CURSO SUPERIOR DE ADS

SNMP – Gerenciamento de Redes

Prof. Fernando Marlon Soares Figueiredo

Disciplina: Fundamentos de Redes de Computadores

SECTRAS

ADS

Introdução Ao Gerenciamento De Redes

Por que o gerenciamento de redes é importante?

As redes de computadores são formadas por diversos dispositivos interconectados, como **roteadores**, **switches**, **servidores**, **access points** e computadores. Em ambientes corporativos, educacionais e industriais, esses dispositivos precisam operar de forma contínua, segura e eficiente.

Com o crescimento das redes e o aumento da quantidade de equipamentos conectados, tornou-se necessário utilizar mecanismos capazes de monitorar, controlar e administrar toda a infraestrutura de rede.

Introdução Ao Gerenciamento De Redes

O gerenciamento de redes permite:

- Monitorar o funcionamento dos dispositivos
- Detectar falhas e problemas de desempenho
- Controlar configurações e serviços da rede
- Coletar informações sobre tráfego e utilização
- Garantir disponibilidade e estabilidade da infraestrutura

Sem um sistema de gerenciamento adequado, identificar falhas ou analisar o comportamento da rede torna-se uma tarefa complexa, demorada e sujeita a erros.

Nesse contexto, surgem protocolos e ferramentas específicas voltadas para o gerenciamento de redes, sendo o **SNMP (Simple Network Management Protocol)** um dos principais padrões utilizados atualmente.

SNMP – Simple Network Management Protocol

O **SNMP (Simple Network Management Protocol)** é um protocolo utilizado para monitoramento e gerenciamento de dispositivos em redes de computadores. Seu principal objetivo é permitir que administradores acompanhem o funcionamento da infraestrutura de rede de forma centralizada e padronizada.

Esse protocolo possibilita a coleta de informações sobre dispositivos conectados à rede, como roteadores, switches, servidores, impressoras, access points e até equipamentos de Internet das Coisas (IoT).

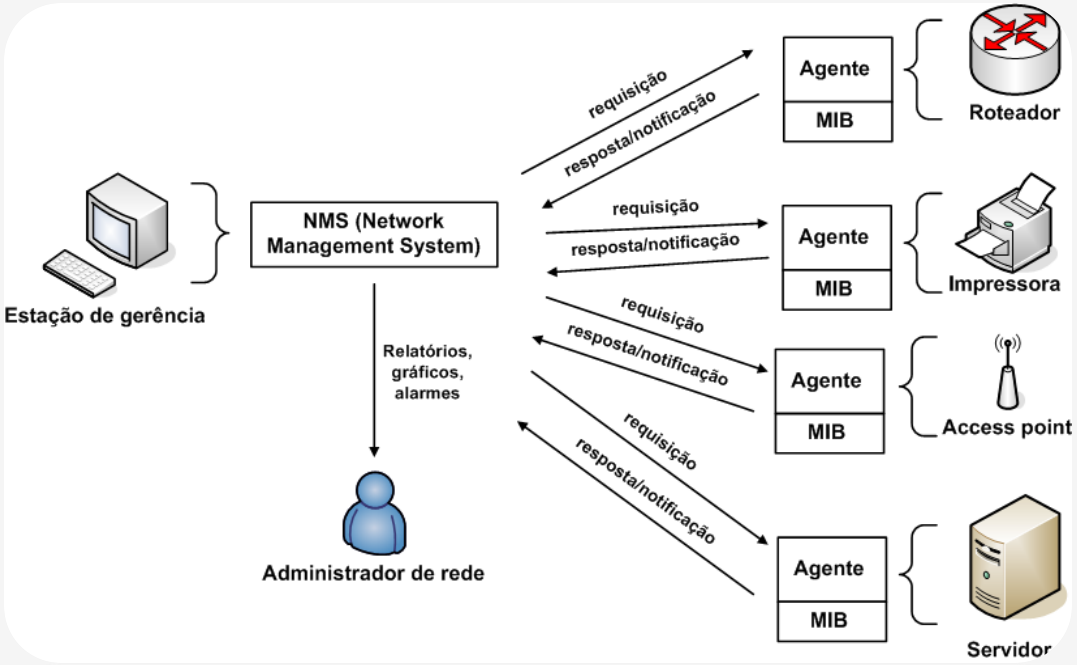
SNMP – Simple Network Management Protocol

Por meio do SNMP, é possível:

- Monitorar o desempenho da rede em tempo real
- Verificar o estado de funcionamento dos dispositivos
- Detectar falhas e indisponibilidades
- Coletar estatísticas de tráfego e utilização
- Automatizar tarefas de gerenciamento

O SNMP opera seguindo um modelo de comunicação entre gerentes e agentes:

