Telemetria para automação em redes IPv6

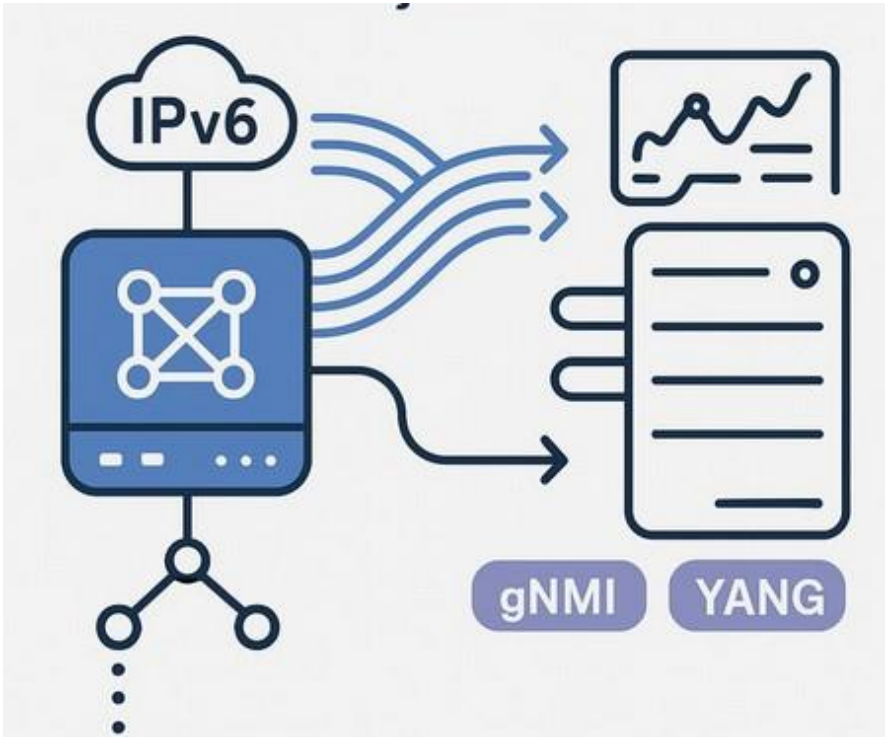
Henri Alves de Godoy - Universidade Estadual de Campinas - UNICAMP

Ernesto Sánchez - Universidad Católica de Salta - UCASAL

GTER 54 GTS 40

Sumário

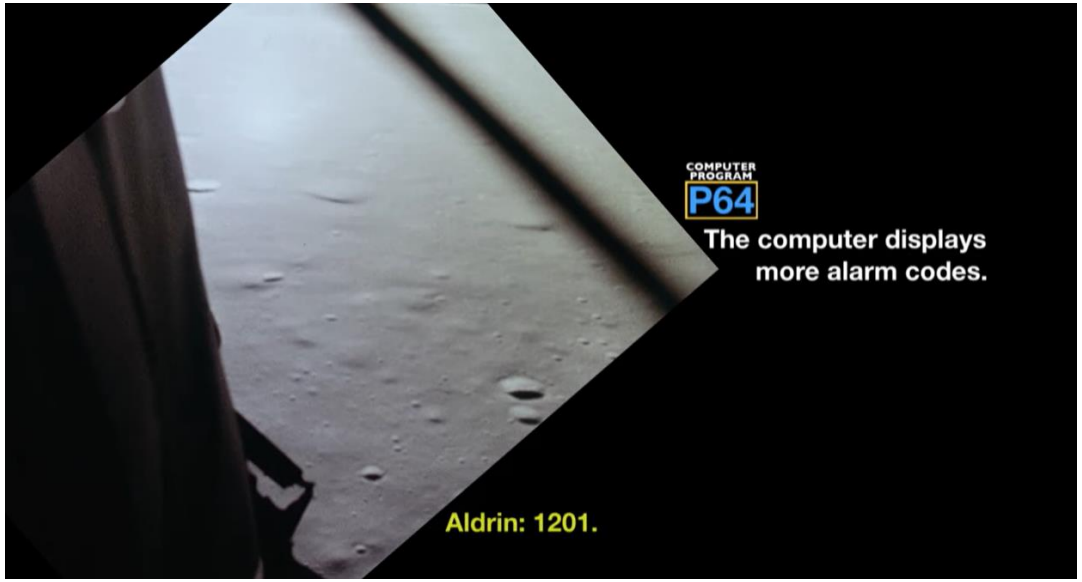
1) O que é Telemetria
2) Limitações do Modelo SNMP
3) Telemetria Moderna (gNMI/YANG)
4) Arquitetura e Casos Práticos em IPv6
5) Benefícios e Considerações Finais



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.

