Introdução à Telemetria de rede baseada em gRPC/gNMIc

Palestrantes:
Ernesto Sánchez (UCASAL) - esanchez@ucasal.edu.ar
Henri Alves de Godoy (UNICAMP) - henri@unicamp.br

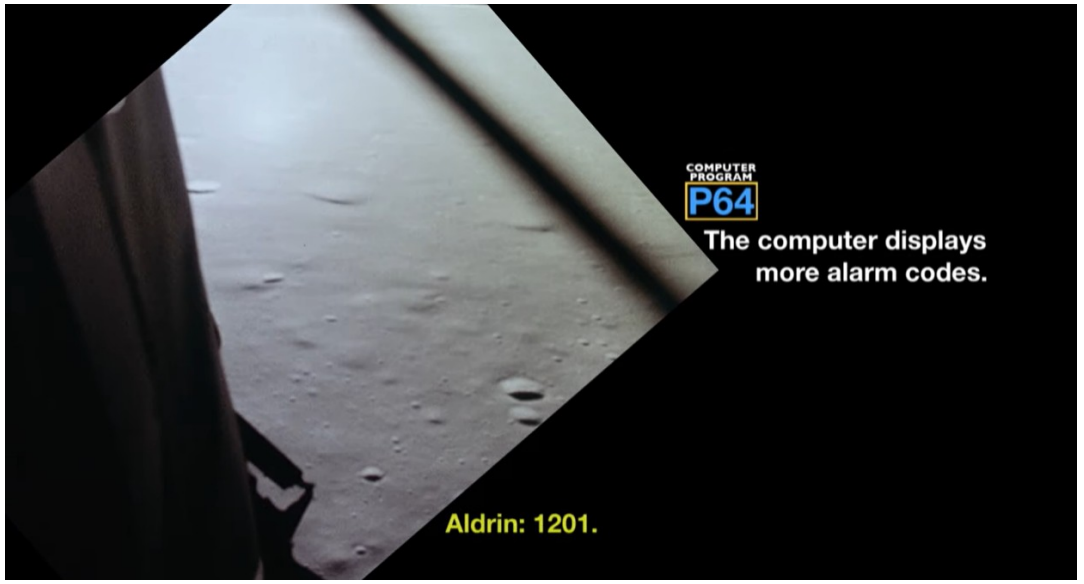
Agenda – Parte 1

1) O que é Telemetria
2) Evolucão do SNMP para a Streaming Telemetry
3) Framework para a Telemetria Moderna
4) Modelo de dados YANG
5) gNMI: gRPC Network Management Interface

O que é Telemetria ?

- Telemetria vem da ideia de 'medir a distância'.
- Essencial nas Missões Apolo durante a exploração espacial.
- Telemetria era a única “visão” que a Terra tinha sobre o módulo lunar.
- Alarmes e decisões críticas precisavam ser tomadas em 30 segundos.
- Em redes modernas, significa o processo contínuo de coleta e análise de dados operacionais dos dispositivos e fluxos da rede.

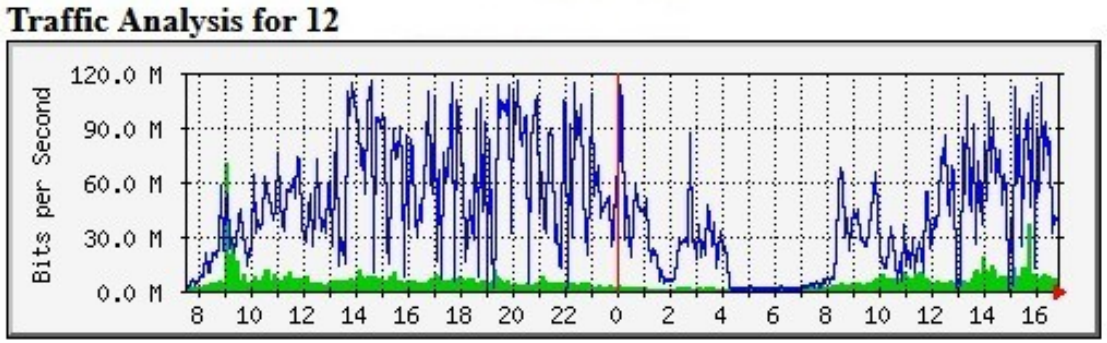
https://www.nasa.gov/history/alsj/a11/a11.landing.html



Monitoramento Básico

Tradicionalmente, a coleta de dados ocorre via SNMP (Simple Network Management Protocol) no modo polling, em que o gerenciador pergunta e o dispositivo responde.

Hoje, o desafio é que as redes cresceram. Ambientes com redes IPv6, IoT, 5G e Datacenters produzem milhões de eventos por segundo.



