

# INTRAREDE 2024

## TELEMETRIA, GERENCIAMENTO E MONITORAMENTO DE REDES

---

Leonardo Furtado  
Senior Network Development Engineer

<https://ead.leonardofurtado.academy/>

(Plataforma de cursos para Engenheiros de Redes)



# Disclaimer

1. As opiniões expressas aqui são estritamente pessoais e não refletem, de forma alguma, as posições do meu empregador.
2. As ideias discutidas neste espaço não violam quaisquer acordos de confidencialidade, NDAs ou compromissos similares.

# Objetivos

1. A realidade das redes dos ISPs e de muitas organizações.
2. Compreendendo os domínios de gerenciamento
3. A modernização requerida para as abordagens tecnológicas.

*A realidade do ISP regional*

# A realidade do gerenciamento no ISP

- Embora a realidade a seguir seja comum a diversos ambientes de rede em várias empresas, vamos focar aqui no cenário de ISP.
- ISPs regionais frequentemente direcionam sua atenção excessivamente para:
  - ...**Ferramentas de gerenciamento** (Zabbix, Grafana, PRTG, etc.)...
  - ...**múltiplos dashboards**...
  - ...**representações visuais elegantes de dados**.
- No entanto, eles tendem a negligenciar como essas informações podem — e devem — ser utilizadas para impulsionar ações efetivas que gerem benefícios tangíveis e resultados concretos para o negócio.

# A realidade do gerenciamento no ISP

- Ênfase excessiva na coleta de dados de objetos gerenciáveis, como:
  - Contadores de utilização e erros de interfaces.
  - Sessões e adjacências.
  - Prefixos.
  - Temperatura, CPU, memória e outros indicadores de interesse.
- Tarefas simples de automação, incluindo coleta e backup de configurações, bem como geração de configurações para implantação.
- Há uma preocupação reduzida ou pouca ação voltada para resolver desafios técnicos e operacionais, bem como para compreender como estes se convertem em impactos ou benefícios para o negócio.

# A realidade do gerenciamento no ISP

## OIDs específicos para BGP comumente empregados

```

bgpPeerIdentifier
bgpPeerState
bgpPeerAdminStatus
bgpPeerNegotiatedVersion
bgpPeerLocalAddr
bgpPeerLocalPort
bgpPeerRemoteAddr
bgpPeerRemotePort
bgpPeerRemoteAs
bgpPeerInUpdates
bgpPeerOutUpdates
bgpPeerInTotalMessages
bgpPeerOutTotalMessages
bgpPeerLastError
bgpPeerFsmEstablishedTransitions
bgpPeerFsmEstablishedTime
bgpPeerConnectRetryInterval
bgpPeerHoldTime
bgpPeerKeepAlive
bgpPeerHoldTimeConfigured
bgpPeerKeepAliveConfigured
bgpPeerMinASOriginationInterval
bgpPeerMinRouteAdvertisementInterval
bgpPeerInUpdateElapsedTime
  
```

**B.P.F.**  
Brasil Peering Forum  
Leonardo Furtado  
Comitê de Programa



Solicitação "GET"

Resposta

Rede de Gerência Inband ou Out-of-Band (OOB)  
Roteadores monitorados

## Interface Web do Zabbix/Grafana na Estação do Operador/NOC



## Interface Web do NMS na Estação do Operador/NOC



!! Falha detectada na rede !! STOP

SNMP Trap

**B.P.F.**  
Brasil Peering Forum  
Leonardo Furtado  
Comitê de Programa

Servidor com Sistema de Gerenciamento (NMS)

# A realidade do gerenciamento no ISP

## MONITORAMENTO BGP VYOS

STATUS E MÉTRICAS SISTEMA

LATENCIA: **0.0005 ms** PERDA DE PACOTE: **0** DISPONIBILIDADE: **UP**

USO CPU: **9%**

USO DE MEMÓRIA: **10%**

ESPAÇO UTILIZADO NO SISTEMA DE ARQUIVOS

/boot	0.28%	/boot/grub	0.28%	/lib/live/mount/overlay	0%	/lib/live/mount/paranormalboot	0.28%
/lib/live/mount/paranormal	0.28%	/opt/vyatta/config	0.01%	/opt/vyatta/etc/config	0.28%	/tmp	0.00%