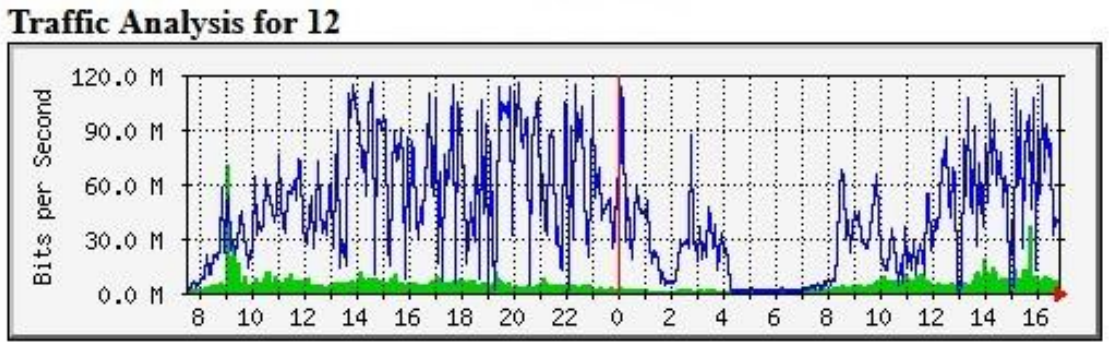
https://www.nasa.gov/history/alsj/a11/a11.landing.html



Monitoramento Básico

Tradicionalmente, a coleta de dados ocorre via SNMP no modelo polling, em que o gerenciador pergunta e o dispositivo responde.

