Artigos Técnicos

- Percentil 95 vs Quantidade de Amostragens
- Cache Inteligente de Requisições
- ISP: Cálculo de Tráfego para a ANATEL com Apenas um Clique!
- Compreendendo as diferenças entre as versões v1, v2c e v3 do SNMP
- Como Monitorar a Quantidade de Usuários por Servidor PPPoE Server no Mikrotik

Percentil 95 vs Quantidade de Amostragens

O **Percentil 95** é uma métrica estatística amplamente utilizada em diversas áreas, mas com destaque em **redes de computadores e telecomunicações**, para medir e tarifar o uso de largura de banda e para monitorar o desempenho de sistemas.

O que é um Percentil?

Um percentil é uma medida que indica o valor abaixo do qual uma dada porcentagem de observações em um conjunto de dados ordenado cai. Por exemplo, o 50º percentil é a mediana, o valor abaixo do qual 50% dos dados se encontram.

Percentil 95 em Redes de Computadores e Telecomunicações

No contexto de redes, especialmente para provedores de internet (ISPs) e empresas que contratam links dedicados, o Percentil 95 é uma metodologia de **medição e cobrança de tráfego de dados**. A ideia é oferecer um modelo de faturamento mais flexível e justo, que acomode picos de uso ocasionais sem penalizar o cliente com custos excessivos.

Como funciona?

1. **Coleta de Dados:** O uso de largura de banda é monitorado e amostrado em intervalos regulares, geralmente a cada 5 minutos, ao longo de um período de tempo (tipicamente um mês). Cada amostra representa a média da largura de banda utilizada nesse intervalo.
2. **Ordenação:** Ao final do período de medição, todas essas amostras são coletadas e ordenadas em ordem crescente, do menor uso de banda para o maior.
3. **Descarte dos Picos:** Os **5% maiores valores de uso de largura de banda são descartados**. Isso significa que os picos de tráfego mais elevados e esporádicos, que poderiam inflacionar o custo, não são considerados na cobrança.

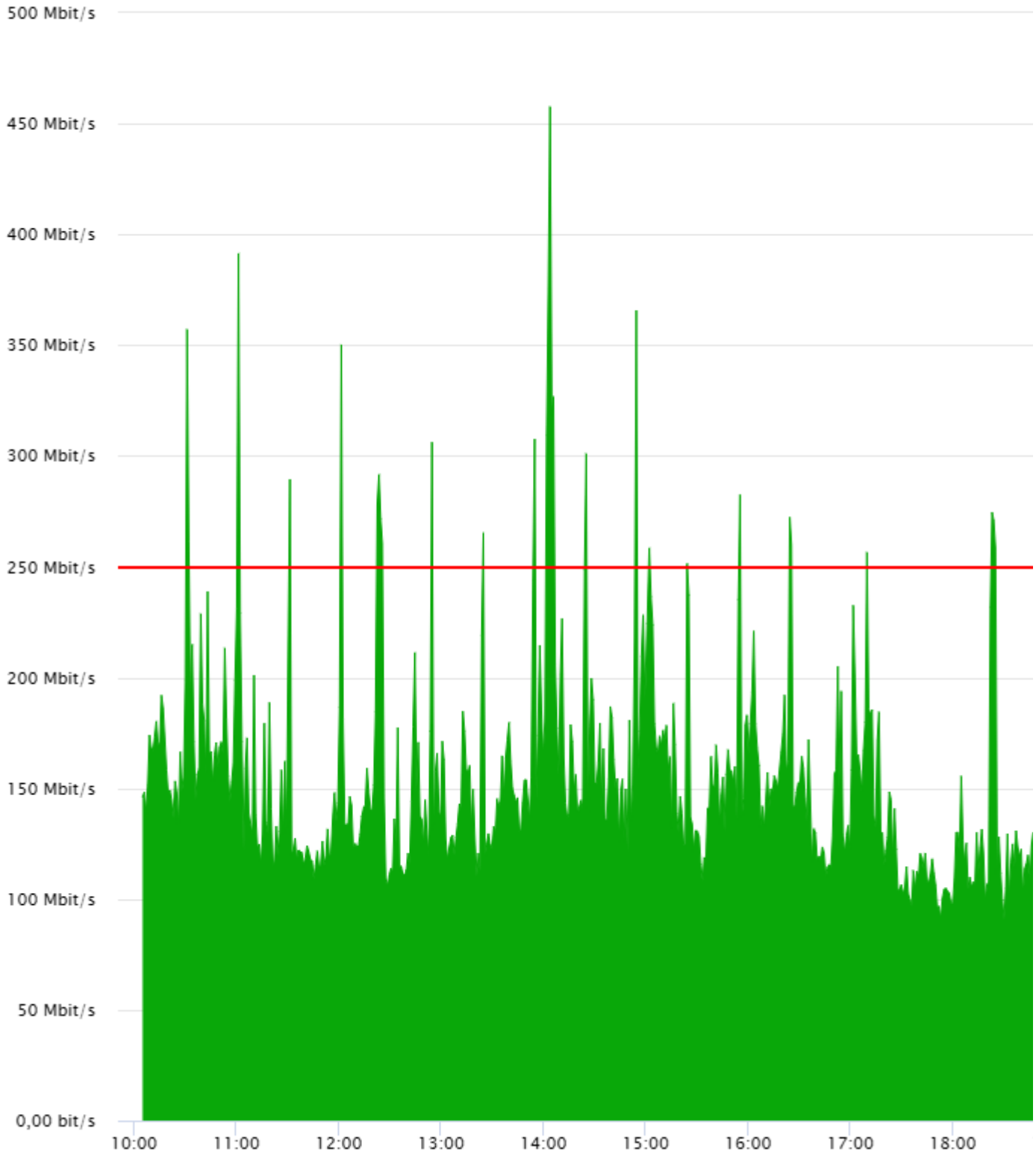
4. **Cálculo do Percentil 95:** O próximo valor mais alto após o descarte dos 5% superiores é o **Percentil 95**. Este é o valor que será utilizado para a cobrança. Em outras palavras, 95% do tempo, o uso de largura de banda esteve abaixo ou igual a esse valor.