STATUS BGP

### BGP Admin Status

192.168.1.48	192.168.1.51	192.168.1.101	192.168.1.102	192.168.1.103	192.168.1.104	192.168.1.200	192.168.204.204	192.168.205.205
UP	UP	UP	UP	UP	UP	UP	UP	UP

### BGP Peer State

192.168.1.48	192.168.1.51	192.168.1.101	192.168.1.102	192.168.1.103	192.168.1.104	192.168.1.200	192.168.204.204	192.168.205.205
ESTABLISHED	ATENÇÃO	ESTABLISHED	ESTABLISHED	ESTABLISHED	ESTABLISHED	ESTABLISHED	ESTABLISHED	ESTABLISHED

### BGP Remote AS

192.168.1.48	192.168.1.51	192.168.1.101	192.168.1.102	192.168.1.103	192.168.1.104	192.168.204.204	192.168.205.205	
267613	268253	264144	264144	268253	20121	26162	26162	26162

CONSUMO DE PORTAS

Interface	min	max	avg	current	total
eth0	1.4 Gbps	2.0 Gbps	1.7 Gbps	1.6 Gbps	102.8 Gbps
eth1	144.0 Mbps	234.7 Mbps	185.9 Mbps	234.7 Mbps	11.2 Gbps
eth2	99.8 Mbps	223.8 Mbps	149.3 Mbps	135.7 Mbps	9.9 Gbps
eth3	16.0 Gbps	1.1 Gbps	652.7 Gbps	244.0 Gbps	39.2 Gbps
eth4	24.0 Gbps	56.0 Gbps	48.1 Gbps	22.0 Gbps	4.3 Gbps
eth5	12.7 Mbps	39.5 Mbps	23.9 Mbps	33.5 Mbps	1.5 Gbps
eth6	12.3 Mbps	2.4 Mbps	254.9 Mbps	2.4 Mbps	15.3 Mbps
eth7	16.9 Mbps	35.8 Mbps	24.7 Mbps	29.3 Mbps	1.5 Gbps
eth8	1.0 Gbps	1.5 Gbps	1.3 Gbps	1.4 Gbps	78.9 Gbps
eth9	36.7 Mbps	64.9 Mbps	50.4 Mbps	53.0 Mbps	3.9 Gbps
eth10	174.0 Gbps	246.7 Gbps	255.9 Gbps	14.8 Gbps	14.8 Gbps
eth11	146.0 Mbps	337.1 Mbps	207.1 Mbps	214.8 Mbps	12.4 Gbps
eth12	24.0 Gbps	160.0 Gbps	62.3 Gbps	32.0 Gbps	3.7 Gbps
eth13	1.8 Mbps	7.3 Mbps	4.1 Mbps	4.5 Mbps	247.0 Gbps
eth14	11.9 Mbps	20.3 Gbps	15.1 Mbps	16.2 Mbps	906.4 Gbps

## MONITORAMENTO BGP NE20 E NE40

STATUS SESSÃO BGP

CONTROLÉ DE SESSÕES ONLINE

UPTIME SESSÕES BGP

TOTAL PREFIXOS IPV4

PREFIX ACTIVE SESSÕES BGP

PREFIX RECEIVED SESSÕES BGP

PREFIX SENT SESSÕES BGP

MÓDULO ÓPTICO

192.168.1.48	192.168.1.51	192.168.1.101	192.168.1.102	192.168.1.103	192.168.1.104	192.168.1.200	192.168.204.204	192.168.205.205
-5.44 dbm	-5.09 dbm	-3.06 dbm	-5.11 dbm	-2.81 dbm	-2.67 dbm	-10.79 dbm		
-0.82 dbm	-0.27 dbm	-3.17 dbm	-1.02 dbm	-2.93 dbm	-3.22 dbm	-5.41 dbm		

25.00 °C	31.00 °C	32.00 °C	31.00 °C	30.00 °C	32.00 °C	24.00 °C	0 °C	0 °C	0 °C	0 °C
33.55 VA	33.57 VA	32.50 VA	33.06 VA	33.11 VA	31.85 VA	33.61 VA	0 VA	0 VA	0 VA	0 VA
0.62 mA	0.47 mA	0.08 mA	0.45 mA	0.08 mA	0.08 mA	0.17 mA	0 mA	0 mA	0 mA	0 mA

TRÁFEGO POR PORTA

DOWNLOAD

UPLOAD

## ESTATÍSTICAS BGP

BGP ESTABELECIDO: **223**

BGP DESATIVADOS: **17**

BGP OFFLINE: **54**

Latência	9.70 ms	7.90 ms	1.50 ms
ASes	10	10	10
Prefixos	10	10	10
Outros	10	10	10

Latência	119.2 ms	16.7 ms	24.9 ms	2.90 ms
ASes	10	10	10	10
Prefixos	10	10	10	10
Outros	10	10	10	10

## Pilha de dados

Gráficos de desempenho de rede e estatísticas de tráfego.