O desafio hoje é que as redes cresceram. Ambientes com 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
```

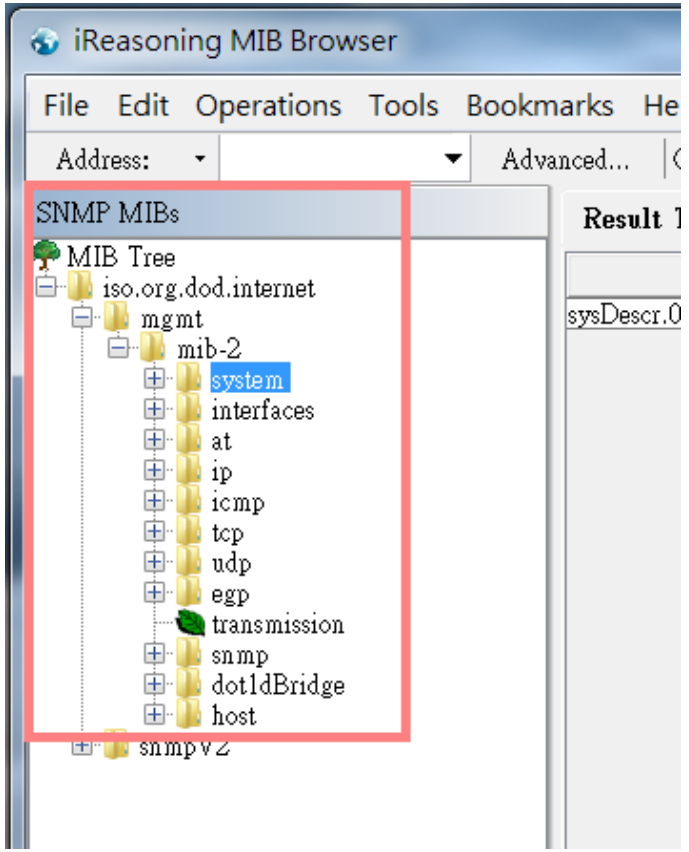
SNMPv1, SNMPv2, SNMPv3

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.

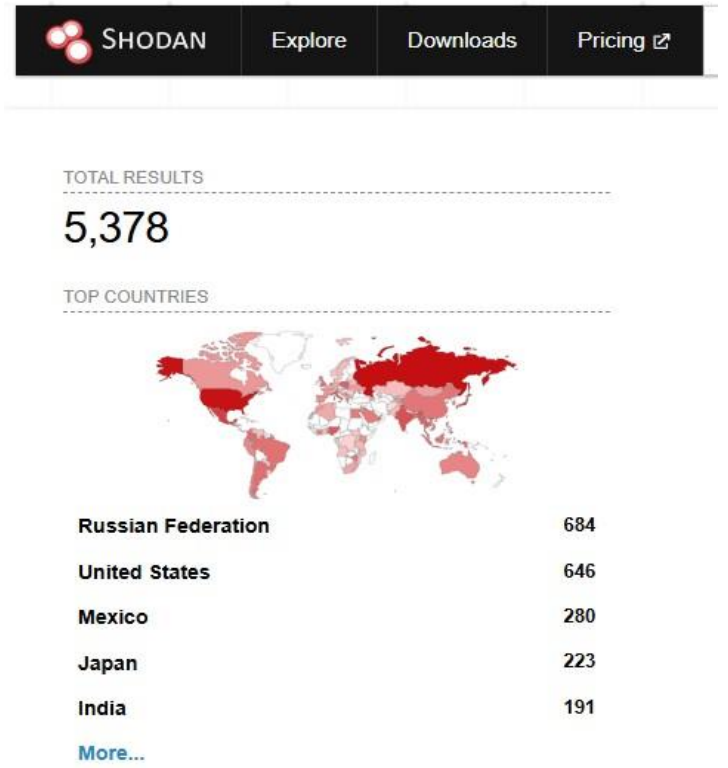
Incompatibilidade: MIBs proprietárias dificultam a integração entre fabricantes.



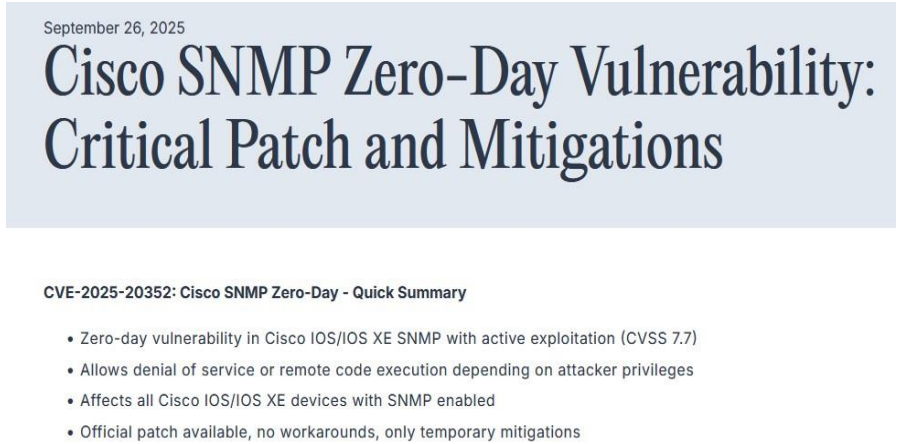
https://www.ireasoning.com/mibbrowser.shtml

Aposentadoria do SNMP

- Incidentes recentes exploram vulnerabilidades em implementações SNMP. (CVE-2025-20352).
- A transição deve ser gradual e servir como estratégia de defesa e modernização da rede.
- Considerar que o SNMP tende a ficar restrito a ambientes legados, não a novos projetos.



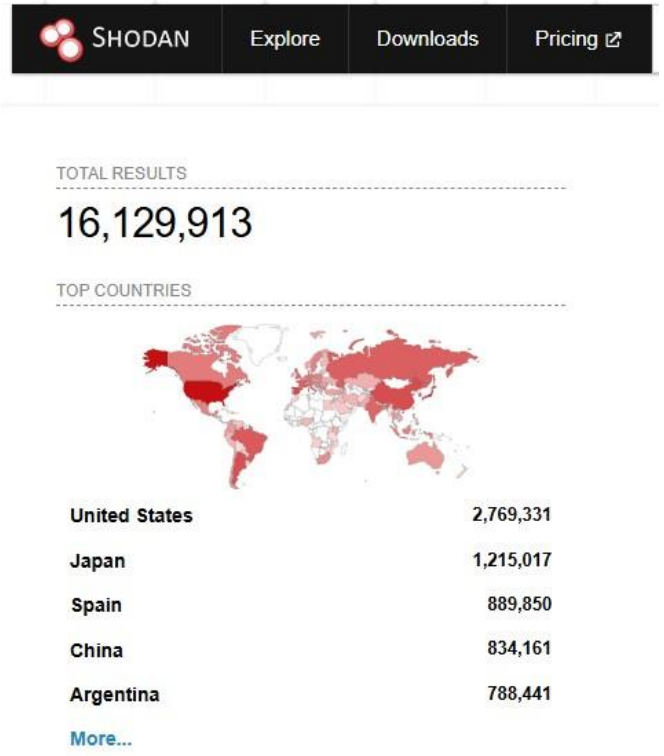
Dispositivos expostos ainda não corrigidos. Nov. 2025



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

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/

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

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: Autoria Própria

Observabilidade em redes IPv6

- Desenvolver um sistema baseado em gNMI, JSON-RPC, Scapy e Python.
- Descobertas automáticas de hosts em IPv6.
- Fortalecer a segurança de acesso nas bordas da rede.
- Detectar dispositivos desconhecidos ou não autorizados.
- Automatizar políticas de segurança com base em métricas de telemetria.

Hackers abuse IPv6 networking feature to hijack software updates

By **Lawrence Abrams** April 30, 2025 08:33 PM 6

A China-aligned APT threat actor named "TheWizards" abuses an IPv6 networking feature to launch adversary-in-the-middle (AitM) attacks that hijack software updates to install Windows malware.

https://www.bleepingcomputer.com/news/security/hackers-abuse-ipv6-networking-feature-to-hijack-software-updates