Impacto da Granularidade da Amostragem no Percentil 95

No monitoramento de tráfego de dados, a **granularidade da amostragem** — ou seja, a frequência com que os dados são coletados — tem um impacto direto no valor do percentil 95. No experimento abaixo, observamos que o percentil 95 foi **maior em monitoramentos com amostragem a cada 1 minuto** em comparação com monitoramentos com amostragem a cada 5 minutos.

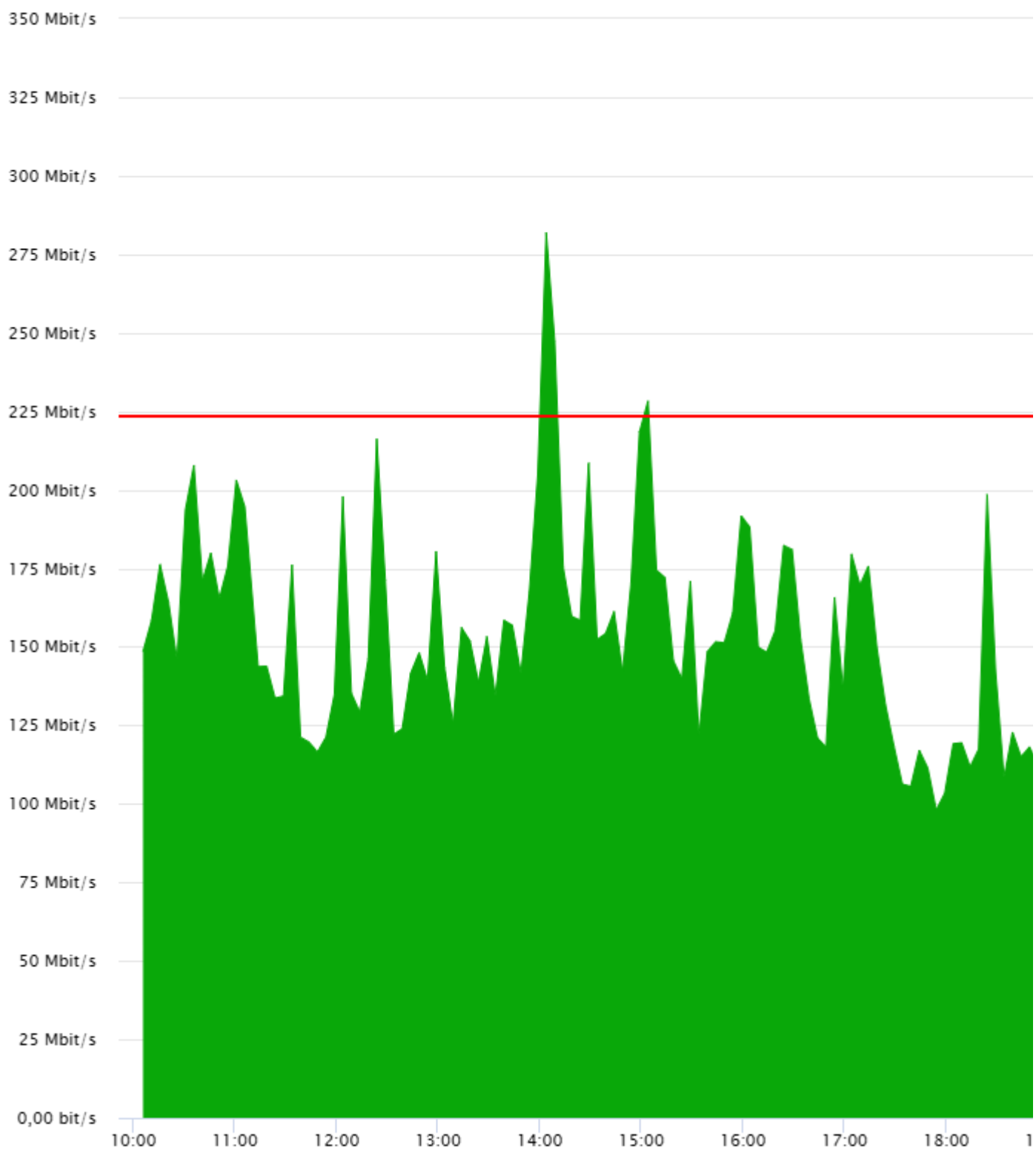
Isso ocorre devido à capacidade inerente da amostragem mais frequente de capturar variações mais rápidas e picos de uso. Vamos detalhar tecnicamente:

Amostragem a Cada 1 Minuto: Captura mais Precisa de Picos



Quando os dados são amostrados a cada 1 minuto, o sistema de monitoramento registra o tráfego de dados em intervalos muito curtos. Isso permite que ele **capture com maior precisão os picos de uso transitórios e de curta duração**. Imagine um cenário onde há um aumento abrupto no tráfego de dados por 30 segundos e depois ele retorna aos níveis normais. Uma amostragem a cada 1 minuto tem uma alta probabilidade de registrar esse pico, já que o intervalo de coleta possui um intervalo menor entre as amostras.