- O **gerente (manager)** é responsável por monitorar e solicitar informações
- O **agente (agent)** é executado nos dispositivos da rede e responde às solicitações

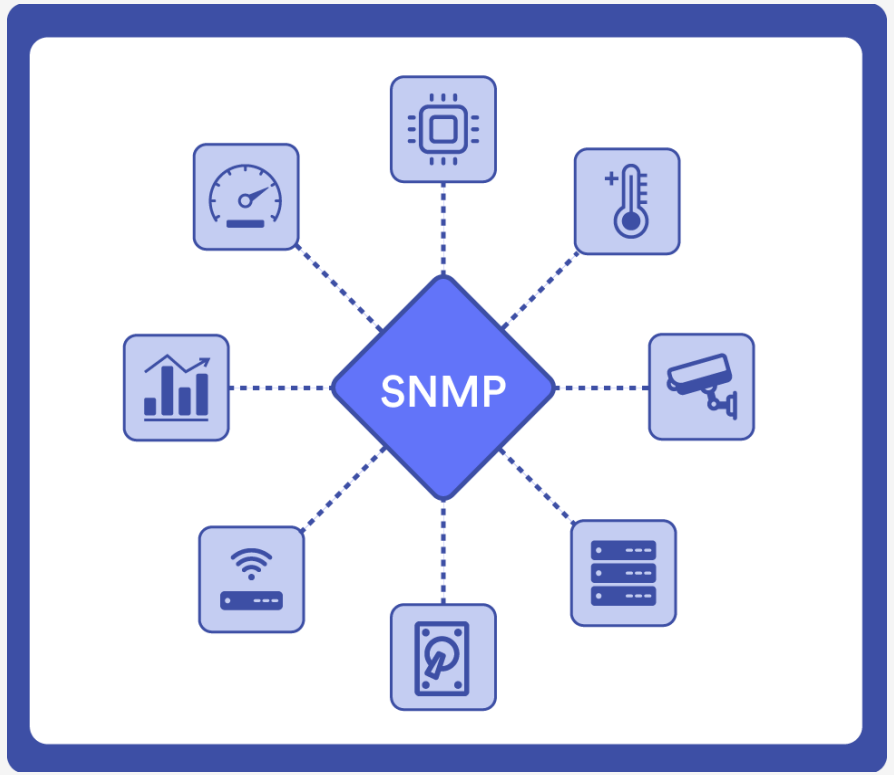


Arquitetura e funcionamento do SNMP

O funcionamento do SNMP baseia-se em uma arquitetura simples composta por dispositivos gerenciados, agentes e um sistema central de gerenciamento. Essa estrutura permite monitorar e controlar diversos equipamentos de rede de forma centralizada.

São os equipamentos monitorados pelo protocolo SNMP, como:

- Roteadores
- Switches
- Servidores
- Impressoras de rede
- Access points



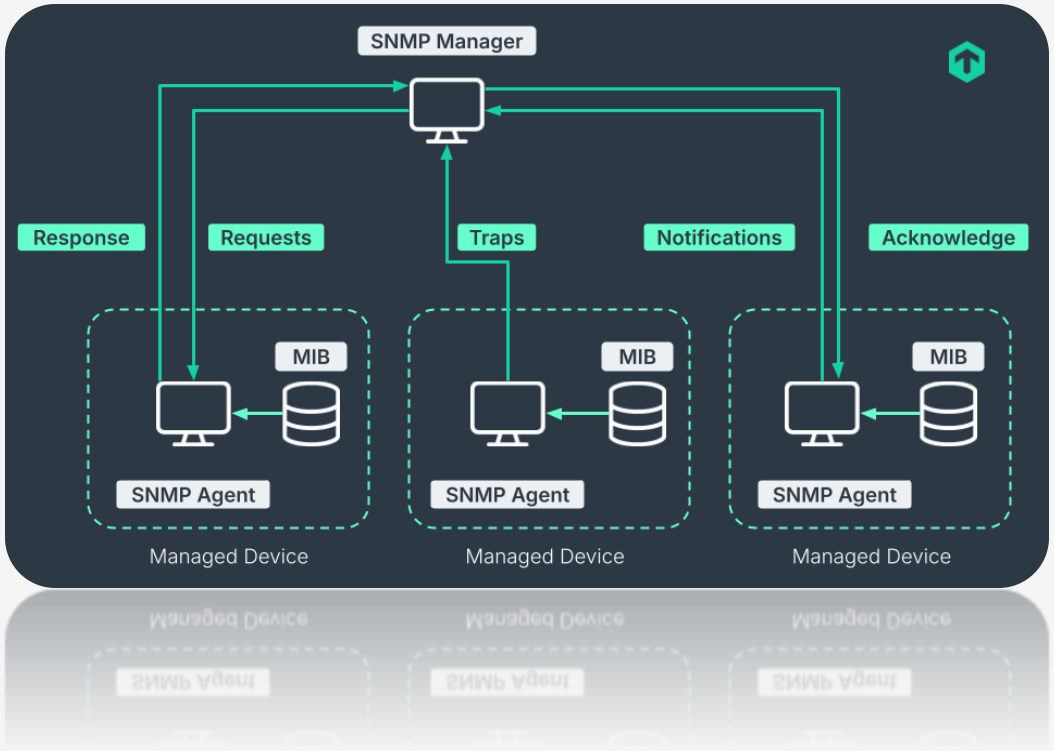
Arquitetura e funcionamento do SNMP

Gerente (SNMP Manager)

