la asequibilidad.

2 Enfoque Y Objetivos

En este proyecto, recopilaremos datos de acceso para los números de sistemas autónomos (ASN) en África y usaremos los datos para analizar métricas de resiliencia, confiabilidad y desempeño de la red para la comunicación entre ASN. Nuestra definición principal de resiliencia se basará en la capacidad de una red para tolerar, solucionar y recuperarse de incidentes de red, como los causados por fallas de dispositivos y cortes de fibra [10], [14]. Al considerar la topología física, estudiaremos la resiliencia geográfica desde las perspectivas integral y de ISP (ASN). Además, se analizarán otras dos métricas relacionadas: desempeño y confiabilidad. Todas las métricas consideradas en este proyecto se evaluarán al nivel de ASN, así como a nivel de ciudad y país. Desde el punto de vista geográfico, agruparemos los enrutadores dentro de diferentes niveles de proximidad como ciudad, país y región. Este análisis se realizará independientemente de la topología a nivel ASN.

⁴ El diagrama muestra el alcance inicial del proyecto y no es una lista completa de todos los posibles aspectos de la resiliencia.

2.1 // Descripción general del diseño

Como se muestra en la Figura 2, el marco MIRA se compone de varios componentes básicos. El Panel Internet Society Pulse permitirá a los usuarios finales visualizar los datos recopilados en el marco del proyecto MIRA. Los usuarios podrán construir paneles personalizados de acuerdo con sus necesidades. Por ejemplo, los usuarios podrán elegir sus índices y construir su propio índice final. El panel Internet Society Pulse extraerá datos utilizando la API de MIRA, que también pueden utilizar los programadores para recuperar datos de MIRA sin utilizar la GUI. La canalización de análisis es responsable de generar los índices basados en los datos recopilados (primarios o secundarios).

El marco de resiliencia de Internet (4.2 WP2: Marco de resiliencia de Internet) proporcionará las especificaciones sobre cómo procesar los datos. Los datos vendrán a través de la canalización de datos, que almacenará y agregará conjuntos de datos primarios y secundarios. Los datos primarios se recopilarán a través de nodos de medición fijos y móviles basados en Raspberry Pi, que ejecutan herramientas de medición, como sondas RIPE Atlas⁵ y el cliente de la herramienta de diagnóstico de red (NDT) de M-Lab⁶. Las secuencias de comandos de medición de la red se basan en herramientas estándar existentes y serán instalados y organizados por el administrador de medición de MIRA. Los datos secundarios provendrán de múltiples fuentes abiertas de datos de Internet, como datos de enrutamiento de IXP, información de asignación de RIR y tablas de enrutamiento del protocolo BGP.

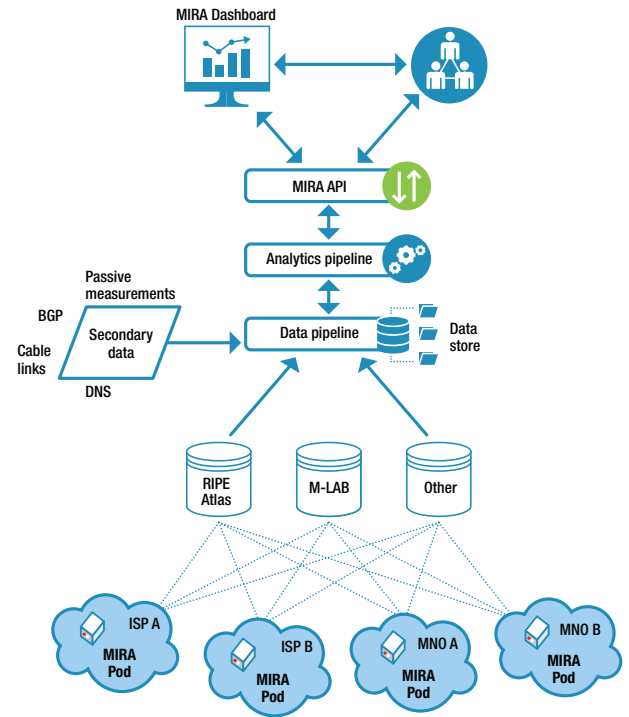


Figura 2: Flujo de trabajo de visualización y recopilación de datos MIRA

2.2 // Métricas

2.2.1 Infraestructura crítica con diversidad de ruta.

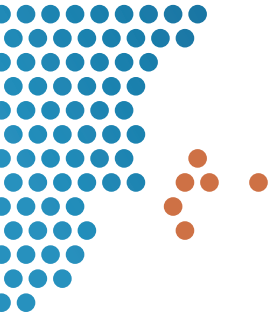
Un enfoque importante para garantizar una Internet resiliente es mediante el aumento de la diversidad de rutas de redes entre cualquier par de hosts de Internet. [10], [15]. En este contexto, la diversidad es el grado en que las rutas alternativas comparten los mismos nodos y enlaces. [15]. Para ser más resiliente a las fallas, es necesario que haya múltiples rutas de enlace y nodos independientes entre las redes [16]. Fundamentalmente, la diversidad de rutas entre hosts conectados a diferentes redes está determinada tanto por la infraestructura física (topología física) como por las políticas de enrutamiento (intra e interdominio) y las políticas de emparejamiento. Inherentemente, la diversidad de rutas se mejora con el alojamiento múltiple por parte de los AS y los hosts. Por lo tanto, es importante estudiar la diversidad de rutas físicas y lógicas en múltiples redes.

2.2.2 Desempeño y calidad del servicio (QoS).

Los operadores de redes por lo general miden el desempeño de la red en términos de calidad estándar del servicio (QoS), como desempeño, demora, fluctuación y pérdida de paquetes. Los operadores pueden, por ejemplo, estar interesados en monitorear la congestión y la pérdida de paquetes en enlaces dentro o entre redes. Para los usuarios de Internet, las métricas de QoS son útiles solo en términos de la forma cómo impactan en la comunicación integral y cómo se ve afectada su calidad de experiencia (QoE). En este caso, QoE describe una evaluación subjetiva de la experiencia de un usuario cuando utiliza un servicio de red en particular [20]. Por ejemplo, en relación con la congestión y la pérdida de paquetes, un usuario generalmente solo estaría interesado en el desempeño efectivo de sus aplicaciones, incluida la determinación de la capacidad y la QoE al utilizar medios enriquecidos en un servicio de red determinado. Si el rendimiento de una

⁵ <https://atlas.ripe.net/probes>

⁶ <https://pypi.org/project/murakami>



red se degrada gravemente, como por congestión o falla del dispositivo, puede provocar la interrupción del reenvío de paquetes y causar brechas donde el servicio de red no está disponible de manera efectiva. Y esto está vinculado a otro aspecto de este proyecto: la confiabilidad de la red.