Amostragem a Cada 5 Minutos: Suavização dos Picos

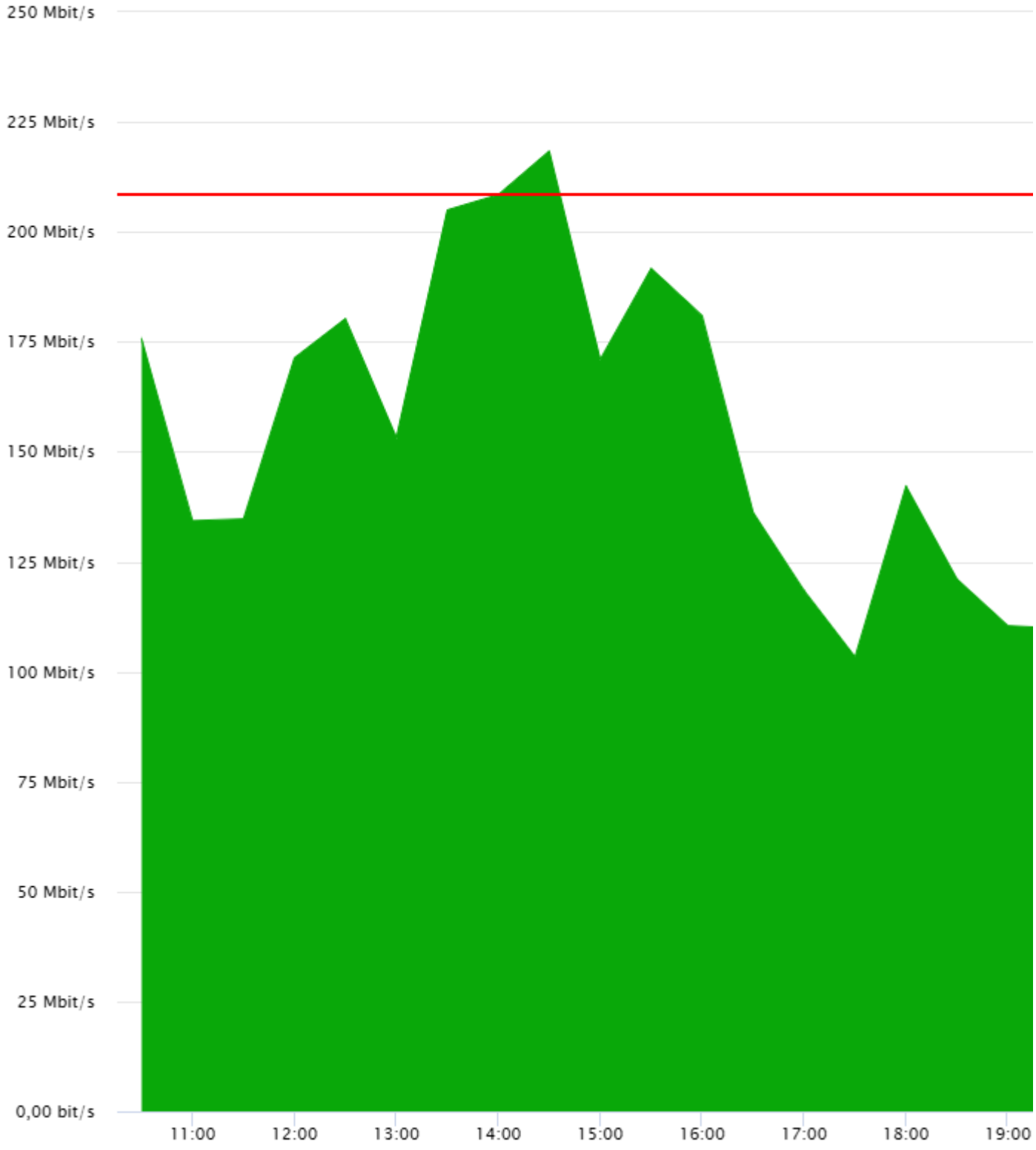


Por outro lado, quando a amostragem é realizada a cada 5 minutos, o sistema calcula uma média do tráfego de dados ao longo de um período de 300 segundos. Essa média de tempo maior inerentemente **suaviza os picos de uso**. Se ocorrer um pico de tráfego de curta duração (por exemplo, 30 segundos) dentro de um intervalo de 5 minutos, seu impacto é diluído pela média dos

4 minutos e 30 segundos restantes de tráfego potencialmente mais baixo.

Em termos técnicos, cada amostra de 5 minutos é uma representação agregada do tráfego nesse intervalo. A menor frequência de amostragem resulta em um conjunto de dados mais "suavizado", onde as variações rápidas são menos perceptíveis. Os valores extremos (os picos) são "achatados" devido ao cálculo da média sobre um período mais longo, o que resulta em um percentil 95 menor. Isso não significa que os picos não existam, mas sim que a amostragem com menor granularidade não os registra com a mesma fidelidade.

Como exemplo, o gráfico abaixo possui um intervalo de amostragem a cada 30 minutos. A diferença do percentil 95 para as demais amostragens atenua consideravelmente:



Conclusão

A escolha da granularidade da amostragem em monitoramento de tráfego de dados é crucial e depende dos objetivos da análise. Para uma **detecção precisa e oportuna de picos de uso** e

para entender a capacidade de explosão da rede, uma **amostragem mais granular (como a cada 1 minuto)** é preferível, mesmo que resulte em um percentil 95 mais alto. Isso fornece uma visão mais detalhada e fiel do comportamento da rede em momentos de alta demanda. Se o objetivo é ter uma visão mais consolidada e estável do tráfego médio e descartar flutuações muito rápidas, uma amostragem menos granular (como a cada 5 minutos) pode ser suficiente. É importante estar ciente de que amostras com intervalos grandes pode subestimar a magnitude real dos picos de uso.