MRTG
MULTI ROUTER TRAFFIC GRAPHER

https://github.com/oetiker/mrtg/

```
*/5 * * * * env LANG=C /usr/bin/mrtg /etc/mrtg/mrtg.cfg >/dev/null 2>&1
```

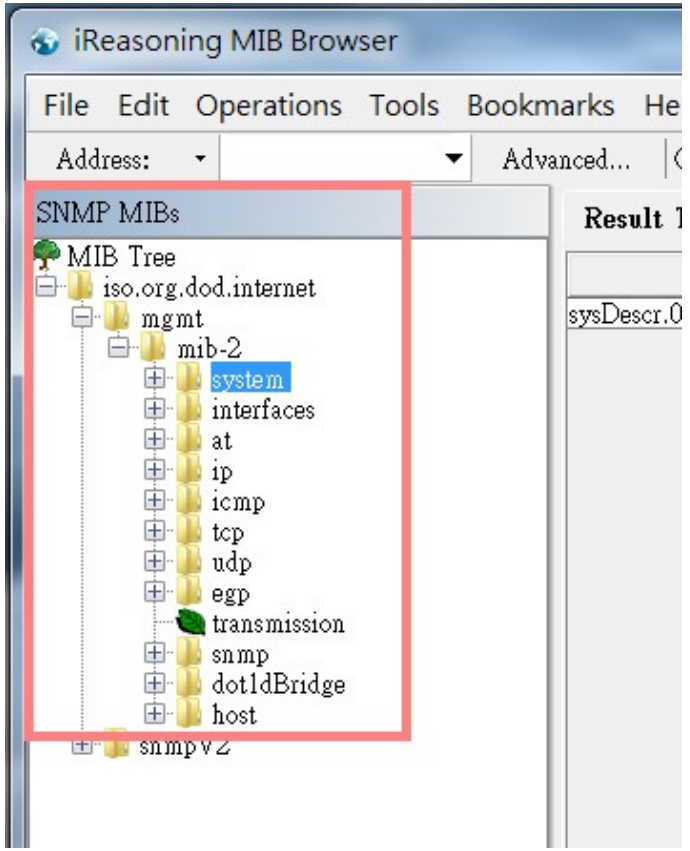
SNMPv1, SNMPv2, SNMPv3

RFC 1157 [1990] - Simple Network Management Protocol (SNMPv1).

Baixa escalabilidade: redes modernas têm milhares de interfaces. O polling gera congestionamento e atrasos.

Formato não estruturado: valores numéricos em OIDs são difíceis de interpretar e integrar.

Incompatibilidade: MIBs proprietárias dificultam a integração entre fabricantes.

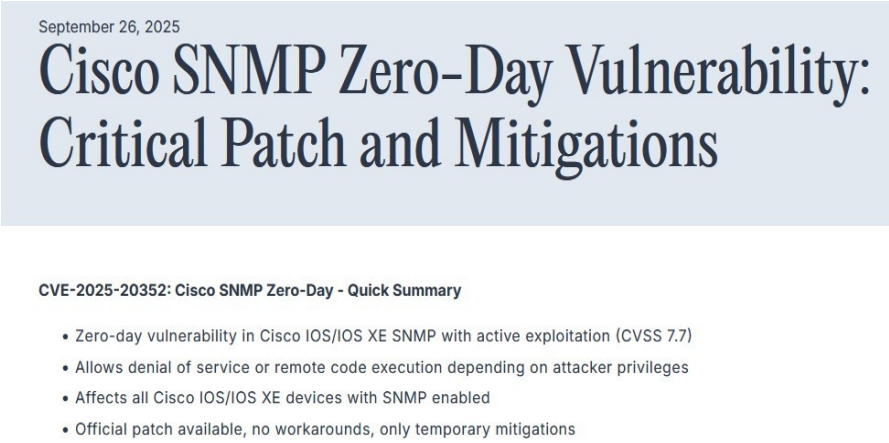


https://www.ireasoning.com/mibbrowser.shtml

Vulnerabilidades do SNMP

- Incidentes recentes exploram vulnerabilidades em implementações SNMP. (CVE-2025-20352).
- Considerar que o SNMP tende a ficar restrito a ambientes legados, não a novos projetos.