É o sistema responsável pelo monitoramento da rede. O gerente realiza consultas, coleta informações e recebe notificações dos dispositivos gerenciados.

Normalmente, o gerente está presente em softwares de monitoramento de rede, como:

- Zabbix
- PRTG
- SolarWinds
- Nagios



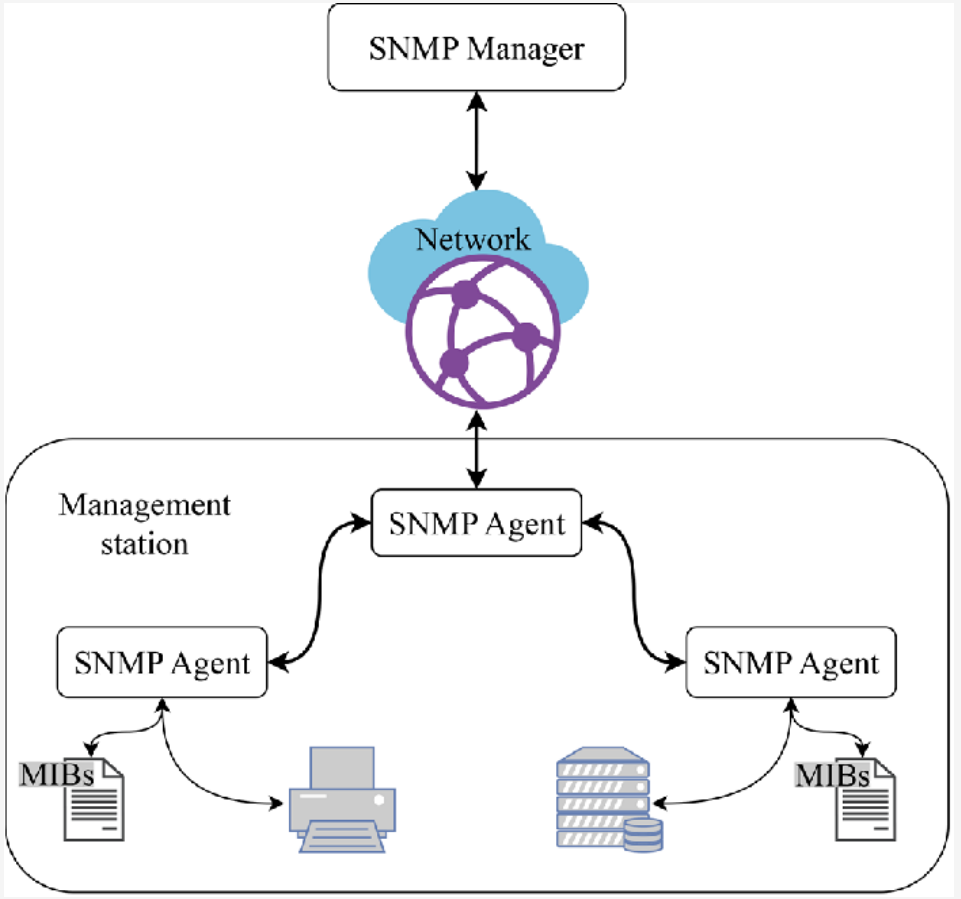
Arquitetura e funcionamento do SNMP

Agente (SNMP Agent)

O agente é um software executado no dispositivo gerenciado. Sua função é coletar informações locais do equipamento e responder às solicitações feitas pelo gerente.

Os agentes podem fornecer informações como:

- Uso de CPU
- Consumo de memória
- Estado das interfaces de rede
- Quantidade de tráfego transmitido