Contato

Monsta Tecnologia Ltda

Site: http://www.monsta.com.br

Downloads: http://www.monsta.com.br/download.html

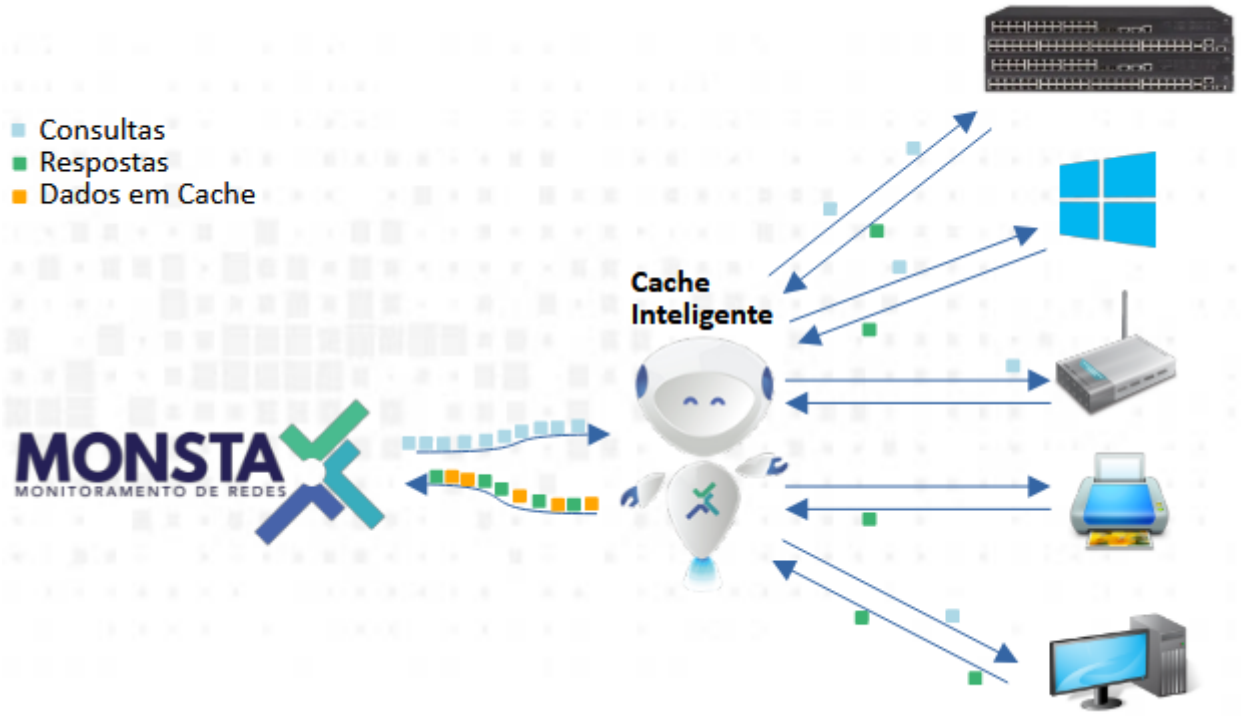
E-mail: contato@monsta.com.br

MONSTA

MONITORAMENTO DE REDES

Cache Inteligente de Requisições

O Monsta emprega um sistema de **cache inteligente de requisições de instâncias** para otimizar o monitoramento de rede, reduzindo significativamente o consumo de banda e o uso de recursos computacionais tanto no dispositivo monitorado quanto no servidor onde o Monsta está hospedado. Este mecanismo opera identificando e armazenando dados de requisições previamente consultadas, evitando a necessidade de novas solicitações para informações já conhecidas.



Funcionamento Técnico

O processo de cache inteligente pode ser detalhado nas seguintes etapas:

1. **Interceptação da Requisição**: Quando um monitor inicia uma requisição para obter informações de um dispositivo de rede (por exemplo, velocidade de uma porta, memória total, lista de instâncias, etc.), a requisição é primeiro interceptada pelo módulo de cache

inteligente.

2. **Validação das instâncias:** O Monsta utiliza uma técnica para validar se houve modificação das propriedades da instância requisitada:
    1. Quando existem alterações, o cache é marcado como expirado e uma nova consulta é efetuada;
    2. Se não existem alterações, a consulta será encaminhada ao cache.

3. **Verificação do Cache**: Antes de encaminhar a requisição ao dispositivo monitorado, o módulo de cache verifica se a instância solicitada já existe em seu **repositório de cache local**. Essa verificação é baseada em um identificador único para cada tipo de requisição e para cada dispositivo.

4. **Cache Hit**:
    1. **Pesquisas individuais:** Se a instância for encontrada no cache (**cache hit**) e estiver dentro de seu período de validade, o Monsta **não envia a requisição para o dispositivo**. Em vez disso, a resposta previamente armazenada é imediatamente retornada a métrica solicitante.

    2. **Walk:** Para consultas que necessitem obter informações de parte da árvore de OID's, como por exemplo o nome de interfaces de rede através de um snmpwalk, o Monsta utiliza técnicas que apenas revalidam o cache quando existirem alterações de posições de seus elementos. Nesse caso o tempo de TTL (Time-to-Live) não é utilizado.

       Estes processos eliminam a necessidade de tráfego de rede e o processamento da requisição pelos dispositivos monitorados, além de poupar recursos do servidor Monsta que seriam despendidos na comunicação e processamento da resposta.

5. **Cache Miss**:
   Se a instância não for encontrada no cache (**cache miss**) ou se o seu período de validade tiver expirado, a requisição é então **enviada para o dispositivo de rede monitorado**. Após o dispositivo responder, a informação é processada e, antes de ser entregue ao módulo solicitante, uma cópia é **armazenada no cache** juntamente com um novo TTL. O TTL é configurável e determina por quanto tempo a informação é considerada válida no cache.