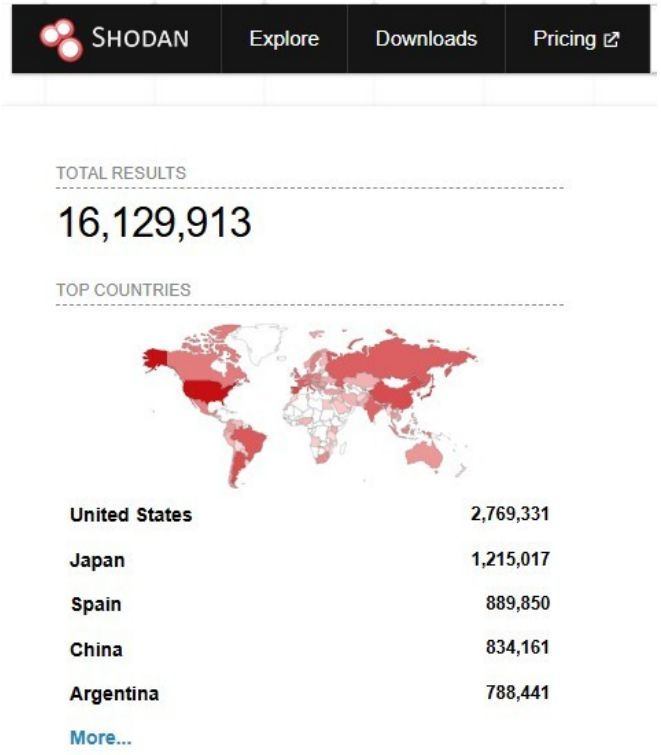
Dispositivos expostos ainda não corrigidos. Nov. 2025



Porta amplamente exposta na Internet

- Porta 161/UDP.
- Muito explorado em ataques de amplificação DDoS.
- Communities padrão (public,private) ainda são comuns em redes de produção.

Dispositivos expostos IPv6 – Nov./2025



Dispositivos expostos IPv4 – Nov./2025

Agentes Autônomos

Quando falamos em bilhões de agentes autônomos (edge, IoT, cloud, sistemas industriais), estamos falando de uma arquitetura distribuída.

Agentic AI = IA que toma decisões, executa ações. Em escala global é, na prática, um sistema distribuído com identidade forte e comunicação constante.

Esses agentes precisam de Identidade de Rede:

- Endereçáveis
- Descobertos
- Autenticados
- Conectividade fim-a-fim

Agentes Autônomos

Imaginem agora um agente por container, por sensor ou workload

- Comunicação frequente entre pares (P2P)
- Coordenação em tempo real
- Troca contínua de estado e telemetria

Se a previsão da próxima década for realmente de bilhões de agentes cooperando, a infraestrutura precisa ser coerente com esse modelo.

Entra em cena o IPv6, que foi projetado para escalar, enquanto o IPv4 ao longo dos anos sofreu adaptações para sobreviver.

Observabilidade em Redes

Observabilidade em redes é a capacidade de entender o comportamento da rede em profundidade, a partir dos eventos que eles próprios produzem, permitindo responder perguntas que não foram previstas no momento do projeto.

Transformação de dados da rede em explicações.

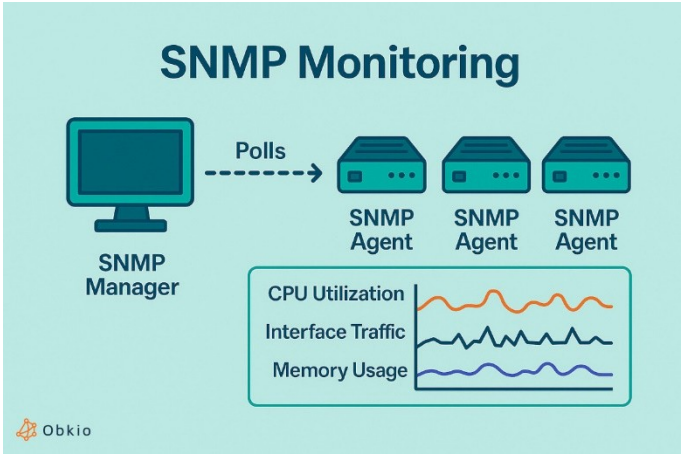
Fatores básicos da observabilidade:

1) Contexto, saber onde ocorre o problema.
2) Correlação de Dados, união de métricas, logs.
3) Exploração, investigar problemas não conhecidos.

https://telesintese.com.br/ipv6-e-observabilidade-por-que-2026-sera-o-ano-em-que-as-redes-precisarao-entender-a-si-mesmas/

Transição do SNMP para Streaming Telemetry

Antigamente: SNMP (Polling)	Atualmente: Streaming Telemetry
Modelo **polling** → o coletor consulta periodicamente os dispositivos. Atrasos na coleta de métricas (minutos). Escalabilidade limitada em grandes redes. Detecção reativa (quando o problema já ocorreu).	Modelo **push/streaming** → os dispositivos enviam métricas em tempo real. Visualização instantânea do estado da rede. Escalável e granular (milhões de métricas por segundo). Permite a detecção **proativa** e a **resposta automatizada** a anomalias ou ataques.