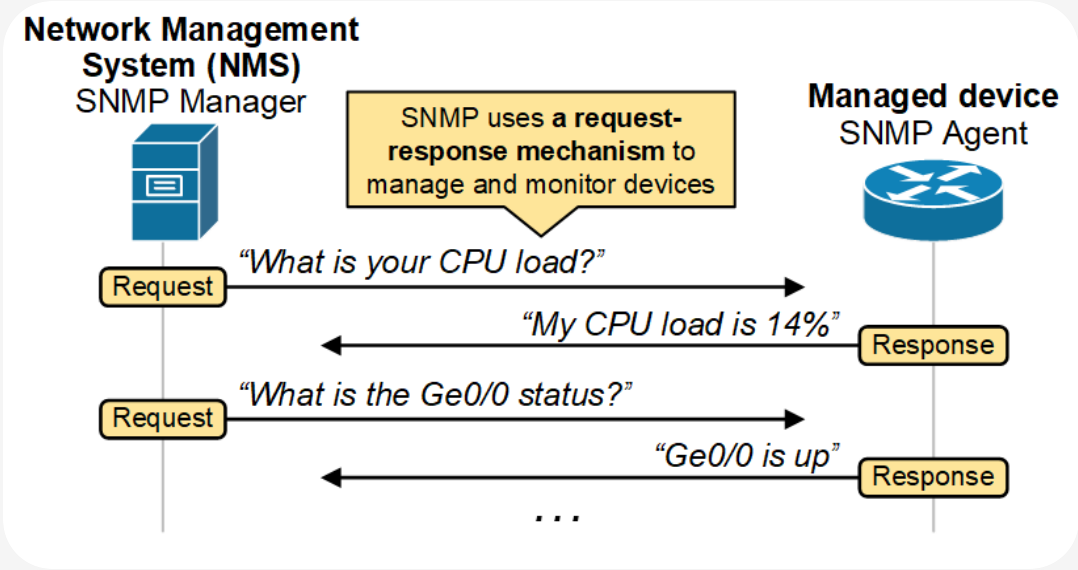
Funcionamento Da Comunicação No SNMP

A comunicação no SNMP acontece entre o gerente e os agentes instalados nos dispositivos da rede. O gerente envia solicitações para coletar informações ou alterar configurações, enquanto os agentes respondem com os dados solicitados.

Esse modelo permite que o administrador acompanhe o comportamento da rede de forma centralizada e em tempo real.

O funcionamento básico ocorre da seguinte maneira:

1. O gerente envia uma solicitação ao agente
2. O agente consulta as informações do dispositivo
3. O agente responde ao gerente com os dados coletados
4. O gerente interpreta e apresenta as informações ao administrador



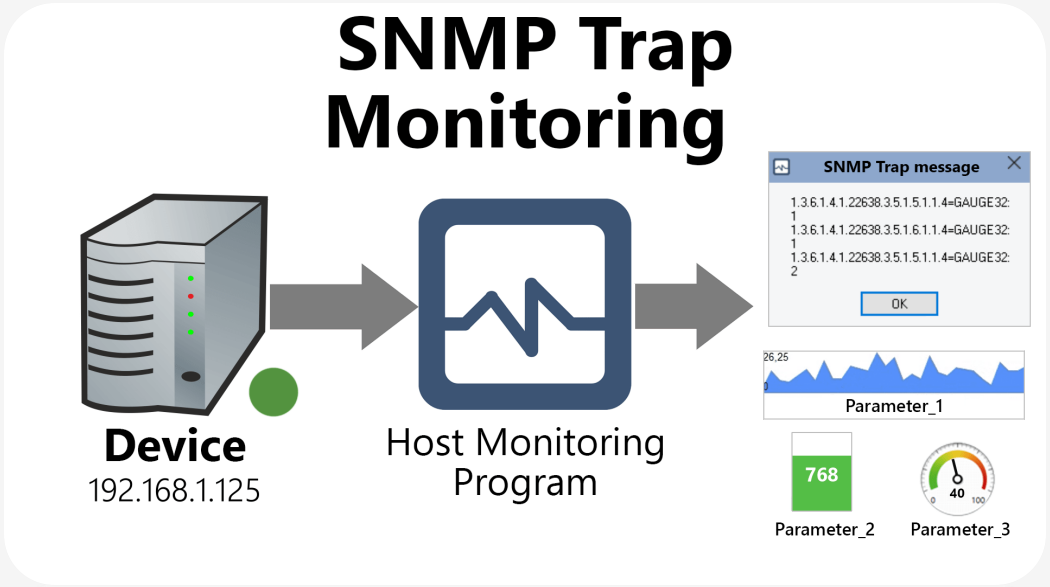
Funcionamento Da Comunicação No SNMP

Além das respostas às consultas, os agentes também podem enviar notificações automáticas quando algum evento importante ocorre na rede, como:

- Falha em interfaces
- Queda de dispositivos
- Sobrecarga de processamento
- Alterações críticas no sistema

Essas notificações são conhecidas como **traps**, permitindo que problemas sejam identificados rapidamente sem a necessidade de consultas constantes.

A comunicação SNMP normalmente utiliza o protocolo UDP, devido à sua leveza e baixo consumo de recursos, tornando o monitoramento mais eficiente em grandes redes.



