

Prof. Esp. Thalles Canela

- **Graduado:** Sistemas de Informação - Wyden Facimp
- **Pós-graduado:** Segurança em redes de computadores - Wyden Facimp
- **Consultor de Tecnologia - [aXR6] Cyber Security e NtecSoftware**
- **Professor no Senac (contratado)**
- **Professor na Wyden Facimp (contratado)**
 - **Pós-graduação:** Segurança em redes de computadores - Wyden Facimp
- **Professor na Wyden Facimp (Efetivado)**
 - **Graduação:** Análise e desenvolvimento de sistemas - Wyden Facimp

Redes sociais:

- **Linkedin:** <https://www.linkedin.com/in/thalles-canela/>
- **YouTube:** <https://www.youtube.com/aXR6CyberSecurity>
- **Facebook:** <https://www.facebook.com/axr6PenTest>
- **Instagram:** https://www.instagram.com/thalles_canela
- **Github:** <https://github.com/ThallesCanela>
- **Github:** <https://github.com/aXR6>
- **Twitter:** <https://twitter.com/Axr6S>

O que é SNMP

- *Simple Network Management Protocol* é um dos protocolos mais utilizados para auxiliar na gerência de redes e protocolo.
- O protocolo simples de gerência de rede (SNMP da siga em Inglês) teve sua origem na RFC 1067 em 1988.
- Conforme necessidades tecnológicas, evoluiu em segurança e performance por algumas versões, estando atualmente na versão 3.
- É um protocolo da camada de aplicação (camada sete do modelo OSI) que utiliza usualmente a porta 161 do protocolo de transporte UDP.

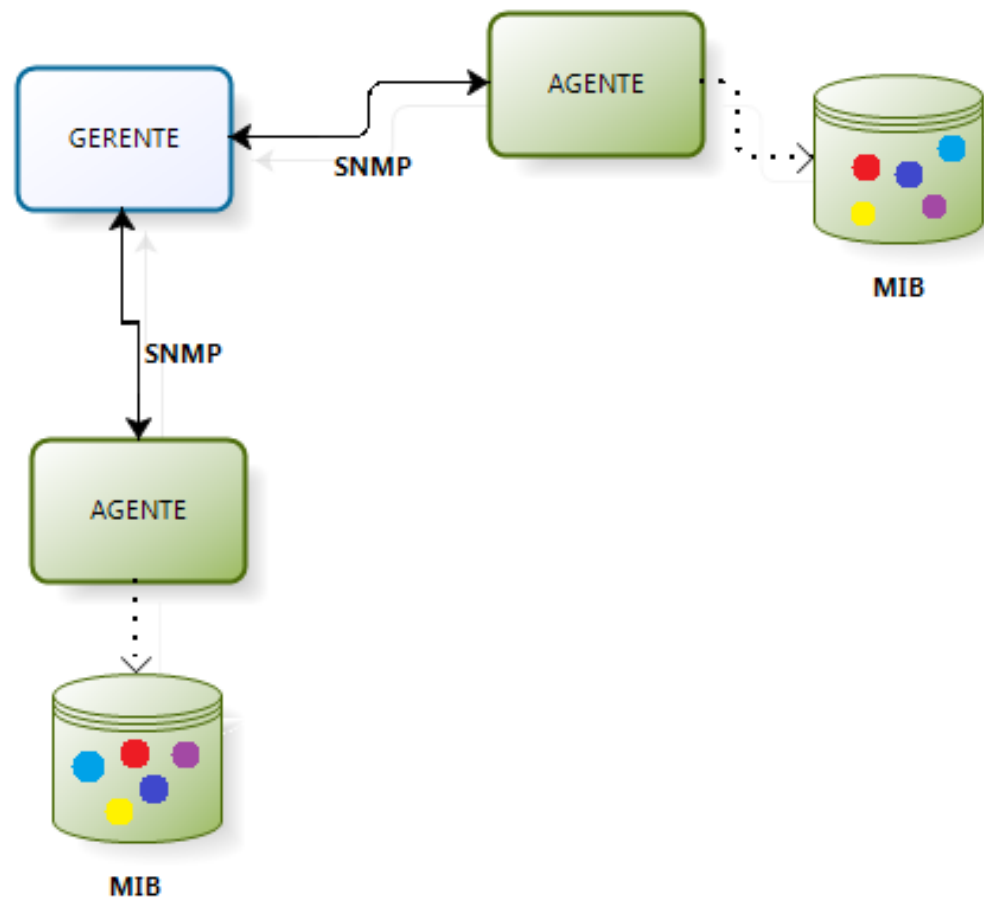
Vantagens do *Simple Network Management Protocol*

- A vantagem de ser um protocolo de camada sete reside no fato da abstração das outras camadas da rede.
- Assim sendo, o gestor pode gerenciar um dispositivo que se encontre fora da sua rede de origem.
- Em virtude de consumir poucos recursos da rede e de processamento, o protocolo acabou se disseminando.
- Isto permitiu a sua inclusão em equipamentos bastante simples como, por exemplo, impressoras.