Estudos de caso e pesquisas com laboratórios práticos

VM	Descrições
Nokia SRL Linux	Container image versão 24.10
gNMIc	Container Alpine Linux. Módulos: gNMI client. Python3. Scapy.
Prometheus*	Container image versão 2.54.1. Recebe e armazena os dados exportados por gNMIc.
Grafana*	Container image versão 12.0.2. Visualização de métricas.
Hosts	Container image Kali Linux. Módulos: THC IPv6 toolkit

Fonte: Autoria Própria

* Baseado em Nokia SR Linux Streaming Telemetry Lab - https://github.com/srl-labs/srl-telemetry-lab/tree/main

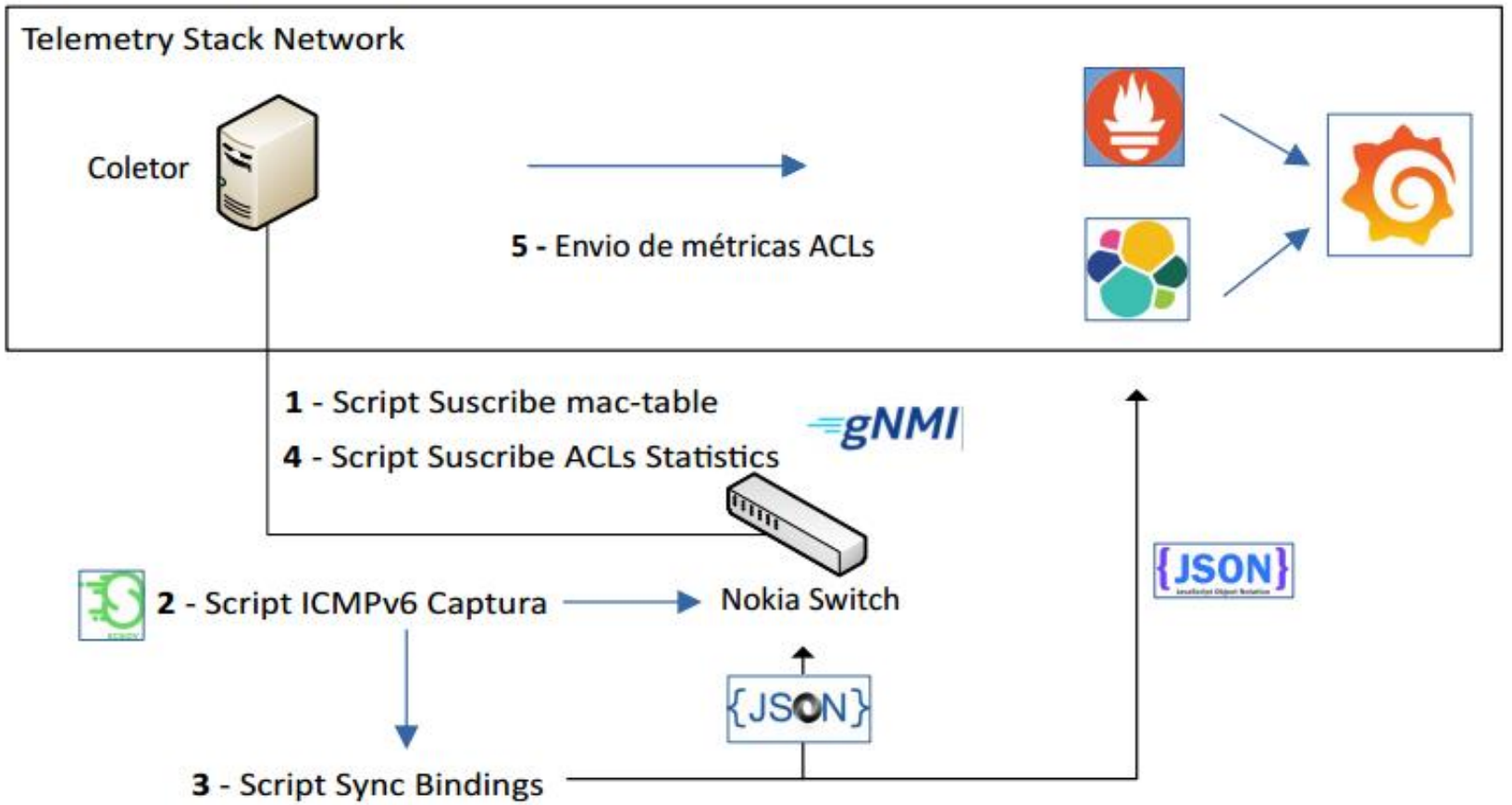
Funcionalidades do gNMIc

Scripts	Descrições
gnmic_subscribe_mactable	subscriptions: srl-mac-table: mode: stream stream-mode: on-change. output file: mac_updates.json
icmpv6_captura*	Captura o tráfego ICMPv6 RS NS durante o processo SLAAC. Correlaciona o tráfego obtido pelo arquivo mac_updates.json Output file: mac_ipv6_bindings_dynamic.json
sync_bindings*	Input file: mac_ipv6_bindings_dynamic.json Cria os ACLs por interface e envia a Nokia Switch via JSON-RPC
gnmic_subscribe_acl	subscriptions: srl-acl-statistics: mode: stream stream-mode: sample. prom-output: Prometheus

Fonte: Autoria Própria

https://github.com/ernestosv73/telemetria-ipv6

Cenário ContainerLab - gNMIc



1 - Correlaciona o tráfego capturado com a tabela MAC obtida via gNMIc
2 - Gera arquivos JSON com bindings MAC ↔ IPv6 Addr ↔ Interface
3 - Aplica ACLs via JSON-RPC a Nokia Switch
4 - Aplica ACLs para visualizar métricas na interfaces (bloqueios, flooding, CPU).
5 - Envio das métricas para Prometheus e em seguida para visualização no Grafana.

NDP Bindings com gNMIc e Scapy

Objetivo: Criar bindings válidos e aplicar as ACLs em tempo real por interface para mitigar ataques baseados em mensagens ICMPv6 ND.