2.2.3 Confiabilidad de la red.

La confiabilidad de la red es una noción que abarca varias métricas de estabilidad que son importantes para la disponibilidad y usabilidad sostenidas de los servicios de red. Una métrica clave de la confiabilidad de la red es el tiempo de actividad, que es una medida del porcentaje de tiempo que un servicio de red está disponible. El nivel de tiempo de actividad de la red determina si un usuario puede acceder a los servicios de Internet en todo momento. Por lo tanto, desde el punto de vista del usuario, podemos medir la confiabilidad de Internet en términos de tiempo de actividad y accesibilidad, pudiendo llegar a cualquier red y servicio de Internet en cualquier momento [17].

2.3 // Medición de la diversidad de rutas

Para medir y evaluar la resiliencia de Internet con respecto a la diversidad de rutas, implementaremos un marco de medición para identificar saltos geográficamente equivalentes en datos de traceroute y luego calcularemos métricas de diversidad geográfica para pares de puntos finales.

2.3.1 Paris-Traceroute

A través de las mediciones de traceroute, recopilaremos rutas a nivel de IP entre los puntos finales seleccionados, tanto dentro de las áreas geográficas específicas (diversidad interna) como entre diferentes áreas (diversidad externa). Un aspecto importante de la medición de la diversidad de rutas es identificar tantas rutas alternativas como sea posible entre cualquier par de redes o puntos finales. Para lograr esto, nuestro marco de medición usará Paris-Traceroute⁷ y ejecutará repetidamente las mediciones entre cada par de puntos finales.

2.3.2 Agrupación geográfica

En primer lugar, utilizaremos múltiples bases de datos de geolocalización, como RIPE IPmap⁸, MaxMind⁹ e IPInfo¹⁰, así como mediciones activas para determinar las ubicaciones geográficas (nivel de ciudad y país) de los saltos IP de traceroute. A partir de entonces, podremos agrupar los saltos en función de zonas geográficas en múltiples niveles de granularidad, y esto nos permitirá identificar rutas geográficamente equivalentes. Luego determinaremos la equivalencia geográfica de las rutas y calcularemos los índices de diversidad geográfica entre las ubicaciones seleccionadas y los puntos finales [18].

2.3.3 Mapeo de topología física y lógica

Para conocer la resiliencia de Internet con respecto a la diversidad geográfica de las rutas, estudiaremos el problema de mapear la topología lógica en la infraestructura de red física [22]. En este contexto, la topología lógica consta de conjuntos de nodos IP o ASN, con bordes que denotan la relación entre redes, como las relaciones cliente-proveedor o de emparejamiento. Por otro lado, una red física denota un conjunto de nodos físicos (por ejemplo, enrutadores fronterizos e IXP), con bordes que representan enlaces de comunicación física, principalmente sistemas de cable. El objetivo es evaluar y comparar la diversidad de las rutas físicas y lógicas entre las redes.

2.4 // Medición de la confiabilidad y el desempeño de la red

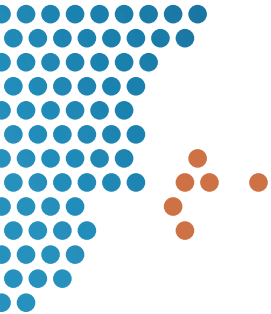
Realizaremos mediciones activas integrales a largo plazo para evaluar la confiabilidad (tiempo de actividad y accesibilidad), así como el desempeño de las redes en África. Las mediciones activas consisten en enviar paquetes de sondeo desde una fuente (punto de vista) a un destino. Estas mediciones activas nos permitirán analizar las colas de red, las pérdidas, los retrasos, el desempeño, los comportamientos de enrutamiento y los retrasos de propagación. Para lograr resultados confiables y completos, las mediciones deberán realizarse entre una gran cantidad de puntos estratégicos distribuidos geográficamente.

⁷ Paris traceroute es otra versión de una conocida herramienta de diagnóstico de redes (traceroute). Aborda los problemas causados por los balanceadores de carga con la implementación inicial de traceroute. Obtenga más información aquí: <https://paris-traceroute.net>

⁸ <https://ipmap.ripe.net>

⁹ <https://www.maxmind.com>

¹⁰ <https://ipinfo.io>



Ya existen múltiples plataformas de medición de Internet con sondas que pueden utilizarse para ejecutar mediciones de red repetidamente. Algunos de los más importantes incluyen, SamKnows¹¹, Speedchecker¹², Archipelago¹³, RIPE Atlas¹⁴ y M-Lab¹⁵. RIPE Atlas tiene aproximadamente 12 mil sondas de hardware en todo el mundo. Sin embargo, a partir de 2018, solo había 229 sondas RIPE Atlas activas en África. En febrero de 2021, solo 194 estaban conectadas y activas. La mayoría de estas sondas las despliegan los operadores de redes en sus redes internas y una pequeña cantidad de sondas están alojadas en viviendas particulares.

Speedchecker es una plataforma de medición activa con un número relativamente mayor de puntos estratégicos en África. En 2018, Speedchecker tenía hasta 850 sondas en África que cubrían 52 países. Al igual que RIPE Atlas, Speedchecker admite una amplia gama de pruebas de red, incluidas Ping (TCP/ICMP), DNS, Traceroute y HTTP. Archipelago de CAIDA tiene actualmente 10 monitores activos en África, y estos monitores actúan como sondas dedicadas que ejecutan repetidamente pruebas de medición de red destinadas a descubrir la topología de Internet y medir el desempeño de la red.

M-Lab es otra plataforma que permite a los usuarios de la web ejecutar pruebas de desempeño desde sus navegadores. Sin embargo, M-Lab tiene solo siete servidores activos en África que actúan como objetivos de las mediciones de desempeño, y esto limita la confiabilidad de los resultados desde muchos puntos de observación. Por fortuna, M-Lab mantiene un vasto depósito de herramientas existentes, y algunas de ellas se pueden personalizar como clientes y servidores para diferentes campañas de medición. Por ejemplo, la herramienta de diagnóstico de red¹⁶ (NDT) proporciona información detallada a nivel de paquete junto con estadísticas a nivel de kernel sobre el rendimiento de una conexión TCP en una ruta determinada. Por lo tanto, NDT se puede utilizar para determinar las causas de las velocidades lentas, así como para verificar los proxys y los dispositivos NAT entre la máquina que ejecuta las pruebas y el servidor M-Lab. Para este proyecto, se desarrollará e implementará un cliente NDT personalizado utilizando Raspberry Pi (módulos MIRA) y se ejecutarán pruebas en nuestros servidores personalizados.

Inicialmente, el proyecto MIRA priorizará el trabajo con las sondas de software M-Lab y RIPE Atlas.