# A ponta do iceberg

## Disponibilidade

Serviços disponíveis sempre que o usuário desejar.



## Desempenho

Baixa latência e acesso fluido aos serviços e conteúdos.



## Segurança

Tecnologias que garantam a autenticidade, privacidade e integridade dos dados.



## Usabilidade

Facilidade de uso e interação, com uma rede "invisível" para o usuário.



## Escalabilidade

Capacidade da rede de crescer sem alterações significativas em seu projeto original.



## Gerenciamento

Gerenciamento FCAPS com melhor equilíbrio entre TCO, Capex, Opex e ROI.



# Compreendendo os domínios de gerenciamento

# Domínios de gerenciamento



# Gerenciamento de Falhas

- **Detecção de falhas de conectividade:** Identificação automática de quedas de link e notificação de equipes de suporte.
- **Monitoramento proativo de degradação de sinal:** Detecção de quedas de sinal em links de fibra óptica e alertas para equipes de suporte.
- **Verificação de redundância:** Garantir a operacionalidade e integridade dos links redundantes.
- **Detecção de falhas intermitentes:** Identificação e registro de falhas recorrentes que possam causar interrupções futuras.
- **Monitoramento do status de dispositivos de rede:** Verificação contínua do estado operacional de roteadores, switches e servidores.
- **Registro e notificação de falhas de hardware:** Detecção de problemas de hardware, como falhas em fontes de alimentação ou módulos de roteadores.
- **Automação de alertas de falha crítica:** Notificação imediata sobre falhas em equipamentos essenciais da rede.
- **Isolamento de falhas:** Implementação de mecanismos para isolamento automático de problemas, minimizando o impacto na rede.
- **Análise de causa raiz:** Facilitação da identificação e resolução das causas subjacentes de falhas frequentes.
- **Sistema de redundância ativa:** Gerenciamento automático do failover entre links redundantes.

# Gerenciamento de Configurações

- **Automação de backups de configuração:** Realização de cópias periódicas das configurações dos dispositivos para recuperação rápida.
- **Deteção de mudanças não autorizadas:** Monitoramento e alertas sobre alterações de configuração não autorizadas ou fora do padrão.
- **Centralização da gestão de configuração:** Gerenciamento centralizado para implementação e validação de políticas em toda a rede.
- **Automação de atualização de firmware:** Planejamento e execução de atualizações automaticamente para manter os dispositivos em conformidade.
- **Aplicação de templates de configuração:** Utilização de configurações padrão para garantir consistência e facilitar a expansão.
- **Rollback automático:** Implementação de mecanismos para restauração de configurações anteriores em caso de falhas após mudanças.
- **Documentação de configuração:** Registros de todas as alterações e configurações para auditoria e conformidade.
- **Verificação de conformidade de configuração:** Validação das configurações para que estejam de acordo com as políticas de rede e segurança.
- **Configuração de novos dispositivos:** Automação do provisionamento de novos equipamentos para rápida integração.
- **Gerenciamento de configuração multi-sites:** Controle remoto da configuração de dispositivos em diferentes localidades.

# Gerenciamento de Contabilidade

- **Medição de uso de banda por cliente:** Coleta de dados de consumo para cobrança e gerenciamento de recursos.
- **Relatórios de consumo mensal:** Geração de análises detalhadas de uso para avaliação e planejamento de capacidade.
- **Monitoramento de tráfego por IP:** Rastreamento de fluxos de dados dos clientes para garantir limites justos de uso.
- **Cobrança baseada no consumo:** Registros de informações para implementação de planos tarifários personalizados.
- **Otimização de custos de peering:** Análise e ajustes de tráfego nas conexões de peering e trânsito IP para controle de despesas.
- **Auditoria de consumo de banda:** Exame de padrões de uso e identificação de picos de demanda por cliente ou região.
- **Registros de acesso de usuários:** Acompanhamento de sessões de clientes para conformidade e controle de utilização.
- **Planejamento de capacidade:** Utilização de dados de consumo para dimensionamento da infraestrutura conforme o crescimento.
- **Monitoramento de recursos adicionais:** Acompanhamento da utilização de serviços extras, como IPs adicionais.
- **Relatórios de SLA:** Avaliação e documentação do cumprimento dos acordos de nível de serviço para clientes.