6. **Gerenciamento do TTL (Time-To-Live)**:
   Cada item armazenado no cache possui um TTL associado. Este valor define a "vida útil" da informação no cache. Uma vez que o TTL expira, a informação é considerada desatualizada e a próxima requisição por essa informação resultará em um "cache miss", forçando uma nova consulta ao dispositivo para garantir a obtenção dos dados mais recentes. O TTL pode ser ajustado com base na criticidade e na frequência de atualização das informações. Para ajustá-lo, acesse o menu Configurações, Parâmetros e altere seu tempo na variável inst.cache_ttl_secs (o valor padrão é de 10 segundos). Configurar esse valor para "0" elimina o cache das pesquisas individuais.

Benefícios Técnicos

- **Redução de Carga no Dispositivo Monitorado**: Diminui o número de requisições processadas pelos dispositivos de rede, liberando recursos para suas funções primárias.
- **Otimização do Uso de Banda de Rede**: Minimiza o tráfego de monitoramento na rede, especialmente em ambientes com grande volume de dispositivos ou links de baixa largura de banda.
- **Economia de Recursos do Servidor Monsta**: Reduz o consumo de CPU e memória no servidor Monsta, uma vez que muitas respostas são entregues diretamente do cache, evitando o overhead de comunicação de rede.
- **Melhora da Latência de Resposta**: As requisições que resultam em um "cache hit" são respondidas instantaneamente, melhorando a experiência do usuário e a agilidade na visualização dos dados.

O cache inteligente de requisições do Monsta é um componente fundamental para garantir a **escalabilidade** e a **eficiência** do sistema, permitindo monitorar grandes e complexas infraestruturas de rede com performance otimizada.

Contato

Monsta Tecnologia Ltda

Site: http://www.monsta.com.br

Downloads: http://www.monsta.com.br/download.html

E-mail: contato@monsta.com.br

MONSTA

MONITORAMENTO DE REDES

ISP: Cálculo de Tráfego para a ANATEL com Apenas um Clique!

Se você é um provedor de telecomunicações, sabe que o cálculo semestral do total de bytes trafegados para a internet é uma exigência da ANATEL. Essa tarefa, que muitas vezes envolve a coleta manual de dados e o processamento em planilhas, pode ser demorada e sujeita a erros.

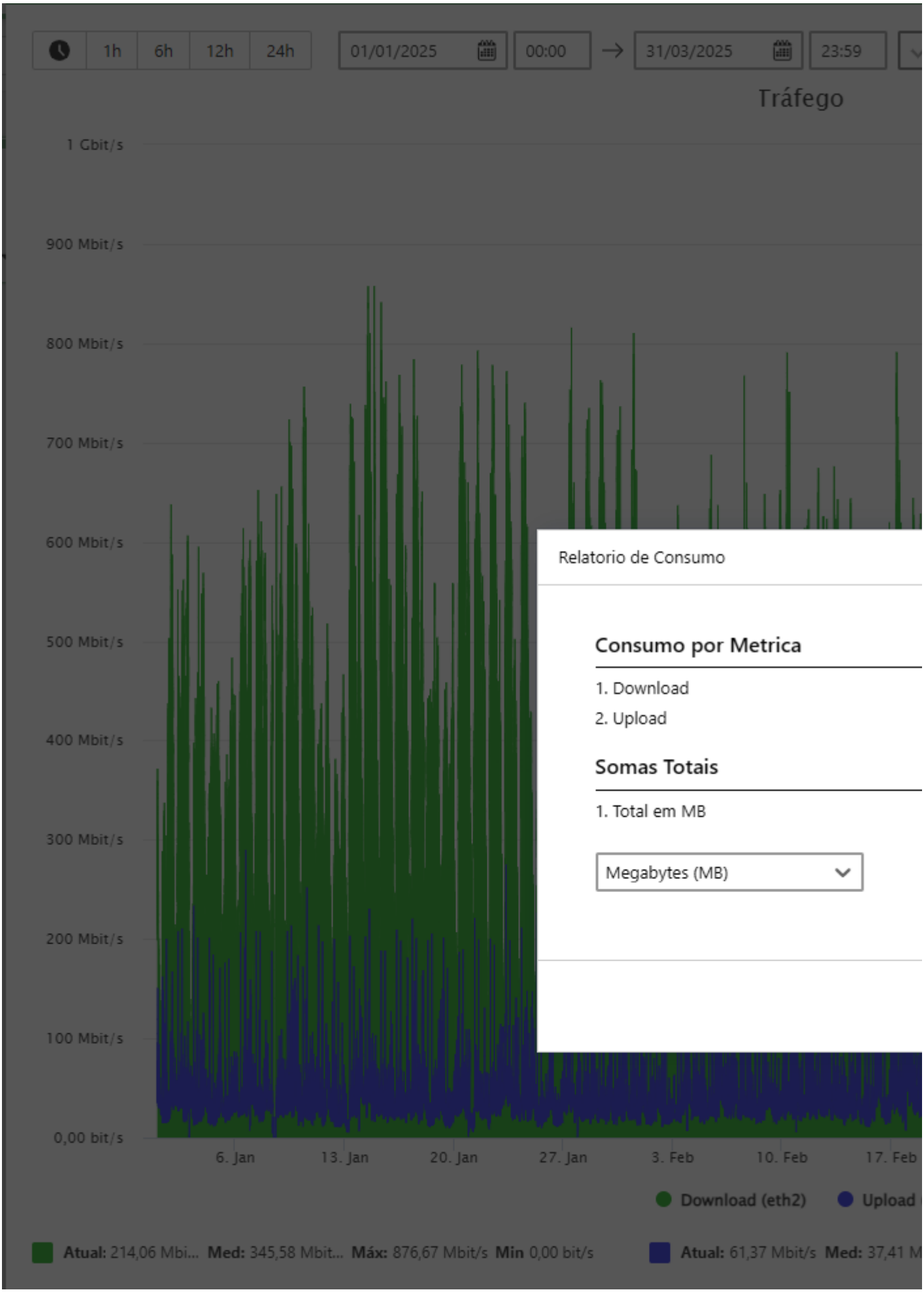
Na Monsta, nós entendemos a importância de simplificar o seu dia a dia. Por isso, desenvolvemos uma nova funcionalidade que automatiza completamente esse processo.