2.5 // Acumulación de métricas

La medición de características de red específicas (QoS, latencia, fluctuación, QoE, pérdida de paquetes, desempeño, diversidad de rutas, etc.) ha sido una rutina diaria y un enfoque ampliamente aceptado para evaluar el desempeño o la resiliencia de la red. Se supone que esta información ayuda a los ingenieros, reguladores, dirección (y otros responsables políticos), así como a los usuarios finales a tomar acciones proactivas para modificar y mejorar el desempeño y la resiliencia de la red. Sin embargo, para cuantificar de manera eficiente el efecto de nuestras acciones, necesitamos agregar estas métricas individuales. Los ingenieros necesitan mediciones acumuladas para destinar sus escasos recursos en la mejora de las redes. Los responsables políticos necesitan estas mediciones acumuladas para orientar sus decisiones de financiamiento y establecer regulaciones. Los usuarios necesitan estas métricas compuestas en su búsqueda de una mejor experiencia de usuario. Desafortunadamente, no es trivial acumular varias métricas en resultados significativos. En la actualidad, no existe una forma sistemática de evaluar el desempeño y la resiliencia de una red dado un vector de medidas de red.

El principal desafío que hace que sea casi imposible acumular métricas de red de manera sólida es la falta de “datos reales”. Por lo general, por “datos reales” se entiende la información recopilada en el lugar. Por ejemplo, en Física, los “datos reales” proviene del mundo físico. En las redes informáticas, es difícil obtener datos reales para medidas como la pérdida de paquetes, el desempeño, etc. Sin embargo, se deben obtener respuestas para tomar decisiones informadas y evaluar si nuestras acciones han mejorado o disminuido la resiliencia de la red.

Para este proyecto proponemos definir (no descubrir) una verdad fundamental para tales mediciones. Nuestro enfoque se basará en las opiniones de los expertos y, con base en ellas, definiremos los métodos de acumulación asignando la ponderación o el coeficiente adecuado a las métricas recopiladas.

¹¹ <https://www.samknows.com>

¹² <http://speedchecker.com>

¹³ <https://www.caida.org/projects/ark>

¹⁴ <https://atlas.ripe.net>

¹⁵ <https://www.measurementlab.net>

¹⁶ <https://software.internet2.edu/ndt>

2.6 // Fuentes de datos

En este proyecto utilizaremos fuentes de datos primarias y secundarias. Las fuentes primarias provendrán de campañas de medición activas y pasivas, mientras que los datos secundarios se extraerán de información de terceros, como la tabla de enrutamiento de BGP, conjuntos de datos de IXP, información de ccTLD, etc. Para que nuestro marco sea sostenible, debemos asegurarnos de que nuestras fuentes de datos estén abiertas, sean confiables y estén actualizadas y sigan proporcionando datos durante un largo período de tiempo. Esto nos permitirá extraer información de las tendencias sobre un tema en particular. El Apéndice 1 es una lista de fuentes de datos, su propósito y categoría.

3 Programa de Trabajo

El programa de trabajo se divide en paquetes de trabajo (WP), concretamente: Etapa 1, dominada por la implementación y prueba del banco de pruebas y el desarrollo del marco de resiliencia de Internet (WP1, WP2). La Etapa 2 consiste en recopilar y analizar las mediciones de red y otras fuentes secundarias de datos disponibles (WP3, WP4). La Etapa 3 se trata de organizar todos los datos capturados, acumularlos, ejecutar análisis estadísticos y proporcionar información a los usuarios finales (WP7). La Figura 3 muestra cómo cada WP se alimenta uno del otro.

Nota: WP5 (medidas móviles) y WP6 (resiliencia de DNS) se llevarán a cabo en una etapa posterior (TBD).

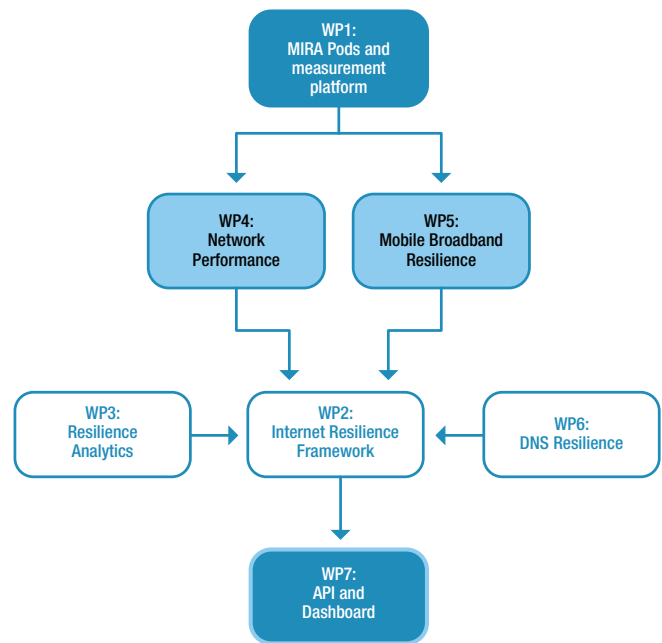


Figura 3: Flujo de trabajo de información entre los paquetes de trabajo (WP) identificados.

3.1 // WP1: Fuentes de datos e infraestructura de medición

Este WP diseñará e implementará pequeños dispositivos llamados Módulos MIRA. Los Módulos son pequeños dispositivos que se dedicarán a realizar las mediciones. En este punto, los módulos son Raspberry Pi. Esto contará con el apoyo de AfriNIC e Internet Society mediante la compra de los dispositivos de medición y la gestión del panel de medición en Internet Society Pulse.

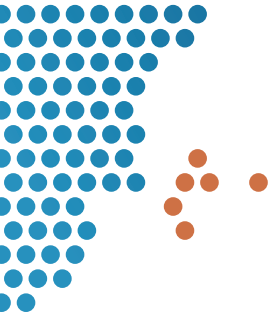
Nota: esto se vinculará a WP5: mediciones de banda ancha móvil

3.1.1 Tarea 1: Módulos de medición

La primera tarea es diseñar y construir la infraestructura adecuada para lanzar las mediciones (por ejemplo: para mediciones de desempeño o latencia). Para ello, aprovecharemos los sistemas de medición existentes, incluido RIPE Atlas o el cliente NDT de M-Lab. Estos dispositivos de medición se llamarán Módulos MIRA. Deben ser livianos y fáciles de conectar a cualquier red. Los Módulos MIRA ejecutarán contenedores virtualizados ligeros (por ejemplo: Docker o LXD) que ejecutarán las diferentes tareas de medición. Debería ser bastante fácil mover o clonar las tareas de medición de un módulo a otro. AfriNIC e Internet Society apoyarán el despliegue de los módulos en algunos países africanos con el apoyo de los Capítulos locales de Internet Society y otros participantes dispuestos.