# Gerenciamento de Desempenho

- **Monitoramento de latência em tempo real:** Acompanhamento da latência de segmentos críticos para garantir SLAs.
- **Medição de perda de pacotes:** Identificação e correção de pontos de perda que prejudicarem o desempenho.
- **Deteção de gargalos de banda:** Identificação da sobrecarga em links e implementação de medidas de alívio.
- **Monitoramento do uso de CPU e memória:** Acompanhamento do consumo de recursos dos dispositivos para prevenção de sobrecarga.
- **Monitoramento de QoS:** Verificação de parâmetros de qualidade de serviço para priorização do tráfego essencial.
- **Avaliação de throughput:** Medição da taxa de transferência efetiva em links cruciais.
- **Previsão de capacidade:** Análise histórica de uso para prever e planejar expansões de capacidade.
- **Análise de desempenho de aplicações:** Verificação da performance de serviços críticos para evitar interrupções.
- **Monitoramento de jitter:** Avaliação de flutuações de latência que afetam a qualidade de aplicações em tempo real.
- **Gerenciamento de desempenho por SLA:** Monitoramento do desempenho em relação aos SLAs para assegurar a satisfação do cliente.

# Gerenciamento de Segurança

- **Monitoramento de tentativas de intrusão:** Detecção e alertas sobre tentativas de acesso não autorizado.
- **Análise e mitigação de ataques DDoS:** Identificação e aplicação de contramedidas automáticas para proteger a rede.
- **Monitoramento de autenticação e autorização:** Registros e análises de acessos a dispositivos para garantir conformidade.
- **Monitoramento de vulnerabilidades:** Condução de varreduras regulares para identificar e corrigir vulnerabilidades.
- **Auditoria de mudanças de configuração:** Assegurar que alterações de segurança sejam devidamente documentadas e autorizadas.
- **Monitoramento de políticas de firewall:** Verificação da conformidade das regras de firewall e de demais componentes com as políticas de segurança estabelecidas.
- **Detecção de anomalias de tráfego:** Identificação de padrões de tráfego incomuns que possam indicar ataques em curso.
- **Gerenciamento de certificados SSL:** Monitoramento e renovação de certificados proativamente para prevenir falhas de segurança.
- **Prevenção contra ameaças internas:** Identificação e investigação de acessos suspeitos ou anormais de usuários e clientes.
- **Respostas automatizadas a incidentes:** Implementação de protocolos de resposta automática para mitigação rápida de incidentes.
- **Segurança de roteamento:** Validação e aplicação da conformidade das políticas de roteamento.