Adeus, Planilhas e Horas de Trabalho!

Com apenas um clique, você pode gerar o relatório completo com o total de tráfego de internet, pronto para ser entregue à ANATEL. Nossa ferramenta coleta todos os dados necessários de forma precisa e segura, eliminando a necessidade de qualquer intervenção manual.

Como Funciona?

1. No menu Dispositivos, selecione o dispositivo e clique sobre o monitor de tráfego que deseja efetuar o cálculo.
2. Selecione o período da consulta.
3. Após gerar o gráfico com o consumo do período, clique em ☰ localizado no canto superior direito do gráfico.
4. Selecione a opção "Relatório de Consumo".


1h
6h
12h
24h
01/01/2025
00:00
31/03/2025
23:59
Tráfego
1 Gbit/s
900 Mbit/s
800 Mbit/s
700 Mbit/s
600 Mbit/s
500 Mbit/s
400 Mbit/s
300 Mbit/s
200 Mbit/s
100 Mbit/s
0,00 bit/s
6. Jan
13. Jan
20. Jan
27. Jan
3. Feb
10. Feb
17. Feb
Relatorio de Consumo
Consumo por Metrica
1. Download
2. Upload
Somas Totais
1. Total em MB
Megabytes (MB)
Download (eth2)
Upload
Atual: 214,06 Mbi... Med: 345,58 Mbit... Máx: 876,67 Mbit/s Min 0,00 bit/s
Atual: 61,37 Mbit/s Med: 37,41 M

Pronto! O sistema faz o cálculo e entrega o resultado em segundos. A soma total é o valor que deve ser reportado a Anatel.

Essa novidade foi criada para que você possa focar no que realmente importa: a gestão e o crescimento do seu negócio. Com a nova ferramenta do Monsta, o cumprimento da exigência da ANATEL se torna uma tarefa rápida, simples e sem complicações.

Contato

Monsta Tecnologia Ltda

Site: http://www.monsta.com.br

Downloads: http://www.monsta.com.br/download.html

E-mail: contato@monsta.com.br

MONSTA

MONITORAMENTO DE REDES

Compreendendo as diferenças entre as versões v1, v2c e v3 do SNMP

O Simple Network Management Protocol (SNMP) é um protocolo fundamental para o gerenciamento e monitoramento de dispositivos em redes de computadores. Ele permite que administradores de rede coletem informações, configurem parâmetros e recebam notificações de eventos em roteadores, switches, servidores e outros equipamentos.

Desde sua criação, o SNMP passou por evoluções significativas para se adaptar às crescentes demandas de segurança e funcionalidade. As versões mais conhecidas e utilizadas são a v1, v2c e v3. Embora todas tenham o mesmo propósito central, elas se distinguem por recursos, principalmente em termos de segurança.

SNMP v1: O Pioneiro Simples e Inseguro

Lançada em 1988, a versão SNMPv1 foi a primeira a ser amplamente adotada. Ela se destacou por sua simplicidade, utilizando um modelo de gerenciamento baseado em comunidades. Uma comunidade é, essencialmente, uma senha de texto simples (chamada de string de comunidade) que permite o acesso de leitura ou leitura/escrita a um dispositivo.

- **String de Comunidade:** É o único mecanismo de "autenticação". Se a string de comunidade do gerenciador de rede corresponder à do dispositivo, o acesso é concedido.
- **Mensagens:** Utiliza três tipos básicos de mensagens: GET (para obter valores), SET (para alterar valores) e TRAP (para notificar eventos).
- **Vulnerabilidade:** A principal fraqueza do SNMPv1 é a falta de segurança. As strings de comunidade são transmitidas em texto puro, tornando-as suscetíveis a interceptação e uso malicioso. Isso significa que qualquer pessoa com acesso à rede pode capturar o tráfego e descobrir a comunidade, obtendo acesso ao SNMP dos dispositivos.

> Recomenda-se o uso do SNMP v1 apenas se o equipamento não possui suporte às versões seguintes, devido às suas limitações.

SNMP v2c: Melhorias e Maior Flexibilidade

O SNMPv2 foi uma tentativa de modernizar o protocolo, introduzindo melhorias substanciais. A versão SNMPv2c (onde o "c" significa Community-Based, ou seja, "baseado em comunidades") manteve o modelo de segurança do SNMPv1, mas trouxe avanços importantes em outras áreas.

- **Melhorias na Mensagem:** Introduziu novos tipos de mensagens, como GETBULK, que permite a recuperação de grandes volumes de dados de forma mais eficiente, reduzindo a carga na rede. Também aprimorou o mecanismo de TRAP com a introdução do INFORM, que confirma o recebimento da notificação.
- **Tipos de Dados:** Aprimorou a definição de tipos de dados, oferecendo mais flexibilidade e precisão na representação das informações gerenciadas.
- **Suporte a Variáveis de 64 bits:** Uma melhoria técnica significativa é a capacidade de gerenciar valores maiores, como contadores de tráfego de rede. O SNMPv1 é limitado a contadores de 32 bits, que podem atingir o valor máximo e "virar" (reiniciar do zero) rapidamente em redes de alta velocidade. O SNMPv2c e o v3 suportam contadores de 64 bits, que podem rastrear volumes de dados muito maiores antes de "virar", oferecendo estatísticas mais precisas e confiáveis para o monitoramento de tráfego.
- **Modelo de Comunidade:** Apesar das melhorias, o SNMPv2c ainda utiliza a mesma abordagem de segurança do SNMPv1, com strings de comunidade transmitidas em texto simples. Por isso, ele herda as mesmas vulnerabilidades de segurança, tornando-o inadequado para ambientes onde a confidencialidade é crítica.