3.1.2 Tarea 2: Organización de módulos.

Un aspecto importante es la organización y la gestión de los módulos MIRA. Debería ser fácil escindir y programar mediciones desde un sistema centralizado. El organizador debe tener acceso a los módulos MIRA y recuperar el estado de salud de los módulos, así como el estado de las mediciones. El organizador también coordinará las campañas de medición y recopilación de datos en diversos conjuntos de módulos. Será responsable de recopilar datos de los módulos. Los controles de acceso a los datos serán cruciales para esto, permitiendo que múltiples abstracciones de datos estén expuestas a diferentes partes.



3.1.3 Tarea 3: Canalización y almacenamiento de datos

El sistema debe poder manejar datos primarios de los módulos y datos de terceros que se utilizarán para complementar las mediciones. Los módulos MIRA generarán una gran cantidad de datos de medición con el tiempo. Esto significa que la capa de “canalización y almacenamiento de datos” necesita: (1) manejar una gran cantidad de datos, (2) realizar la acumulación y (3) descartar los datos innecesarios. Una API debería permitir un fácil acceso a los datos recopilados. En esta tarea, utilizaremos técnicas de almacenamiento de última generación (por ejemplo, noSQL, clústeres de Hadoop, etc.) para aumentar la escalabilidad y la facilidad de uso.

3.2 // WP2: Marco de resiliencia de Internet

En este WP, desarrollaremos herramientas para acumular métricas de resiliencia de las redes. Dicha acumulación nos permitirá derivar valores resumidos que pueden dar indicaciones de forma rápida e intuitiva sobre la capacidad de recuperación de la red. Primero estableceremos la base teórica de la acumulación aprovechando datos reales que planeamos definir.

En la primera fase, construiremos un marco simple acumulando los diferentes índices usando una fórmula simple. En una etapa posterior, crearemos un marco más complejo que aprovechará las opiniones de los expertos y luego utilizaremos el aprendizaje automático para refinar aún más el marco.

Los datos reales también servirán para validar y recalibrar continuamente nuestra herramienta de acumulación. Una vez que se establezcan nuestros métodos de acumulación de métricas, los pasaremos a la canalización de análisis, que define cómo las diferentes métricas (medidas desde diferentes puntos de observación) se enviarán a los módulos de acumulación. Por último, con una acumulación sólida de las métricas de resiliencia, los operadores de red podrán establecer un punto operativo de referencia y dirigir continuamente la red hacia el valor de referencia deseado.

3.2.1 Tarea 1: Marco teórico

En esta tarea, nuestro objetivo es desarrollar la base teórica para acumular métricas de resiliencia de la red. Esto debe comenzar identificando las métricas que se pueden utilizar para evaluar de manera efectiva el nivel general de resiliencia de los sistemas. Luego, estas métricas se acumularán para proporcionar un breve resumen de la resiliencia de la red en forma de índice, llamado Índice de Resiliencia de Internet. Construiremos las herramientas de acumulación respondiendo a dos preguntas principales: (1) ¿cómo agregar medidas de métricas similares tomadas desde puntos estratégicos dentro de la red y medidas recopiladas para diferentes métricas de la misma red? Y (2) ¿cómo agregar métricas con un efecto de ampliación y alejamiento a diferentes niveles, como ciudad, país y región? La métrica acumulada se asignará a puntajes numéricos que luego se traducirán en una representación cualitativa (como baja, media, alta y crítica) para ayudar a las organizaciones a evaluar y priorizar adecuadamente sus procesos de decisión.

Para ayudar a construir la base teórica y validar nuestras teorías, definiremos unos datos reales para las métricas de resiliencia de la red.

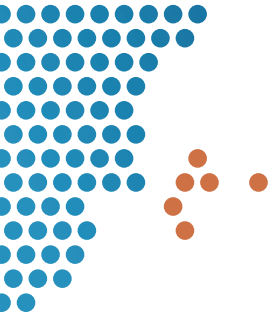
3.2.2 Tarea 2: Evaluación comparativa y datos reales.

Proponemos desarrollar y documentar un procedimiento que siga principios científicos sólidos y que permita aprovechar el conocimiento experto humano para construir una matriz de resiliencia a partir de las métricas de resiliencia elegidas. Además, permitirá la colaboración de múltiples personas expertas de manera que los datos reales utilizados para el proceso de acumulación se basen en el conocimiento conjunto de estas personas expertas.

Internet Society y AfriNIC mantienen bases de datos de personas expertas en este campo. Proponemos proporcionarles nuestro proceso y las herramientas asociadas para permitirles evaluar la precisión de nuestros puntajes de acumulación (para comparar lo que su opinión experta dice que debe ser un puntaje con lo que realmente es el puntaje). A medida que aumenta la experiencia humana y cambia nuestra comprensión de la resiliencia de la red, los puntajes “reales” cambian (según la opinión de los expertos humanos). El resultado es que nuestra verdad fundamental y nuestras métricas cambiarán con el tiempo. Al utilizar este nuevo conocimiento, calibraremos y mejoraremos sistemáticamente nuestros métodos acumulados.

3.2.3 Tarea 3: Canalización de análisis.

La canalización de análisis albergará unidades de cálculo discretas denominadas Módulos de análisis. Estos módulos serán definidos por el marco de resiliencia de Internet. Estos recibirán flujos de datos de los módulos MIRA y otras fuentes, y luego los transformarán en una forma procesada (por ejemplo, centralidad informática de mapas de topología). Esta tarea desarrollará las API y el marco para ejecutar estos módulos de manera escalable.



Tener métodos de acumulación métrica permitirá a los operadores de redes y proveedores de servicios definir puntos de referencia y dirigir continuamente el sistema hacia el punto deseado. El objetivo de resiliencia refleja los requisitos de los usuarios finales, reguladores y otras partes interesadas de un punto operativo aceptable. La dirección continua de la red podría realizarse siguiendo marcos de orientación como el marco de resiliencia de la red NIST [23] y el marco de resiliencia de Sterbenz et al. [18]. Un ejemplo (siguiendo el marco de cinco pasos NIST) podría ser:

1. Proteger: tomando medidas “proactivas” para mantener la red en el punto operativo deseado.
2. Detectar: indicaciones de degradación de la resiliencia de la red, que deberían reflejarse en una disminución en el puntaje.
3. Identificar: las métricas/parámetros que son más relevantes para la degradación de la resiliencia.
4. Responder: solucionar adoptando medidas “reactivas” para que el sistema vuelva al punto de funcionamiento deseado.
5. Recuperar: a pesar de la supervisión y la protección continuas, el sistema podría sufrir eventualmente una falla desastrosa (debido a causas intencionales o no intencionales). Esto conducirá a una degradación sustancial en el puntaje de resiliencia. Se adoptarán las medidas apropiadas para recuperarse de tal desastre.

3.3 // WP3: Análisis de resiliencia

Este paquete de trabajo se centra en cuantificar la resiliencia de Internet africana en tres niveles.