RFC 9232 [2022] Framework for Network Telemetry

- Documento da IETF que define o framework de telemetria de rede para coleta, transporte e análise de dados.
- Organiza a visibilidade em planos: dados, controle e gestão.
- Suporta streaming (push), consultas sob demanda e eventos.
- Usa modelos YANG padronizados para representar métricas e protocolos (gNMI, RESTCONF).

https://datatracker.ietf.org/doc/rfc9232

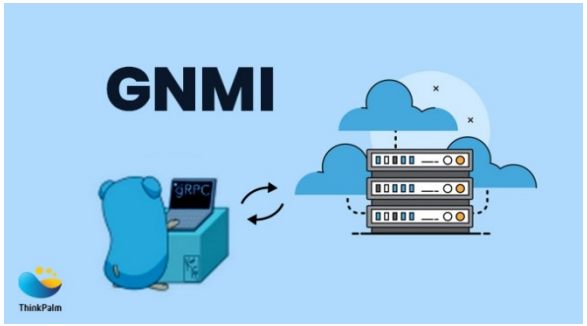
Evolução da Gestão de Redes

- gNMI (gRPC Network Management Interface) é um protocolo moderno de aplicação da OpenConfig para configuração, operação e telemetria em tempo real.
- Streaming telemetry nativo (push).
- Seguro: transportado sobre gRPC + TLS.
- Baseado nos modelos YANG (padronização real entre fabricantes). Exporta dados em formato JSON (fácil integração).
- Suporte a Set, Get, Subscribe e Capabilities.
- Alta interoperabilidade (Cisco, Nokia SRL, Juniper, Arista).

https://gnmic.openconfig.net/

Network Telemetry Framework: componentes

- Modelos de dados padronizados: permitem estruturar a informação de rede de maneira uniforme. Exemplo: os modelos YANG.
- Protocolos de coleta: permitem a assinatura de métricas como fluxos contínuos de dados, em vez de sondagens periódicas. Exemplo: gNMI (gRPC Network Management Interface).
- Sistemas de armazenamento e consulta: realizam a coleta e o armazenamento de séries temporais de métricas.
- Ferramentas de visualização e análise: usadas para interpretar os dados por meio de dashboards e gerar alertas.



Modelo de Dados YANG

Linguagem de modelagem de dados orientada para redes, desenvolvida pela IETF em 2010, projetada especificamente para definir modelos de dados usados no gerenciamento de dispositivos de rede por meio de protocolos como NETCONF, RESTCONF e gNMI.

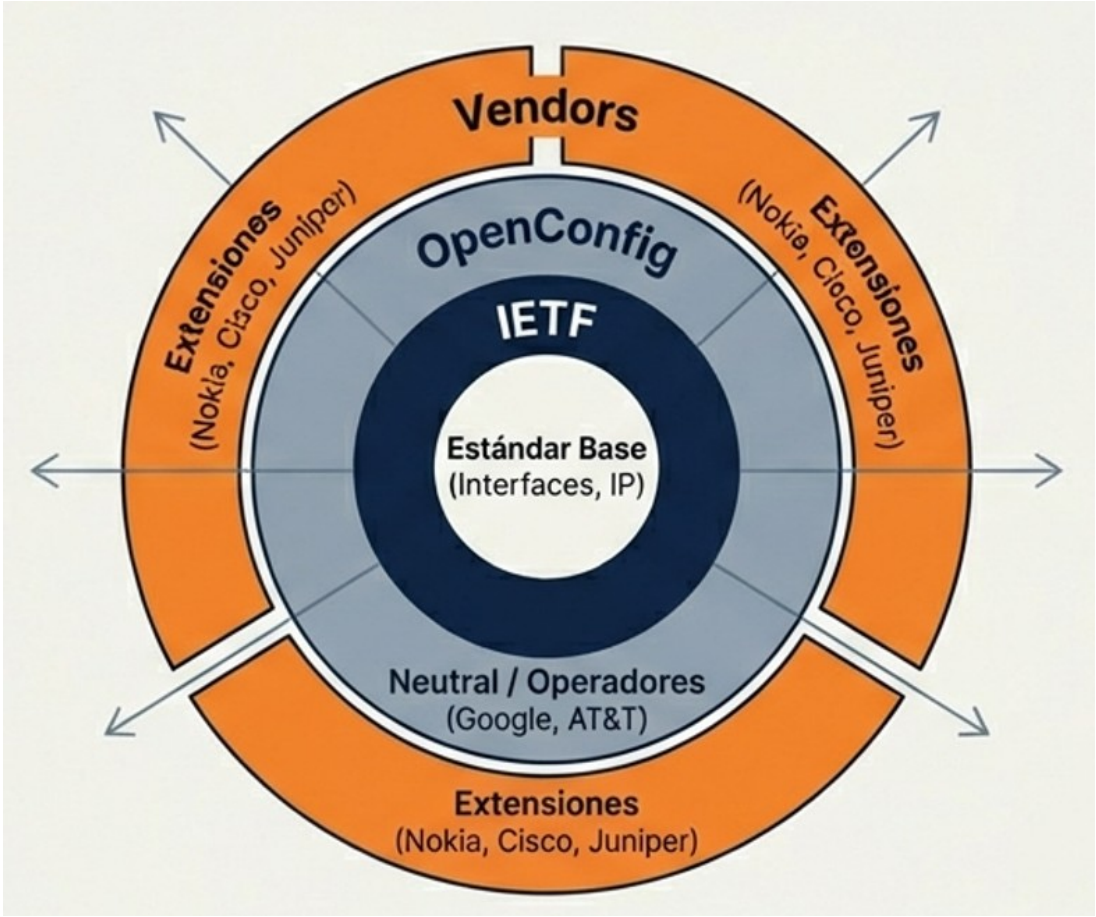
Permite descrever de forma estruturada, modular e extensível:

- A configuração dos dispositivos.
- Seu estado operacional atual.
- As políticas e serviços associados.