SNMP v3: A Resposta para a Segurança

O SNMPv3 representa um salto gigantesco em termos de segurança e é a versão recomendada para o gerenciamento de redes modernas. Ele abandona o modelo de comunidades e implementa um framework robusto de segurança e autenticação.

- **Autenticação (Authentication):** O SNMPv3 exige a configuração de um nome de usuário e uma senha para cada dispositivo. As mensagens são assinadas digitalmente para garantir que vêm de uma fonte confiável. Isso impede que terceiros mal-intencionados injetem mensagens falsas na rede. Os algoritmos de autenticação mais comuns são MD5 e SHA.
- **Privacidade (Privacy):** Além da autenticação, o SNMPv3 oferece criptografia. Os dados transmitidos entre o gerenciador e o dispositivo podem ser criptografados, impedindo que sejam lidos caso sejam interceptados. Os algoritmos de criptografia mais utilizados são DES e AES.
- **Modelo de Usuário:** A segurança é baseada em usuários, onde cada um pode ter diferentes níveis de acesso e permissões. Isso permite um controle de acesso granular e mais rigoroso.

Característica	SNMP v1	SNMP v2c	SNMP v3
Segurança	Nenhuma (texto simples)	Nenhuma (texto simples)	Autenticação e Criptografia
Autenticação	String de Comunidade	String de Comunidade	Usuário e Senha (MD5/SHA)
Criptografia	Não	Não	Sim (DES/AES)

Tipos de Mensagem	GET, SET, TRAP	GETBULK, INFORM (e as da v1)	GETBULK, INFORM (e as da v1)

Portas de Comunicação

O protocolo utiliza duas portas de comunicação por padrão:

- **161/UDP**: para comunicação do gerente (sistema de monitoramento) para o agente (equipamento que é monitorado);
- **162/UDP**: para comunicação do agente para o gerente (comunicações que parte do equipamento monitorado, como no caso do **TRAP**).

Alguns equipamentos permitem alterar as configurações do SNMP, como comunidade, porta e, para o caso de SNMPv3, credenciais de autenticação e tipo de criptografia. É sempre importante verificar nas configurações do equipamento essas informações para utilizar no sistema de monitoramento.

Monsta

O Monsta tem suporte às três versões do SNMP e permite informar os parâmetros necessários para monitorar os equipamentos de acordo com cada versão (comunidade, porta, usuário, senha, tipo de criptografia).

No momento, o Monsta atua apenas com a comunicação **gerente > agente**, utilizando os tipos de mensagem **GET** e **GETBULK**.

Contato

Monsta Tecnologia Ltda

Site: http://www.monsta.com.br

Downloads: http://www.monsta.com.br/download.html

E-mail: contato@monsta.com.br


MONSTA
MONITORAMENTO DE REDES

Como Monitorar a Quantidade de Usuários por Servidor PPPoE Server no Mikrotik

Para provedores que utilizam o **Mikrotik** como concentrador PPPoE, saber o número exato de clientes conectados em cada servidor é uma métrica essencial. Este guia rápido mostra como você pode configurar o **Monsta** para monitorar o total de usuários por `pppoe-server`.

1. Coleta de Dados

O método utilizado para obter a contagem *por servidor* no Mikrotik é através da execução de um comando via **SSH** (Secure Shell).

1.1. Configuração de Acesso no Mikrotik

Antes de configurar no Monsta, seu Mikrotik deve permitir o acesso SSH:

1. **Crie um Usuário Específico:** No Mikrotik, crie um usuário (ex: `monsta`) com uma senha forte e permissões mínimas (apenas o necessário para executar o comando, como `read`).
2. **Habilite o Serviço SSH:** Garanta que o serviço SSH (porta 22, por padrão) esteja ativo e que o Firewall do Mikrotik permita conexões de entrada do IP onde o seu Monsta está instalado.

2. Configurando o Monitor no Monsta

Clique no botão para adicionar um novo dispositivo e insira as seguintes informações:

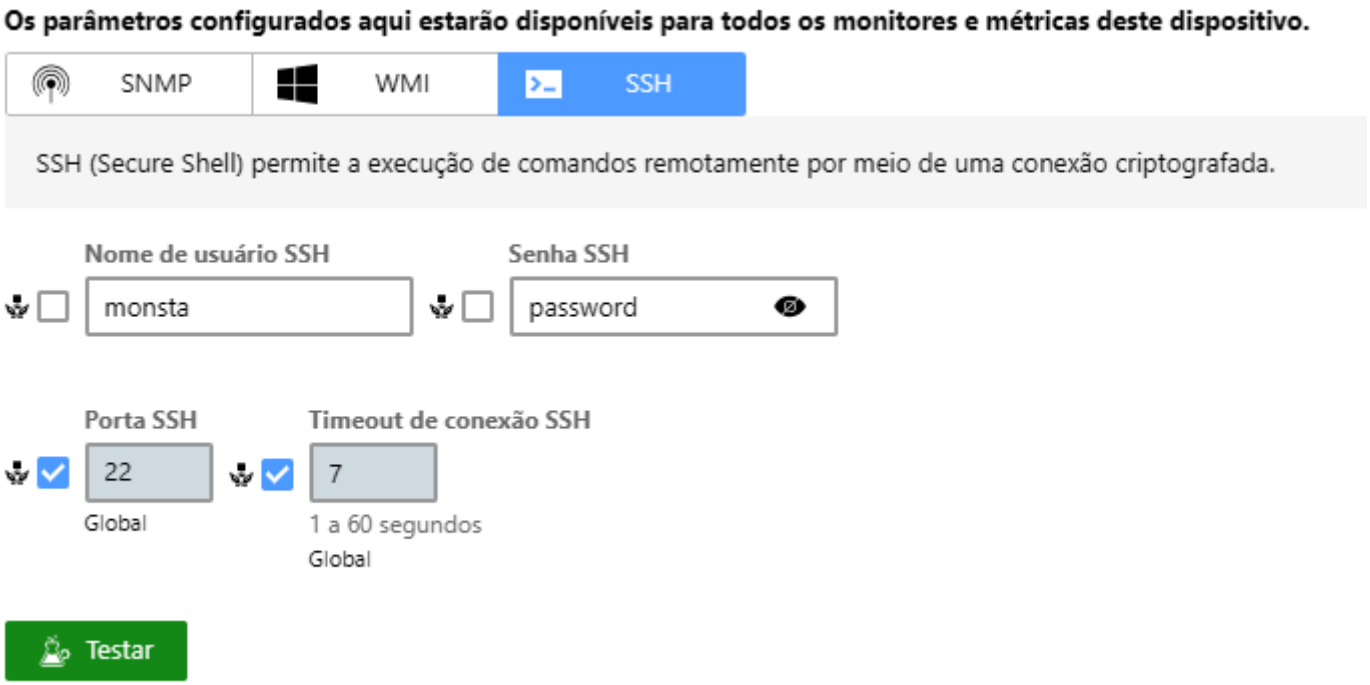
1. Na aba Detalhes, preencha as seguintes informações:
    1. Nome do Dispositivo: Nesse campo digite qualquer texto que identifique seu equipamento;