3.3.1 Tarea 1: Análisis de topología física.

En esta tarea, evaluaremos la diversidad de cables submarinos situados en el continente, así como los cables terrestres que recorren el continente. También cuantificaremos los elementos físicos, como estaciones e IXP. Este paquete de trabajo proporcionará (al Marco de resiliencia - WP2) métricas sobre la diversidad de cables y estaciones en los respectivos países y ciudades. Estos datos nos permitirán evaluar y comparar, en métricas cuantificables, la diversidad de rutas físicas dentro y entre países, ciudades y redes.

3.3.2 Tarea 2: Análisis de topología lógica.

En esta tarea, deduciremos dependencias con respecto al enrutamiento entre ISP en todo el continente y su dependencia de proveedores fuera del continente. Nos basaremos en las mediciones de Paris-Traceroute para recopilar rutas lógicas entre los puntos finales seleccionados con el objetivo de identificar rutas alternativas. Además de los datos de Traceroute, también utilizaremos conjuntos de datos de BGP para inferir la diversidad de rutas lógicas entre redes y países.

En particular, interactuaremos con ARDA¹⁷, un sistema que sintetiza la información de enrutamiento y de emparejamiento disponible públicamente recopilada por los recopiladores de rutas en África, especialmente de los recopiladores de rutas de RouteViews¹⁸ y Packet Clearing House¹⁹ (PCH). El resultado clave del paquete de trabajo serán los valores de índice que representan la diversidad de rutas lógicas de redes y países.

3.3.3 Tarea 3: Mapeo de la topología física y lógica.

Esta tarea implicará mapear la topología lógica en la infraestructura de red física. El objetivo es identificar la infraestructura física (cables, puntos de aterrizaje, etc.) que utilizan las distintas ASN. El objetivo es evaluar y comparar la diversidad de las rutas físicas y lógicas entre las redes. Además de identificar los cables, también marcaremos las instalaciones de interconexión y los IXP que son fundamentales para la estabilidad de Internet en el continente. Además, los flujos de tráfico de los países africanos estarán asociados a los cables respectivos. Un índice clave de esta tarea será la diversidad de rutas físicas internacionales para países y redes.

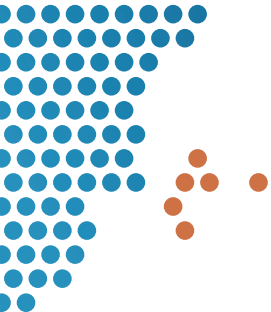
3.3.4 Tarea 4: Posibilidad de puntos de embotellamiento y hegemonía AS.

Internet está compuesta de numerosas redes que dependen una de la otra para brindar conectividad global. Esto significa que la accesibilidad de una red depende de la conectividad con otras redes. Esta interdependencia generalmente refleja las limitaciones políticas y económicas dentro de las fronteras nacionales. Cuando existe una dependencia acumulada de algunas redes específicas para la conectividad global, esta concentración puede representar un “punto de embotellamiento”. Este tarea trata la medición de la posibilidad de puntos de embotellamiento [19] o la hegemonía AS [20] de un país.

¹⁷ African Route-collector Data Analyzer[5]

¹⁸ <http://www.routeviews.org>

¹⁹ <https://www.pch.net>



3.4 // WP4: Desempeño de la red

3.4.1 Tarea 1: Desempeño de acceso.

Uno de los mayores desafíos en el despliegue de nuevos servicios en África es la baja calidad del servicio de banda ancha en ciertas regiones. Cuantificar esto es de vital importancia para los reguladores, así como para los operadores de redes (incluidos los nuevos participantes) que desean orientar mejor sus esfuerzos. MIRA proporcionará la posibilidad de monitorear la calidad de la experiencia (QoE) del usuario para proveedores de servicios móviles, Wi-Fi público y de banda ancha en el hogar. Esto irá más allá de las pruebas de desempeño básicas y se centrará en capturar las experiencias del usuario final en un conjunto diverso de servicios. La métrica clave de esta tarea serán los índices que representen la QoE en redes y países.

3.4.2 Tarea 2: Infraestructura de peering.

Tomar decisiones con respecto al despliegue y la interconexión de la infraestructura (por ejemplo, redes, servidores de contenido) puede ser difícil, particularmente en los entornos en desarrollo y altamente dinámicos que se encuentran en toda África. Se ha documentado ampliamente que el peering tiene un efecto positivo en la mayoría de las métricas de desempeño de Internet. También es bien sabido que África está muy por detrás de Europa en términos de su infraestructura de peering. Esta tarea utilizará los datos de MIRA en el panel de Internet Society Pulse para extraer las métricas relevantes para ofrecer consejos a los proveedores de redes y contenido, que deseen saber si deben hacerlo, con quién deben hacerlo y dónde debe ocurrir. Esto tendrá un enfoque particular en los IXP que se están desplegando en la región, que es uno de los principales objetivos estratégicos de la Unión Africana. Los operadores de redes y los proveedores de contenido podrán ingresar información estadística sobre su tráfico y necesidades, y esta información luego se fusionará con los datos recopilados por MIRA (por ejemplo, rutas conocidas, ubicaciones de PoP, disponibilidad de IXP), para recomendar redes y ubicaciones para el peering. Las métricas clave de esta tarea serán índices que representen la potencia de peering de las redes. El sistema ARDA será una fuente de información para esta tarea.

3.4.3 Tarea 3: Mantener local el tráfico local.

Mantener los servicios y el contenido de Internet lo más cerca posible de los usuarios finales contribuye a hacer de Internet un ecosistema más seguro y robusto. Los IXP juegan un papel importante al establecer relaciones de peering (intercambio de tráfico) entre los ISP, proveedores de contenido y operadores de redes de entrega de contenido (CDN), lo que les permite intercambiar tráfico localmente. Esta tarea analizará hasta qué punto se aloja y distribuye el contenido local popular dentro de un país y cuál es el impacto relativo en la calidad de la experiencia desde la perspectiva de los usuarios finales. Esto se logrará ejecutando mediciones desde los módulos MIRA.

3.4.4 Tarea 4: Interferencia de red y web.

Una preocupación creciente es la privacidad web, la interceptación (por ejemplo, la inyección de encabezados HTTP) y la limitación de velocidad. Esta tarea hará uso de herramientas existentes como OONI²⁰ que se basa en mediciones activas para detectar la interferencia del tráfico web, así como las tecnologías que sustentan la interferencia del tráfico. Esto se hará mediante mediciones activas de TCP, DNS, HTTP y TLS. En esta tarea, también aprovecharemos los datos de terceros de otros servicios de monitoreo de censura para extraer tendencias.

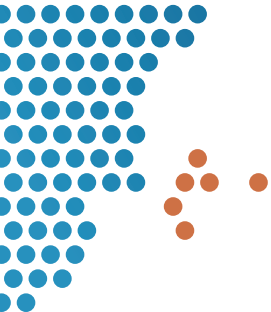
3.5 // WP5: Resiliencia de la red de banda ancha móvil

En este paquete de trabajo buscamos desarrollar una comprensión integral de la capacidad de uso de Internet móvil en la región, desde una amplia variedad de puntos de observación.