MIB e OID: organização das informações no SNMP

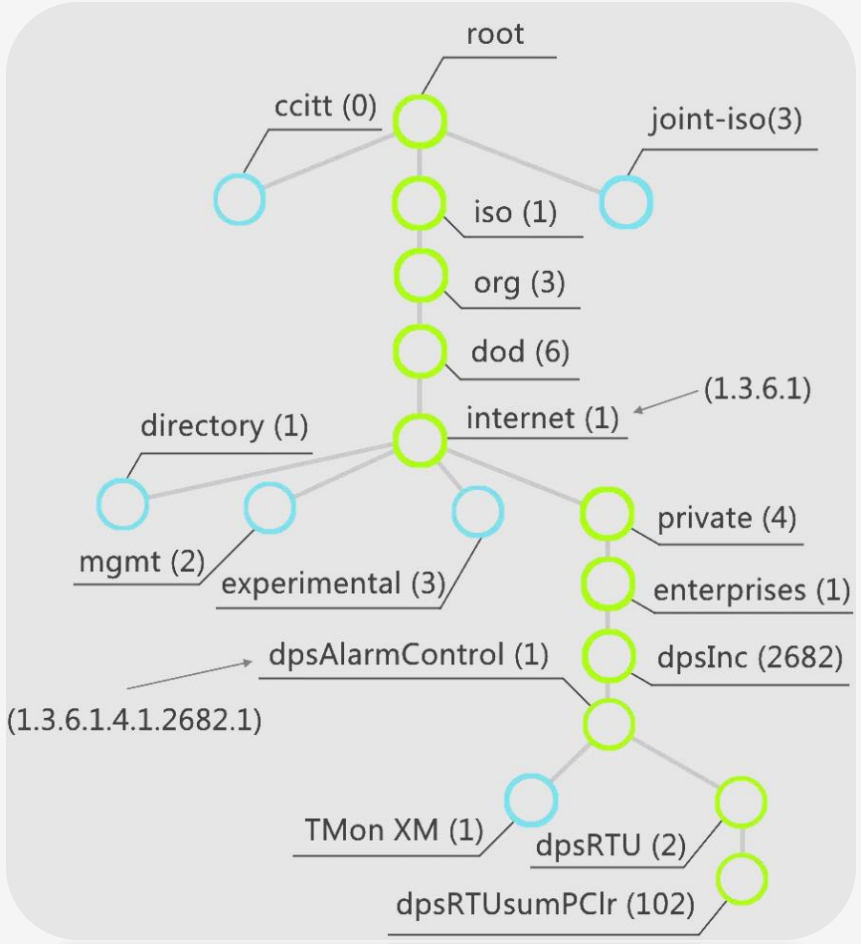
Para que o gerente consiga interpretar corretamente os dados fornecidos pelos dispositivos da rede, o SNMP utiliza estruturas padronizadas de organização das informações. As principais são a **MIB (Management Information Base)** e os **OID (Object Identifiers)**.

MIB – Management Information Base

A MIB pode ser entendida como uma base de informações organizada de forma hierárquica. Ela funciona como um "banco de objetos" contendo os dados que podem ser monitorados em um dispositivo.

Cada equipamento possui informações específicas armazenadas em sua MIB, como:

- Nome do dispositivo
- Tempo de atividade (uptime)
- Uso de CPU e memória
- Estado das interfaces de rede
- Quantidade de pacotes transmitidos



MIB e OID: organização das informações no SNMP

OID – Object Identifier

Os OIDs são identificadores únicos utilizados para localizar informações dentro da MIB. Cada objeto monitorado possui um endereço numérico específico.

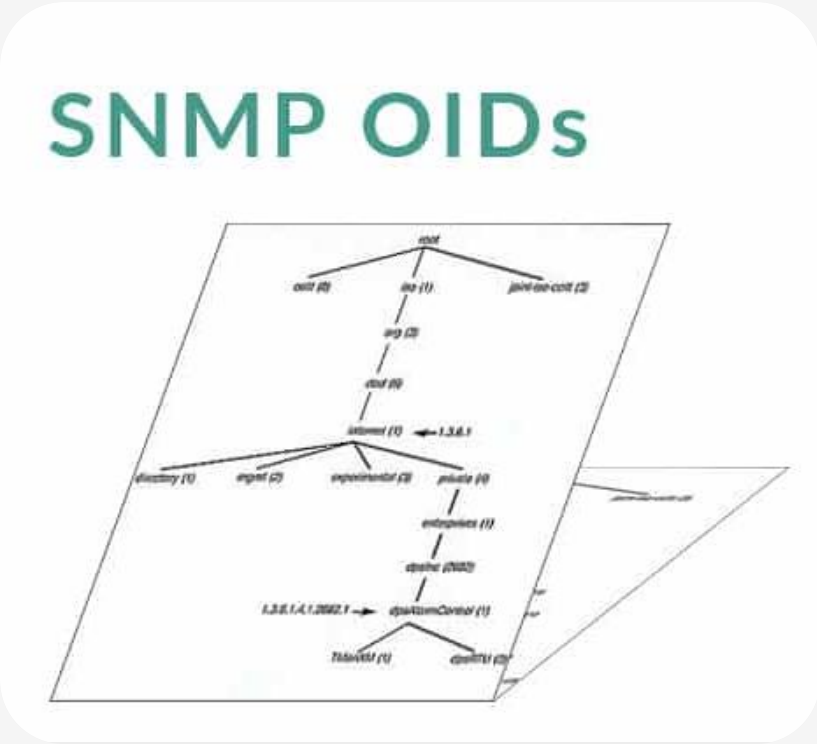
Exemplo de OID:

1.3.6.1.2.1.1.5

Esse identificador pode representar o nome de um dispositivo dentro da estrutura SNMP.

A estrutura hierárquica dos OIDs funciona como uma árvore organizada, permitindo que o gerente encontre exatamente a informação desejada dentro do dispositivo monitorado.

Sem a utilização de MIBs e OIDs, o SNMP não conseguiria padronizar a comunicação entre diferentes fabricantes e equipamentos de rede.



Tipos de mensagens utilizadas no SNMP

A comunicação entre gerente e agente no protocolo SNMP ocorre por meio de mensagens específicas, responsáveis por solicitar informações, enviar respostas ou notificar eventos da rede.

Cada tipo de mensagem possui uma função diferente dentro do processo de gerenciamento.

GET

A mensagem GET é utilizada pelo gerente para solicitar informações ao agente.

Exemplos:

- Verificar o uso de CPU de um roteador
- Consultar o estado de uma interface de rede
- Obter o tempo de atividade de um servidor

Tipos de mensagens utilizadas no SNMP

GET-NEXT

Permite ao gerente navegar sequencialmente pelos objetos da MIB, acessando o próximo item disponível na estrutura hierárquica.

Essa operação é muito utilizada para percorrer tabelas e coletar múltiplas informações automaticamente.

SET

Utilizada para alterar configurações em dispositivos gerenciados.

Exemplos:

- Alterar parâmetros de configuração
- Ativar ou desativar interfaces
- Modificar valores administrativos

RESPONSE

Mensagem enviada pelo agente como resposta às solicitações realizadas pelo gerente.

Ela contém os dados requisitados ou informações sobre possíveis erros na operação.

Evolução das versões do SNMP

Ao longo do tempo, o protocolo SNMP passou por diferentes versões, cada uma trazendo melhorias relacionadas a desempenho, funcionalidades e principalmente segurança.

As versões mais conhecidas são: **SNMPv1**, **SNMPv2c** e **SNMPv3**.

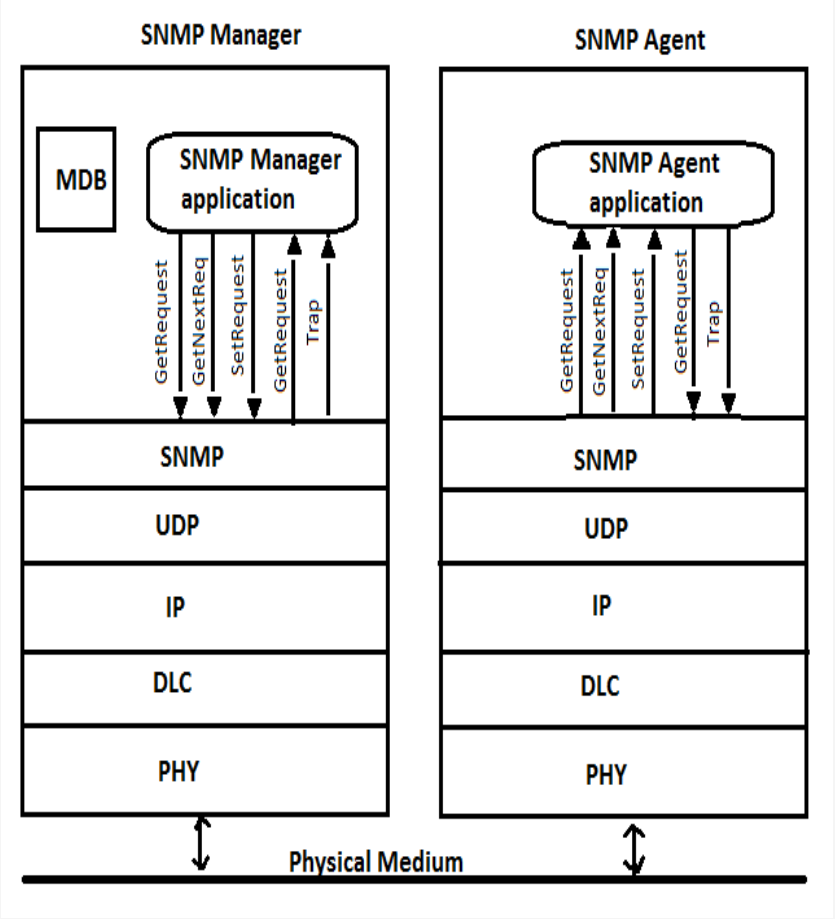
SNMPv1

Foi a primeira versão do protocolo e estabeleceu as bases do gerenciamento de redes utilizando o modelo gerente-agente.