2. Endereço IP: Informe o IP do Mikrotik;

2. Na aba Templates, selecione "Mikrotik Routerboard;
3. Na aba coleta, preencha a opção "SSH" com o usuário, senha e porta caso seja diferente da 22.

> Dica: Você pode utilizar o botão "Testar" para checar se a conexão está ok.

4. Clique em Salvar para criar o novo dispositivo.

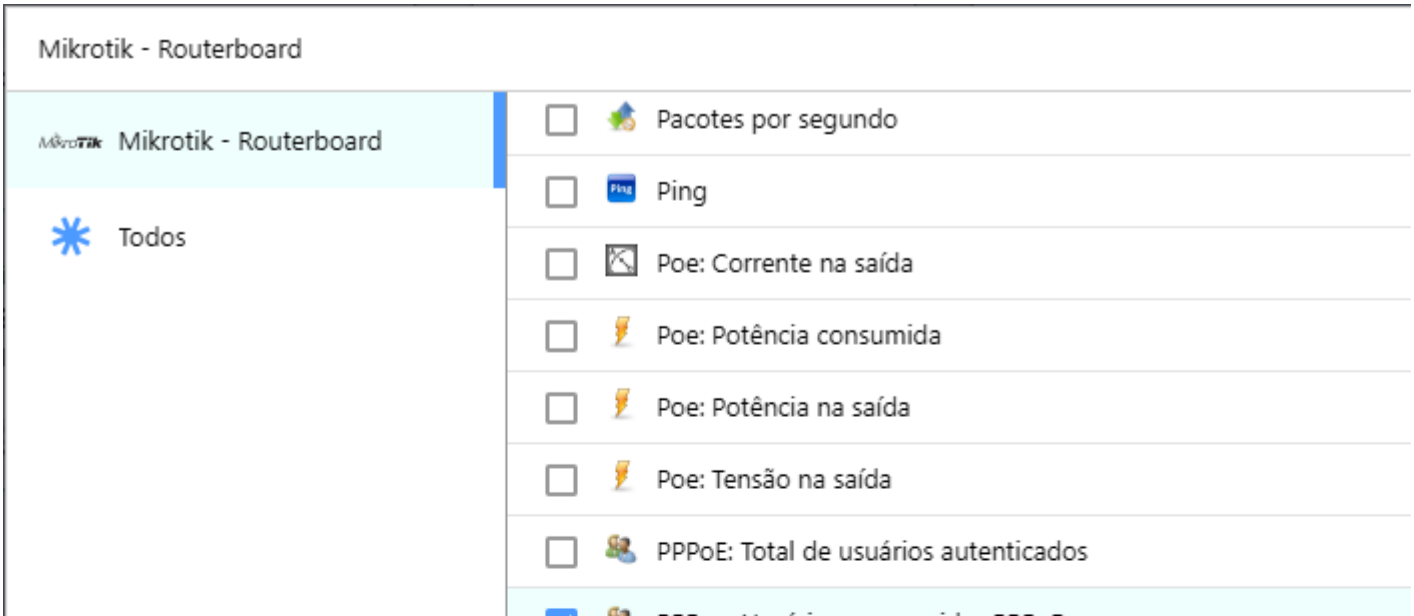


Tela de configuração do SSH

3. Criando o Monitor de Usuários

Após criar o dispositivo, clique sobre ele para que os monitores apareçam na parte inferior da tela. Clique em "+" para adicionar um novo monitor.

Na janela de monitores, procure por "PPPoE: Usuários por servidor PPPoE" e selecione qual servidor você deseja monitorar a quantidade de usuários.



Tela para adicionar monitores

Clique no botão para criar o monitor.

Agora seu Monsta monitora o total de usuários dentro desse servidor. Se deseja adicionar o monitoramento de outros servidores, basta clicar novamente em "+" e selecionar as opções disponíveis.

> Dica: Ao abrir o monitor para visualizar seu gráfico, clique no botão "Editar" localizado no canto superior direito e informe os limites no qual gostaria de receber alertas em caso de problemas.

Exemplo de limites de alerta

Contato

Monsta Tecnologia Ltda

Site: http://www.monsta.com.br

Downloads: http://www.monsta.com.br/download.html

E-mail: contato@monsta.com.br

MONSTA
MONITORAMENTO DE REDES