Referências:

- https://datatracker.ietf.org/doc/html/rfc6020
- https://datatracker.ietf.org/doc/html/rfc7950

YANG: Modelos de Dados



YANG define o que é o dado.

O IETF fornece a sintaxe.

OpenConfig padroniza e os fabricantes adicionam especificidades.

Referências:

- https://github.com/YangModels/yang
- https://www.openconfig.net/projects/models/

Fonte: imagen gerada com NotebookLM

Comparativo: SNMP vs YANG

	SNMP IF-MIB	(YANG path)
Counters	Nativo	Nativo
Rates (bps)	Calculado	Nativo
Modelo Hierárquico	Não	Sim
Timestamp	Não	Sim
Escalabilidade	Baixa	Alta
Contexto semántico	Não	Sim

Exemplo SNMP:

snmpwalk -v2c -c public 172.100.100.5 ifHCInBroadcastPkts.3 IF-MIB::ifHCInBroadcastPkts.3 = Counter64: 135

Exemplo gNMIc:

gnmic -a srlswitch:57400 --skip-verify -u admin -p "NokiaSrl1!" -e json_ietf get –path /interface[name=ethernet-1/3]
/statistics/in-broadcast-packets

Resumo: quadro comparativo

Características	Tradicionais	Modernas
Exemplos	CLI, SNMP, NETCONF, RESTCONF	gNMI, JSON-RPC
Formato de dados	Texto plano, XML	JSON, Protobuf, YANG
Transporte	SSH (CLI/NETCONF), UDP/TCP (SNMP), HTTP/HTTPS (RESTCONF)	gRPC (gNMI), HTTP/HTTPS (JSON-RPC)
Escalabilidade	Baixa a moderada	Alta
Interoperabilidade	Limitada, MIBs proprietárias	Alta, baseada em YANG/OpenConfig
Segurança	Variável (SNMPv1/v2 inseguro, SNMPv3/SSH seguro)	TLS obrigatório (gNMI), APIs seguras
Uso recomendado	Redes legadas, troubleshooting manual	Automação, observabilidade, IPv6 em larga escala

Fonte: Próprio autores

Estrutura do dados: componentes principais

De acordo com a definição fornecida na RFC 6020, os quatro tipos de nós usados para definir um modelo de dados são: Leaf Nodes, Leaf-List Nodes, Container Nodes e List Nodes.

- **Container Node:** São utilizados para definir a estrutura interna de um modelo de dados; podem conter outros nós.
- **Leaf Node:** Contêm um único valor. Representam a folha de uma árvore de dados e são usadas para definir propriedades individuais dentro de um modelo de dados.
- **Leaf-List Node:** São utilizadas para definir listas de elementos que compartilham o mesmo tipo de dados.
- **List Node:** São utilizados para definir coleções de elementos que podem ter múltiplas instâncias Cada instância de um List Node pode conter vários Leaf Nodes ou Leaf-List Nodes.

Exemplo de estrutura de dados:


```
{
   "source": "srlswitch:57400",
   "timestamp": 1772254968847365995,
   "time": "2026-02-28T05:02:48.847365995Z",
   "updates": [
    {
     "Path":
"srl_nokia-interfaces:interface[name=ethernet-1/3]/statistics/in-broadcast-
packets",
      "values": {
       "srl_nokia-interfaces:interface/statistics/in-broadcast-packets": "100"
      }
    }
   ]
}
```

gNMIc: o coletor

O gNMIc prove o suporte as operações RPC:

- **Capabilities:** permite que o cliente e o servidor possam compartilhar as informações sobre suas capacidades (modelos YANG suportados, versões, etc.)
- **Get:** obter os dados das configurações ou operações de um dispositivo.
- **Set:** modificar as configurações em um ou mais dispositivos.
- **Subscribe:** assinatura para receber os dados específicos em tempo real. O servidor envia atualizações automáticas quando esses dados são alterados. Essencial para telemetria contínua e monitoramento proativo.

Essas operações permitem a substituição dos mecanismos tradicionais de sondagem por um modelo de envio contínuo, no qual o dispositivo envia dados continuamente para o sistema de monitoramento.