Vantagens do *Simple Network Management Protocol*

- O SNMP ajuda o gestor da rede a localizar eventuais problemas e falhas em sua rede.
- Através de um gerente SNMP, pode-se visualizar gráficos referentes a estatísticas de tráfego, nível do toner em impressoras, CPU e memória de diversos dispositivos.
- Até mesmo a quantidade de processos que estão sendo executados em um dado dispositivo pode ser analisada.
- Além do gerenciador SNMP, é necessário que cada dispositivo que se deseja monitorar tenha um agente SNMP.
- O agente receberá as requisições do gerente e retornará com as informações.
- A estrutura pode ser visualizada na figura 1.

Vantagens do *Simple Network Management Protocol*



Conexão

- Quando se fala em protocolo SNMP é importante ter em mente que ele não é orientado a uma conexão além de não requerer ações prévias ou posteriores ao envio de mensagens.
- Ele foi desenvolvido com o propósito de ser uma solução leve, já que os equipamentos que ocupam a posição de ponta — hubs, switches, roteadores e servidores de rede — têm um poder de processamento baixo.

Habilitação

- O SNMP não pode ser instalado, tendo em vista que ele já vem de fábrica. O que o usuário pode fazer é habilitá-lo.

Arquitetura

- A arquitetura do SNMP conta com um manager e uma aplicação, funcionando da mesma maneira que um sistema de gerência de rede. O funcionamento ocorre por meio de uma solução ou da alteração de configuração do status.

Dashboards

- Hoje, ferramentas mais evoluídas oferecem a opção de [dashboards](#), que são painéis visuais que apresentam dados de indicadores críticos relacionados ao funcionamento da rede, por meio de informações emitidas em tempo real.
- O protocolo SNMP é um meio de acessar informações de maneira fácil e rápida, de diferentes sistemas e no momento em que as coisas estão acontecendo.
- De forma resumida, podemos dizer que a função essencial do SNMP é facilitar o processo de troca de informações de gerenciamento entre dispositivos de uma rede. Isso é feito por meio do fornecimento de dados de status dos elementos ativos da rede e estatísticas relevantes acerca do seu funcionamento, como por exemplo, taxa de erros, vazão, uso, entre outros.

O que pode ser monitorado a partir do protocolo SNMP?

- Uma das características que torna o protocolo tão popular é que ele consome poucos recursos de rede e de processamento, isso faz com que ele possa ser utilizado até em equipamentos mais simples.
- Mas, afinal, o que pode ser monitorado por meio do SNMP? Entre as informações passíveis de monitoramento podemos destacar:

O que pode ser monitorado a partir do protocolo SNMP?

- quantidade de processos que estão sendo executados em cada dispositivo;
- estatísticas de tráfego;
- informações atualizadas sobre a quantidade de toner nas impressoras;
- informações sobre uso da memória dos dispositivos.

Por que é importante contar com um protocolo SNMP?

- Situação: Imagine que sua organização tem 1.000 dispositivos e você foi solicitado a verificar cada um deles todos os dias.
- Resolvendo: Normalmente, o SNMP usa um ou vários computadores administrativos (gerentes) para supervisionar grupos de computadores em rede e dispositivos associados. Um programa de software em execução constante, denominado agente, fornece informações aos gerentes por meio de SNMP.

Como ele funciona na prática?

Existem três componentes principais de uma rede gerenciada por protocolo SNMP:

- Roteadores
- Servidores
- Switches

Agentes de software e um sistema de gerenciamento de rede — pode haver mais de um sistema de gerenciamento em uma determinada rede gerenciada. Aqui está um pouco mais de detalhes sobre os 3 componentes do SNMP:

Como ele funciona na prática?

- sistema de gerenciamento de SNMP: é um sistema centralizado de [monitoramento da rede](#). Também é conhecido como Network Management Station (NMS);
- agente SNMP: é um módulo de software de gerenciamento de software instalado em um dispositivo gerenciado. Dispositivos gerenciados podem ser dispositivos de rede como PC, roteador, switches, servidores etc.;
- base de informações de gerenciamento: consiste em informações sobre os recursos que devem ser gerenciados. Essas informações são organizadas hierarquicamente.

O que pode ser configurado ou monitorado via SNMP?

- fornece habilidades de leitura/gravação — por exemplo, você pode usá-lo para redefinir senhas remotamente ou reconfigurar endereços IP;
- coleta informações sobre quanta largura de banda está sendo usada;
- coleta [relatórios](#) de erros em um log, útil para solucionar problemas e identificar tendências;
- envia um alerta por e-mail quando o servidor estiver com pouco espaço em disco;
- monitora o uso de CPU e memória de seus servidores, e alerta quando os limites forem excedidos;
- pode realizar polling ativo, ou seja, a estação de monitoramento pede o status dos dispositivos a cada poucos minutos;
- os dispositivos podem enviar alertas para uma estação de monitoramento em condições de erro.

Como extrair o melhor do protocolo SNMP?

- O SNMP reúne todos os dados de muitos dispositivos e permite colocar esses dados em contexto, o que, por sua vez, possibilita o rastreamento de problemas e a tomada de decisões com base em dados reais (Gerenciamento de rede).
- E é por isso que os administradores de sistemas lucrarão com o uso de SNMP para monitorar redes.