```
{
    "mac": "aa:c1:ab:55:20:5a",
    "interface": "ethernet-1/2.0",
    "ipv6_link_local":
"fe80::a8c1:abff:fe55:205a",
    "ipv6_global":
"2001:db8:20:0:a8c1:abff:fe55:205a",
    "timestamp": "2025-06-10T01:28:39.773935"
}
```

File: mac_ipv6_bindings_dynamic.json

```
set acl acl-filter {iface} type ipv6 entry 10 match ipv6 next-header icmp6 source-ip prefix
{ipv6_link_local}/128
set acl acl-filter {iface} type ipv6 entry 10 action accept
set acl acl-filter {iface} type ipv6 entry 11 match ipv6 next-header icmp6 source-ip prefix {ipv6_global}/128
set acl acl-filter {iface} type ipv6 entry 11 action accept
set acl acl-filter {iface} type ipv6 entry 100 match ipv6 next-header icmp6
set acl acl-filter {iface} type ipv6 entry 100 action log true drop
```

Via JSON-RPC YANG Model

Nokia SRL Switch

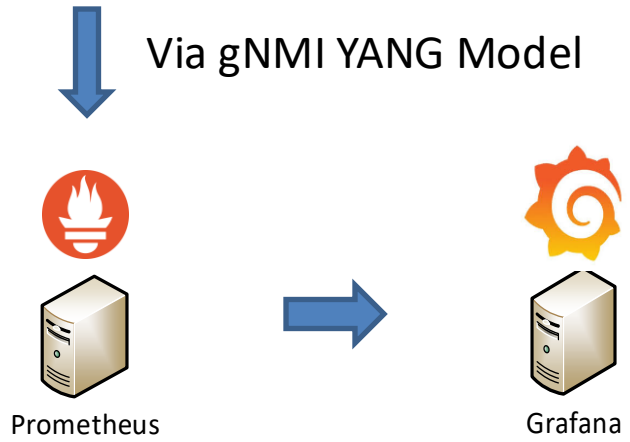
Métricas ACLs match packets

Objetivo: Obter estatísticas de ACLs match packets de Nokia SRL Switch.