3.5.1 Tarea 1: Adaptar las herramientas de medición móvil existentes.

Esta tarea se basa en esfuerzos anteriores para medir y catalogar los problemas del uso de Internet móvil en algunos países de la UE. En esta tarea, (a) adaptaremos una aplicación de medición móvil existente al contexto africano, incluida la integración de una lista de servicios de información cruciales en África, (b) estudiaremos la capacidad de uso y la calidad del acceso a Internet para la región (c) trabajaremos con colaboradores de investigación locales para realizar mediciones de campo en sus propios países.

²⁰ <https://ooni.org>



3.5.2 Tarea 2: Capacidad de uso de la banda ancha móvil.

En esta tarea, desarrollaremos una comprensión integral de la capacidad de uso de la conectividad móvil en África, desde una amplia variedad de puntos de vista. Esto proporcionará, por primera vez, una imagen completa del estado del acceso a Internet en la región.

3.5.3 Tarea 3: Lista informada de servicios cruciales.

En esta tarea, ejecutaremos mediciones de QoE en una lista informada de diferentes sitios web que brindan “servicios de información cruciales” en toda la región. Dicha lista proporcionará una taxonomía y una categorización claras del sinfín de fuentes de información pública y comercial en la región. Mediremos y catalogaremos los problemas que surgirán en el acceso a servicios cruciales en la región, proporcionando indicaciones a los legisladores sobre dónde y cómo enfocarse para minimizar la brecha digital en la región.

3.6 // WP6: Resiliencia de la infraestructura de DNS

Al utilizar varias fuentes de datos, este WP profundizará en el ecosistema del DNS africano. Con este fin, examinaremos la confiabilidad de la infraestructura de DNS en el continente tanto para resolver contenido fuera del continente como dentro de este. Esto implica examinar el alojamiento, la confiabilidad y el desempeño de los ccTLD africanos y todos los servicios de DNS globales con presencia en África. Dos estudios recientes de AfriNIC destacaron una serie de problemas que pueden afectar la resiliencia del ecosistema del DNS.^{21,22}

3.6.1 Tarea 1: Resiliencia de ccTLD.

Muchos ccTLD africanos no cumplen con las recomendaciones de BCP-16²³ al colocar servidores de nombres en ubicaciones tanto topológica como geográficamente diversas, para minimizar la probabilidad de que una sola falla los deshabilite a todos. Investigaremos si los ccTLD africanos cumplen con el requisito mínimo BCP-16 de tener al menos dos IP para prestar servicio en sus zonas.

3.6.2 Tarea 2: Adopción y uso de DNSSEC.

Queremos saber cuáles de los ccTLD africanos han adoptado DNSSEC y han firmado su zona. Además, con base en los datos obtenidos de APNIC²⁴, podemos observar quién está realizando la validación de DNSSEC.

3.6.3 Tarea 3: Desempeño de Do53 / DoH / DoT.

Compararemos el desempeño de Do53 (DNS tradicional), DNS sobre TLS (DoT) y DNS sobre HTTPS (DoH) en diferentes condiciones de red (móvil y fija). Descubriremos las causas de la latencia y las rutas tortuosas de resolución de DNS, que amplifican el impacto en el desempeño de los protocolos DNS seguros en el tiempo de resolución de DNS y el tiempo de carga de la página.

3.7 // WP7: Panel MIRA

Este WP se ocupa principalmente de la difusión de los datos (después del procesamiento) a través de un panel de visualización alojado en la plataforma Internet Society Pulse y una API para permitir una fácil recuperación de los datos.

3.7.1 Tarea 1: API para uso externo.

Una API proporcionará un fácil acceso a los diferentes índices recopilados, así como a los datos recopilados para calcular el índice. Los datos deben estar disponibles durante un período de tiempo razonable para permitir un análisis longitudinal.

3.7.2 Tarea 2: Panel de visualización

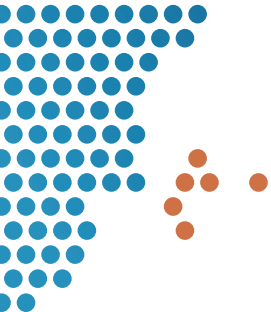
MIRA presentará los datos utilizando la plataforma Internet Society Pulse, que será personalizable en función de las necesidades de los usuarios finales (por ejemplo, reguladores, ISP, etc.). Primero, el usuario verá un mapa de calor de África con los países coloreados según el “Índice de resiliencia de Internet” que se calculará en el WP2. Será posible comparar dos o más países uno al lado del otro. Luego, el usuario puede sumergirse en índices más granulares que en conjunto contribuyeron al índice macro de resiliencia de Internet. Es probable que los participantes que alojan sondas de medición tengan acceso a más datos internos (backend) que los usuarios normales.

²¹ <https://afrinic.net/research/african-ccTlds-technical-environment>

²² <https://afrinic.net/research/african-dns-authoritative-nameservers>

²³ <https://tools.ietf.org/html/bcp16>

²⁴ <https://stats.labs.apnic.net/dnssec>



4 Difusión

La difusión de los resultados del proyecto se hará a través del portal de la plataforma Internet Society Pulse que estará disponible de manera abierta para todos los usuarios de Internet. Los participantes en el proceso de medición que alberguen sondas de medición o infraestructura podrán obtener más datos técnicos del proyecto MIRA

4.1 // Reclutamiento de hosts para módulos MIRA

La sostenibilidad y precisión del proyecto MIRA dependerá del número de módulos MIRA que lleven mediciones activas en África. Por lo tanto, es importante reclutar y mantener un grupo sustancial de hosts de módulos.

AfriNIC e Internet Society, a través de sus relaciones con investigadores, comunidades técnicas y los Capítulos de Internet Society, mantienen una lista de hosts voluntarios. A medida que el proyecto evolucione, continuaremos reclutando nuevos hosts.

4.2 // Compromiso y desarrollo de capacidades

A través del Grupo de trabajo de medición de AfriNIC, pretendemos organizar una serie de talleres en torno al amplio tema de las mediciones de Internet. Tenemos la intención de cubrir áreas temáticas como la medición del desempeño de la red, el monitoreo de QoE y la censura de Internet. Invitaremos a operadores de infraestructura de medición como M-Lab, OONI, RIPE Atlas a contribuir con nuestras sesiones del taller. Tenemos la intención de organizar los siguientes talleres:

1. Taller 1: AIS 2021, junio de 2021
2. Taller 2: AfPIF 2021, agosto de 2021
3. Taller 3: SAFNOG 2021, noviembre de 2021

Además, cada paquete de trabajo se dividirá en varios estudios científicos. Los resultados se difundirán en forma de publicaciones científicas (ponencias de congresos o publicaciones en revistas), publicaciones en blogs e informes técnicos. En general, pretendemos hacer que nuestros hallazgos sean muy accesibles para diferentes audiencias (técnicas y menos técnicas).