Fonte: https://gnmic.openconfig.net/

gNMIc: características

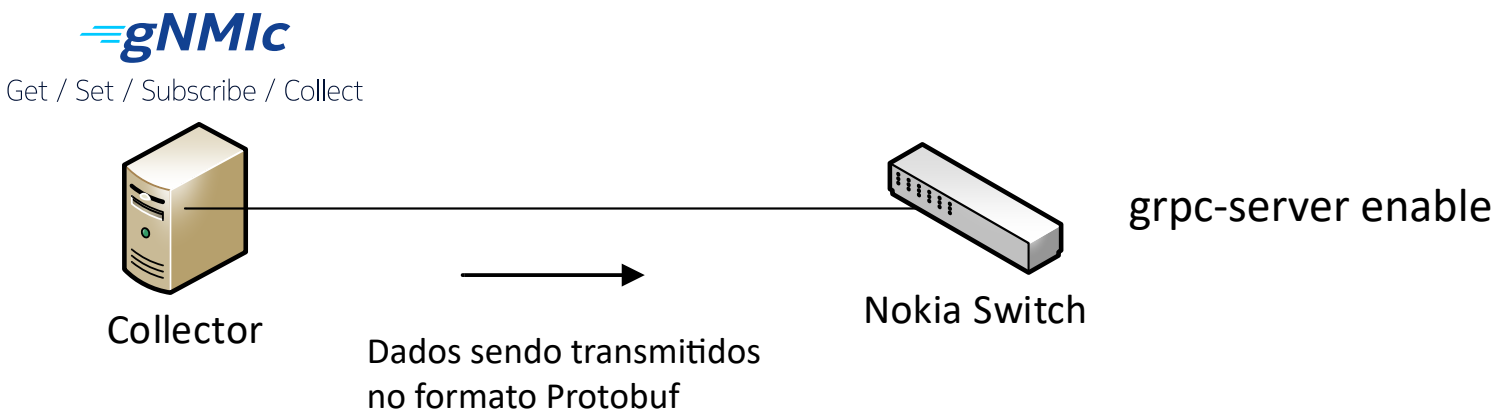
- **Collector Deployment:** permite colectar métricas com suporte para múltiplas saídas como: Kafka, Prometheus, InfluxDB.
- **Data Manipulation:** transformação de dados em tempo real.
- **YANG-based Path Suggestions:** modo interativo. Preenchimento automático de rotas com base em modelos YANG.
- **Multiple configuration sources:** suporta flags CLI, variáveis de ambiente e arquivos .yml.
- **Multi-target operations:** permite executar comandos em vários dispositivos simultaneamente.
- **Multiple subscriptions:** permite definir múltiplas assinaturas por meio de um arquivo. Cada assinatura pode ser associada a diferentes destinos**.**
- **TLS enforcement:** suporte a TLS para ambientes seguros.

gNMIc: configuração

- Uma característica importante do gNMIc é que podemos obter sua configuração a partir de múltiplas fontes, o qual facilita seu uso tanto em ambientes automatizados como também interativos.
- https://gnmic.openconfig.net/user_guide/configuration_intro/

Fonte	Descrição	Prioridade
Flags global e local	Parametros definidos diretamente ao executar o comando. Exemplo: --address, --username, --password	Alta
Variáveis de Ambiente	Valores definidos no sistema operacional, accessiveis por gNMIc. Exemplo: GNMIC_ADDRESS, GNMIC_USERNAME	Média
Arquivo de configuração local (config.yml)	Arquivo YAML onde estão descritas as opções predeterminadas do cliente gNMI	Baixa

gNMIc: configuração

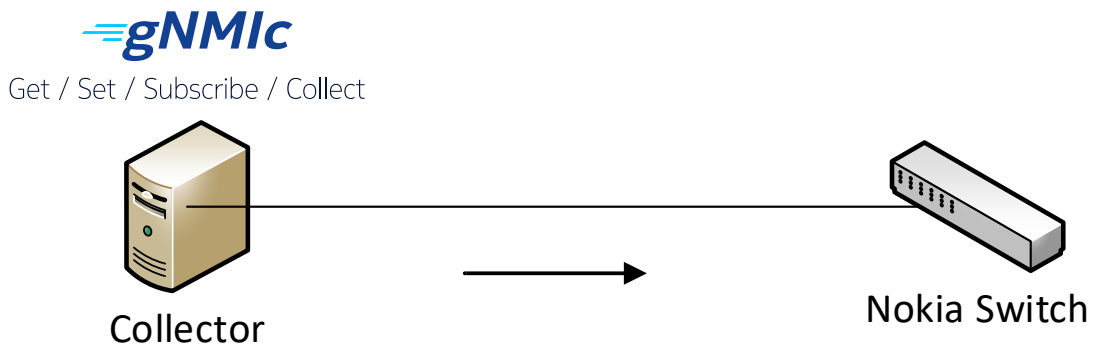


- Um exemplo de execução gNMI por linha de comando:

```
# gnmic -a srlswitch:57400 --skip-verify -u admin -p "NokiaSrl1!" -e json_ietf get --path /system/name/host-name
```