```
srl-acl-statistics:
    mode: stream
    stream-mode: sample
    sample-interval: 5s
    paths:

       - /acl/interface[interface-id=ethernet-1/*]/input/acl-filter[name=*][type=ipv6]/entry[sequence-id=100]/statistics/

outputs:
    prom-output:
       type: prometheus
```



Métrica: acl_interface_input_acl_filter_entry_statistics_matched_packets

Outras métricas úteis

Objetivo: Detectar ataques de RA flood desde um endereço de rede válido.

```
srl-if-stats:
    mode: stream
    stream-mode: sample
    sample-interval: 5s
    paths:
      - /interface[name=ethernet-1/*]/statistics
      - /interface[name=ethernet-1/*]/traffic-rate
```

Métrica: interface_statistics_in_multicast_packets

Objetivo: Visualizar o consumo de recurso CPU de um Nokia Switch.

```
srl-system-performance:
    mode: stream
    stream-mode: sample
    sample-interval: 5s
    paths:
      - /platform/control[slot=*]/cpu[index=all]/total
```

Métrica: platform_control_cpu_total_instant

Vídeo Demonstrativo

https://www.youtube.com/watch?v=Rb7LNyiCqqc

Benefícios Estratégicos

Visibilidade em tempo real do estado da rede IPv6.

Detecção imediata de anomalias e ataques baseados em ND spoofing e RA flood.

Automação de políticas de segurança, reduzindo ação manual.

Maior interoperabilidade via modelos abertos (OpenConfig/YANG).

Base sólida para futuras integrações com IA generativa.

Considerações Finais

- Telemetria é uma ferramenta indispensável para as redes IPv6.
- Traz observabilidade, automação e segurança.
- Supera o modelo tradicional com o SNMP em escala e velocidade.
- Passamos de um modelo reativo, limitado pelo SNMP, para um modelo proativo e inteligente.
- Integração de gNMI e JSON-RPC viabiliza a segurança dinâmica em redes IPv6.

- Próximos passos: expandir os estudos de casos, incluir novos dispositivos e métricas.
- Fortalecer a cultura de automação e telemetria em operações de rede.

Referências

https://www.rfc-editor.org/rfc/rfc9232.html/

https://gnmic.openconfig.net/

https://documentation.nokia.com/srlinux/24-10/index.html

https://github.com/srl-labs/srl-telemetry-lab/

https://yang.srlinux.dev/

https://grafana.com/docs/grafana/latest/datasources/prometheus/

https://grafana.com/docs/grafana/latest/datasources/elasticsearch/

https://github.com/ernestosv73/telemetria-ipv6/

Muito Obrigado !!
Perguntas ???

Ernesto Sánchez
linkedin.com/in/ernestosánchez

Henri Alves de Godoy
linkedin.com/in/henri-alves-godoy

UNICAMP

UCASAL
UNIVERSIDAD CATÓLICA DE SALTA