Principais características:

- Simplicidade de implementação
- Baixo consumo de recursos
- Comunicação baseada em community strings
- Ausência de mecanismos avançados de segurança

Apesar de sua importância histórica, o SNMPv1 possui limitações significativas relacionadas à proteção das informações transmitidas.



Evolução das versões do SNMP

SNMPv2c

O SNMPv2 trouxe melhorias de desempenho e novas operações de gerenciamento, tornando a comunicação mais eficiente.

Principais melhorias:

- Transferência de dados mais eficiente
- Melhor tratamento de erros
- Inclusão de novas operações de consulta
- Maior desempenho no monitoramento

Entretanto, o modelo de segurança ainda continuava limitado, utilizando community strings semelhantes às da versão anterior.

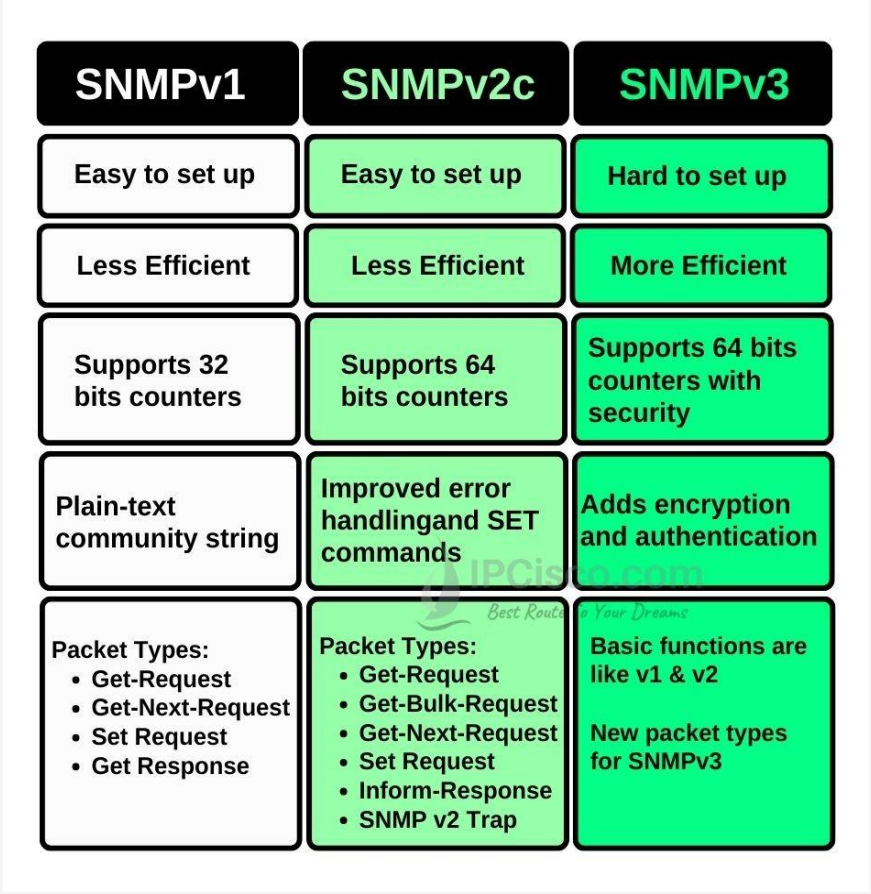
SNMPv3

O SNMPv3 foi desenvolvido com foco em segurança, tornando-se a versão mais recomendada para ambientes corporativos modernos.

Principais recursos:

- Autenticação de usuários
- Controle de acesso
- Criptografia das mensagens
- Integridade e confidencialidade dos dados

Essa versão reduz significativamente os riscos de interceptação e acesso não autorizado às informações da rede.



Segurança No SNMP

Como o SNMP é responsável por acessar informações importantes dos dispositivos da rede, questões relacionadas à segurança tornam-se fundamentais. Um gerenciamento inadequado pode expor dados sensíveis e permitir acessos não autorizados à infraestrutura.

As primeiras versões do protocolo apresentavam limitações significativas em relação à proteção das informações transmitidas.