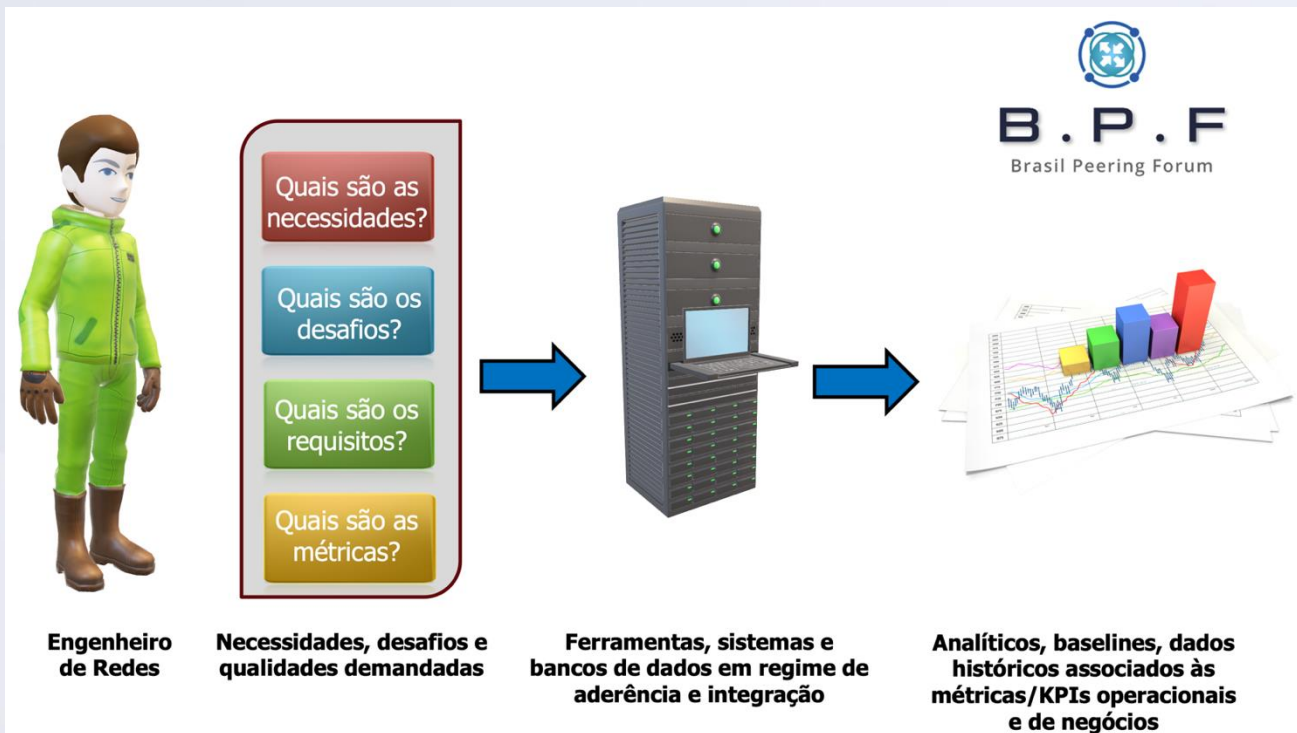


# Gerenciamento de Segurança

- **Monitoramento de latência em tempo real:** Acompanhamento da latência de segmentos críticos para garantir SLAs.
- **Medição de perda de pacotes:** Identificação e correção de pontos de perda que prejudicarem o desempenho.
- **Deteção de gargalos de banda:** Identificação da sobrecarga em links e implementação de medidas de alívio.
- **Monitoramento do uso de CPU e memória:** Acompanhamento do consumo de recursos dos dispositivos para prevenção de sobrecarga.
- **Monitoramento de QoS:** Verificação de parâmetros de qualidade de serviço para priorização do tráfego essencial.
- **Avaliação de throughput:** Medição da taxa de transferência efetiva em links cruciais.
- **Previsão de capacidade:** Análise histórica de uso para prever e planejar expansões de capacidade.
- **Análise de desempenho de aplicações:** Verificação da performance de serviços críticos para evitar interrupções.
- **Monitoramento de jitter:** Avaliação de flutuações de latência que afetam a qualidade de aplicações em tempo real.
- **Gerenciamento de desempenho por SLA:** Monitoramento do desempenho em relação aos SLAs para assegurar a satisfação do cliente.

A modernização requerida para as abordagens tecnológicas

# A modernização requerida



# A modernização requerida

- **Quais problemas você precisa resolver em alinhamento com os objetivos do negócio?**
- **Quais são suas necessidades de negócios, técnicas e operacionais?**
- **Quais dados são necessários para atender a cada uma dessas necessidades?**
- **Em quais sistemas e fontes de informação esses dados podem ser encontrados?**
- **Quais tecnologias estão disponíveis e devem ser utilizadas para consumir esses dados, e agir sobre eles, tanto northbound quanto southbound?**
- **Como não apenas representar resultados, mas também automatizar as ações dos domínios FCAPS em sua organização?**

# A modernização requerida

- **Filosofia de redes definidas por software:**
  - **Gerenciamento e telemetria modernizados com RESTCONF, gRPC/gNMI, NETCONF/YANG/OpenConfig, BMP, sFlow/NetFlow/IPFIX, e menor dependência de SNMPv3.**
  - **Integração com sistemas diversos por meio de APIs na camada northbound.**
  - **Modernização da camada southbound.**
  - **Foco em alinhar dados e ações com os objetivos técnico-operacionais, mapeados diretamente para os objetivos do negócio.**

Obrigado!