5 Ejecución Y Mapa de Ruta

El Apéndice 2 proporciona una descripción general de las tareas y plazo de ejecución.

5.1 // Infraestructura de la medición

El proyecto MIRA llevará a cabo mediciones inicialmente utilizando la herramienta Murakami de M-Lab y agregará el RIPE Atlas de RIPE NCC en los próximos meses. Tenemos la intención de agregar herramientas adicionales de acuerdo con las necesidades futuras. Ambas herramientas son compatibles con clientes de software que se pueden instalar en una variedad de sistemas operativos y pueden realizar varias mediciones de Internet. El software se instalará en pequeños Raspberry Pi que llamamos módulos MIRA. Elegimos esta tecnología para permitir que se lleven a cabo mediciones ininterrumpidas y dedicadas en hardware ligero y de bajo consumo que se puede obtener fácilmente en muchas partes de la región.

5.2 // Participación comunitaria

Varios Capítulos de Internet Society están contribuyendo actualmente a este proyecto mediante el alojamiento de sondas, lo que está ayudando a aumentar el número de puntos estratégicos de medición en África. Actualmente, los Capítulos de Madagascar, Benín, Túnez y Etiopía participan activamente en el establecimiento de sondas de medición y cuentan con una infraestructura activa. Ya estamos recopilando datos en Kenia y Mauricio sobre la infraestructura que ha sido implementada por el personal de Internet Society (Kenia) y el personal de AfriNIC (Mauricio).



5.3 // Fase piloto

Ya hemos comenzado a aumentar el número de puntos de observación de medición de Internet (es decir, los módulos MIRA) en África al proporcionar infraestructura de medición y respaldar la implementación. Ya estamos recopilando, o preparándonos para recopilar, métricas sobre el desempeño, el tiempo de ida y vuelta (RTT) y las mediciones de latencia en Benín, Burkina Faso, República Democrática del Congo, Kenia, Madagascar, Nigeria, Túnez, Ruanda y Sudáfrica.

Se agregarán más países tan pronto como se identifiquen los puntos estratégicos adecuados.

5.4 // Socios

Este proyecto se llevará a cabo en cooperación con diferentes instituciones académicas. A continuación se muestra una lista de los principales investigadores e instituciones para los diferentes paquetes de trabajo.

1. Amreesh Phokeer, AfriNIC y Kevin G. Chege, Internet Society será responsable de la coordinación general de las actividades mencionadas en los diferentes paquetes de trabajo.
2. Assane Gueye, CMU-Rwanda será el responsable de trabajar con el WP2 para modelar el marco de resiliencia de la infraestructura.
3. Ahmed Elmokashfi, Simula Research Lab trabajará en el WP3 para medir y mapear la topología física y lógica.
4. Josiah Chavula, de la Universidad de Ciudad del Cabo será responsable de los WP3 y WP4, midiendo la resiliencia de la red en términos de puntos de conflicto físicos y lógicos, así como la calidad del servicio a nivel de red y aplicación.

Nota: AfriNIC e Internet Society gestionarán el proyecto MIRA y, por lo tanto, supervisarán conjuntamente todos los paquetes de trabajo definidos anteriormente, asegurándose de que los diferentes colaboradores cumplan con los requisitos definidos en términos de entregables y plazos.

6 Consideraciones éticas

El equipo del proyecto tomará las precauciones necesarias para garantizar que no se presenten al dominio público, datos personales identificables. Todos los conjuntos de datos serán anonimizados antes de ser procesados para prevenir la fuga de información confidencial. Solo se recopilarán los datos necesarios. La metainformación sobre la fuente (como IP y geolocalización) no se almacenará ni procesará. Tenemos la intención de acumular datos en dos niveles principales: nivel ASN y nivel de país.

Cualquier conjunto de datos que contenga datos personales limitados se utilizará solo para el propósito de este proyecto y no se transferirá a ningún tercero y se descartará al final de este proyecto.

Además, los módulos MIRA almacenan datos en formato JSON que solo contiene los datos de medición y ningún dato de identificación personal. Estos son los datos que se procesarán y mostrarán en el panel MIRA dentro de Internet Society Pulse para su visualización.

7 Resumen

Evaluar la resiliencia de Internet es una actividad importante para determinar cómo se pueden mejorar el acceso y las experiencias de Internet. La información de contacto y la información relacionada con el proyecto en general estarán disponibles en el sitio web de Internet Society²⁶ y AfriNIC²⁷ y en Internet Society Pulse²⁸. Para obtener detalles sobre el proyecto MIRA y la infraestructura de medición, visite <https://github.com/mira-project/mira/wiki>.