-a srlswitch:57400: especifica o endereço do servidor gNMI (srlswitch) e sua porta (57400).
--skip-verify: omite a verificacão do certificado TLS.
-u admin -p "NokiaSrl1!": credenciais de autenticação (usuário e senha).
-e json_ietf: indica que os resultados devem ser serializados em formato JSON.
get --path /system/name/host-name: realiza uma operação get no path /system/name/host-name.

gNMIc: configuração



Mesmo sendo os dados tráfegados no formato Protobuf, o parametro -e json_ietf indica que o cliente gNMIc deve deserilizar os dados recebidos em formato Protobuf e convertê-los para JSON IETF antes de serem mostrados ou processados.


```
{
  "source": "srlswitch:57400",
  "timestamp": 1752536956323201947,
  "time": "2025-07-14T23:49:16.323201947Z",
  "updates": [
   {
    "Path": "srl_nokia-system:system/srl_nokia-system-name:name/host-name",
    "values": {
     "srl_nokia-system:system/srl_nokia-system-name:name/host-name": "srlswitch"
    }
   }
```

gNMIc: arquivo de configuracão

- Com un arquivo de configuracão, um usuário pode especificar todas as opções que normalmente estão disponiveis por linha de comandos. O gNMIc fará a leitura desse arquivo e obterá as opções de configuração nele contido.
- Um arquivo de configuracão YAML em gNMIc permite:
  - Definir todos os parametros usados como flags na linha de comandos.
  - Configurar múltiplos targets (dispositivos de rede)
  - Definir assinaturas de telemetria
  - Estabelecer saídas (outputs) onde se armazenam os dados
  - Usar opcões avançadas que não estão disponíveis facilmente na CLI
- Maior facilidade e praticidade para realização de laboratórios e automatização em produção.

gNMIc: arquivo de configuração

- Componentes principais:

Bloco	Descrição
addresses	Endereços IP ou nomes de host dos dispositivos de rede
username / password	Credenciais para se autenticar com os dispositivos
insecure / skip-verify	Parâmetros de segurança TLS
encoding	Formato de codificação usado nas respostas (json_ietf, json, proto, etc.)
timeout	Establece um limite de tempo de resposta. Se o dispositivo não responde dentro do tempo, a operacão é cancelada e retorna um erro.
get, set, subscribe	Operações específicas de execução
targets	Define múltiplos dispositivos com configuracões individuais
subscriptions	Define paths em formato YANG a ser monitorado em tempo real
outputs	Define como e por onde enviar os datos coletados (arquivos, elasticsearch, prometheus, etc.)

https://gnmic.openconfig.net/global_flags/

gNMIc: subscriptions

- As assinaturas em gNMI permitem aos clientes receberem atualizações automáticas de dados operacionais (estado, estatísticas, eventos) em tempo real desde um ou mais dispositivos de rede.

Componentes principais de uma assinatura:

Campo	Descrição
mode	Tipo de assinatura: once, poll, stream
stream-mode	Tipo de assinatura stream: target-defined, sample, on-change
paths	Paths YANG a serem assinadas (múltiplas)
sample-interval	Intervalo de tempo para assinaturas em modo sample
prefix	Adiciona um prefixo ao dados recompilados (útil para identificar a origem)
updates-only	Somente mostra dados quando existe uma mudança (útil com on-change)

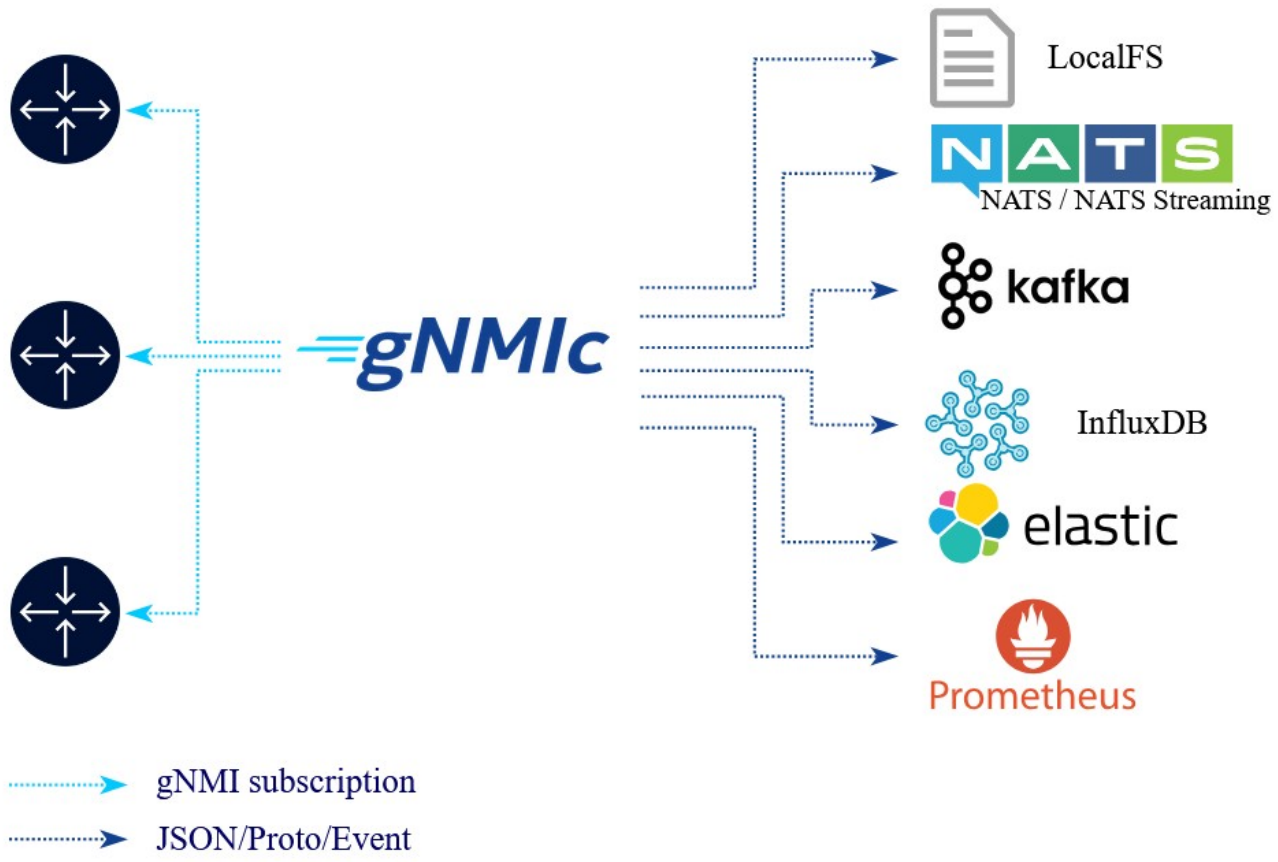
https://gnmic.openconfig.net/user_guide/subscriptions/

gNMIc: outputs

- Um output define como e onde se deve enviar os dados coletados desde os dispositivos da rede através das assinaturas. Estes dados podem ser estatísticas de operações, eventos, notificações ou qualquer outro valor YANG monitorado via gNMI.
- gNMIc permite definir múltiplas saídas simultâneas, no qual permite:
  - Receber os dados do dispositivo de uma só vez.
  - Enviar para diferentes destinos ao mesmo tempo:
    - Arquivo local.
    - Sistema de telemetria como Prometheus ou Kafka.
    - Base de dados.
    - Serviços externos.

https://gnmic.openconfig.net/user_guide/outputs/output_intro/

gNMIc: outputs



https://gnmic.openconfig.net/user_guide/outputs/output_intro/

gNMIc: outputs

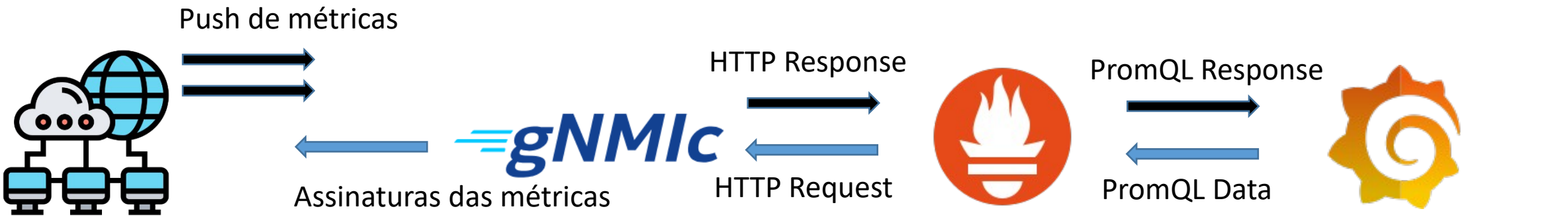
- Formatos suportados:

Format/output	proto	protojson	prototext	json	event
File	✗	✓	✓	✓	✓
NATS / STAN	✓	✓	✗	✓	✓
Kafka	✓	✓	✗	✓	✓
UDP / TCP	✓	✓	✓	✓	✓
InfluxDB	NA	NA	NA	NA	NA
Prometheus	NA	NA	NA	NA	NA

Formato	Descrição
json	Datos estruturados, ideais para processamento posterior
json_ietf	Versão padrão de JSON para modelos YANG IETF
proto	Dados em formato binário de Protocol Buffers
event	Formato útil para alimentar sistemas desestruturados como Kafka

https://gnmic.openconfig.net/user_guide/outputs/output_intro/

Workflow: gNMIc → Prometheus → Grafana



Processa e exibe no formato Prometheus.

Extrai e armazena métricas em séries temporais.

Gera e exibe gráficos em dashboards.