²⁵ <https://internetsociety.org>

²⁶ <https://afrinic.net/research/studies/mira>

²⁷ <https://pulse.internetsociety.org>



Bibliografía

- [1] J. Rydzak, M. Karanja, and N. Opiyo, "Internet Shutdowns in Africa: Dissent Does Not Die in Darkness: Network Shutdowns and Collective Action in African Countries," *Int. J. Commun.*, vol. 14, pág. 24, 2020.
- [2] T. Freyburg and L. Garbe, "Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-Saharan Africa," *Int. J. Commun.*, vol. 12, págs. 3896–3916, 2018.
- [3] R. Kathuria, M. Kedia, G. Varma, K. Bagchi, and R. Sekhani, "The anatomy of an Internet blackout: measuring the economic impact of Internet shutdowns in India," 2018.
- [4] R. Fanou, F. Valera, and A. Dhamdhare, "Investigating the Causes of Congestion on the African IXP substrate," in *Proceedings of the 2017 Internet Measurement Conference*, 2017, págs. 57–63.
- [5] A. Formoso, J. Chavula, A. Phokeer, A. Sathiaselvan, and G. Tyson, "Deep diving into Africa's inter-country latencies," en *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, 2018, págs. 2231–2239.
- [6] A. Gupta, M. Calder, N. Feamster, M. Chetty, E. Calandro, and E. Katz-Bassett, "Peering at the Internet's frontier: A first look at ISP interconnectivity in Africa," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8362 LNCS, págs. 204–213, 2014.
- [7] M. Isah, A. Phokeer, J. Chavula, A. Elmokashfi, and A. S. Asrese, "State of Internet measurement in Africa-A survey," in *International Conference on e-Infrastructure and e-Services for Developing Countries*, 2019, págs. 121–139.
- [8] R. Cohen, K. Erez, D. Ben-Avraham, and S. Havlin, "Resilience of the Internet to random breakdowns," *Phys. Rev. Lett.*, vol. 85, no. 21, pág. 4626, 2000.
- [9] M. Omer, R. Nilchiani, and A. Mostashari, "Measuring the resilience of the global Internet infrastructure system," in *2009 3rd Annual IEEE Systems Conference*, 2009, págs. 156–162.
- [10] J. P. Rohrer, A. Jabbar, and J. P. G. Sterbenz, "Path diversification for future Internet end-to-end resilience and survivability," *Telecommun. Syst.*, vol. 56, no. 1, págs. 49–67, 2014.
- [11] J. P. G. Sterbenz, E. K. Çetinkaya, M. A. Hameed, A. Jabbar, S. Qian, and J. P. Rohrer, "Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation," *Telecommun. Syst.*, vol. 52, no. 2, págs. 705–736, 2013.
- [12] J. P. G. Sterbenz et al., "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Comput. Networks*, vol. 54, no. 8, págs. 1245–1265, 2010.
- [13] J. Wu, Y. Zhang, Z. M. Mao, and K. G. Shin, "Internet routing resilience to failures: analysis and implications," in *Proceedings of the 2007 ACM CoNEXT conference*, 2007, págs. 1–12.
- [14] J. P. G. Sterbenz et al., "Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines," *Comput. Networks Spec. Issue Resilient Surviv. Networks*, vol. 54, no. 8, págs. 1245–1265, 2010.
- [15] J. P. Rohrer and J. P. G. Sterbenz, "Predicting topology survivability using path diversity," in *2011 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, 2011, págs. 1–7.
- [16] R. Teixeira, K. Marzullo, S. Savage, and G. M. Voelker, "Characterizing and measuring path diversity of Internet topologies," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 31, no. 1, págs. 304–305, 2003.
- [17] D. Baltrunas, A. Elmokashfi, and A. Kvalbein, "Measuring the reliability of mobile broadband networks," in *Proceedings of the 2014 conference on Internet measurement conference*, 2014, págs. 45–58.
- [18] A. Csoma, A. Gulyás, and L. Toka, "On measuring the geographic diversity of Internet routes," *IEEE Commun. Mag.*, vol. 55, no. 5, págs. 192–197, 2017.
- [19] K. G. Leyba, B. Edwards, C. Freeman, J. R. Crandall, and S. Forrest, "Borders and gateways: measuring and analyzing national as chokepoints," in *Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies*, 2019, págs. 184–194.
- [20] R. Fontugne, A. Shah, and E. Aben, "As hegemony: A robust metric for as centrality," in *Proceedings of the SIGCOMM Posters and Demos*, 2017, págs. 48–50.

Apéndice 1

Categoría	Elemento de datos	Tipo de datos	Propósito / Preguntas de investigación	Fuente
Resiliencia de ISP	Resiliencia de enlaces	Secundario	<ul style="list-style-type: none"> ¿Qué tan resiliente es un ISP en términos de conectividad ascendente? 	BGP, Registros de enrutamiento, CAIDA
	QoS/QoE	Primario	<ul style="list-style-type: none"> ¿Cuál es la calidad del enlace (desempeño, tiempo de actividad, confiabilidad)? ¿Los usuarios finales están experimentando el mismo nivel de QoE? 	RIPE Atlas M-Lab
	DNS Resiliencia	Primario	<ul style="list-style-type: none"> ¿Los ISP están proporcionando un servicio de resolución de DNS resiliente? 	Información pública de DNS
Resiliencia de la infraestructura	Sistema de cable	Secundario	<ul style="list-style-type: none"> ¿Los puntos de embotellamiento en la conectividad están a nivel físico? ¿Existe alguna concentración (empresarial o geográfica) en los puertos de entrada? ¿Existe alguna concentración en el proveedor de servicios de cable? 	Telegeografía Mapa de transmisión de ITU crítica Mapa de banda ancha de África
	Ecosistema energético	Secundario	<ul style="list-style-type: none"> ¿Qué tan resiliente es el ecosistema energético de un país? 	
	ccTLD	Primario	<ul style="list-style-type: none"> ¿Número de servidores de nombres? ¿Ubicación de los servidores de nombres? DNSSEC 	Conjunto de herramientas ISC
Resiliencia mercado	Posibilidad de punto de embotellamiento	Secundario Primario	<ul style="list-style-type: none"> ¿Vemos concentración hacia un pequeño grupo hacia arriba? 	Vistas de ruta Traceroute
	Localización de tráfico	Primario Secundario	<ul style="list-style-type: none"> ¿Qué porcentaje de AS están intercambiando tráfico en el IX? - ¿Porcentaje de AS que intercambia tráfico? Número de IX en un país Cantidad de contenido popular local alojado en el país 	PeeringDB Datos IXP PCH Traceroute usando RIPE Atlas
	Asequibilidad	Secundario	<ul style="list-style-type: none"> ¿Qué tan asequible es acceder a Internet? 	A4AI

Apéndice 2—Plan 2021

WP/Tarea	Partes interesadas	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
WP 1. Infraestructura de la medición													
1.1 Módulos de medición	AfriNIC/ISOC	//	//	//									
1.2 Organización de módulos	AfriNIC/ISOC	//	//	//									
1.3 Canalización y almacenamiento de datos	AfriNIC/ISOC		//	//									
WP 2. Marco de resiliencia de Internet													
2.1 Marco teórico	CMU/AfriNIC/ISOC		//	//									
2.2 Evaluación comparativa/datos reales	CMU/AfriNIC/ISOC			//	//								
2.3 Canalización de análisis	CMU/AfriNIC/ISOC			//	//	//							
WP 3. Análisis de resiliencia													
3.1 Análisis de topología física	UCT, Simula/AfriNIC/ISOC	//	//										
3.2 Análisis de topología lógica	UCT, Simula/AfriNIC/ISOC		//	//									
3.3 Mapeo de la topología lógica y física	UCT, Simula/AfriNIC/ISOC			//	//								
3.4 Posibilidad de puntos de embotellamiento y hegemonía AS	AfriNIC/ISOC				//	//							
WP 4. Desempeño de red													
4.1 Desempeño de acceso	UCT, AfriNIC/ISOC					//	//	//					
4.2 Infraestructura de peering	UCT, AfriNIC/ISOC						//	//	//				
4.3 Comprender el uso de la web	UCT, AfriNIC/ISOC							//	//	//			
4.4 Interferencia de la red y la web	UCT, AfriNIC/ISOC								//	//	//		
WP 5. Resiliencia de la banda ancha móvil													
5.1 Desarrollar herramientas de medición móviles	A determinar												
5.2 Capacidad de uso de la banda ancha móvil	A determinar												
5.3 Servicios cruciales (QoE)	A determinar												
WP 6. Resiliencia de la infraestructura DNS													
6.1 Solidez de ccTLD	AfTLD/ISOC												
6.2 Desempeño DNS	AfTLD/ISOC												
WP 7. Panel de MIRA													
7.1 API para uso externo	AfriNIC/ISOC			//	//	//	//						
7.2 Panel de visualización	AfriNIC/ISOC					//	//	//					