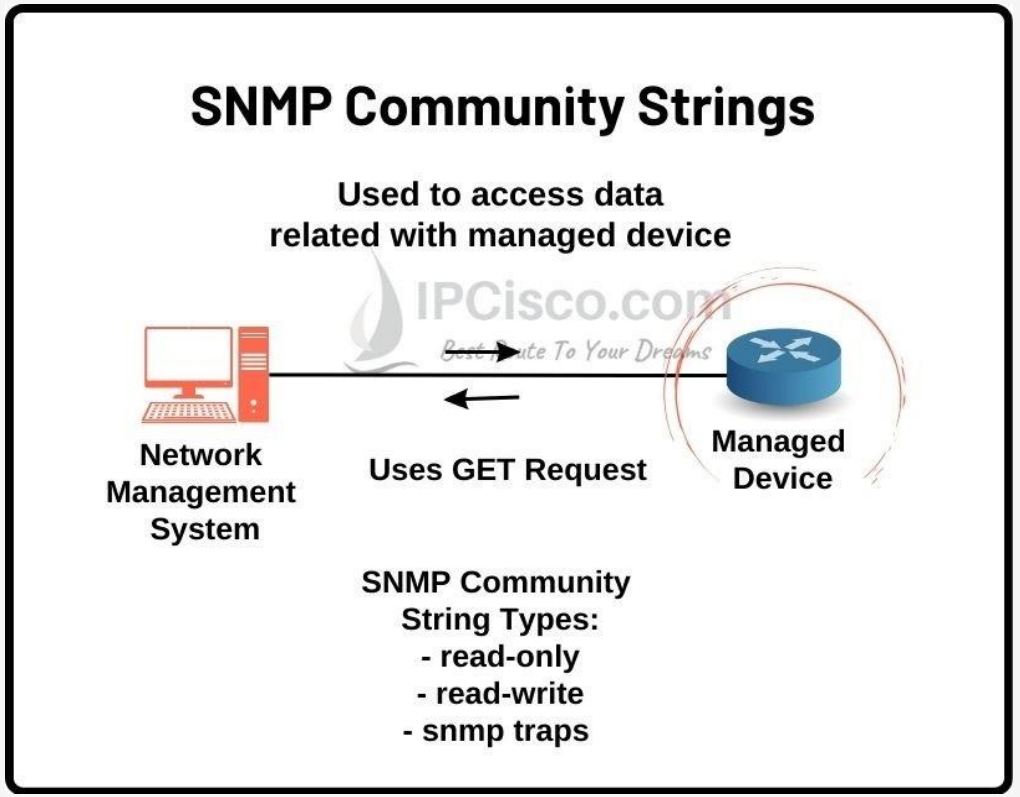
Community Strings

Nas versões SNMPv1 e SNMPv2c, o controle de acesso é realizado por meio das chamadas community strings, que funcionam como senhas utilizadas na comunicação entre gerente e agente.

Os tipos mais comuns são:

- **Read-Only (RO):** permite apenas leitura das informações
- **Read-Write (RW):** permite leitura e alteração de configurações

Entretanto, essas informações são transmitidas sem criptografia, o que representa um grande risco de segurança, principalmente em redes expostas ou mal segmentadas.



Segurança No SNMP

Principais riscos de segurança

O uso inadequado do SNMP pode permitir:

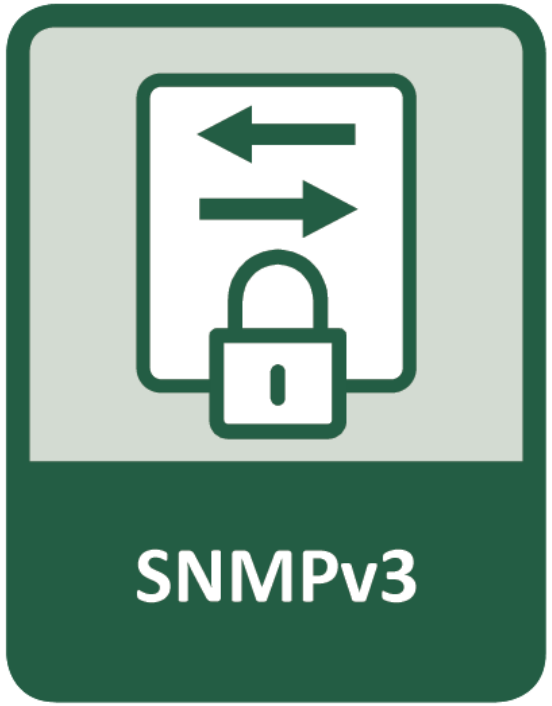
- Interceptação de dados da rede
- Descoberta de informações sensíveis dos dispositivos
- Alteração não autorizada de configurações
- Monitoramento indevido da infraestrutura

SNMPv3 e proteção avançada

O SNMPv3 foi criado para solucionar essas limitações, introduzindo mecanismos de segurança mais robustos, como:

- Autenticação de usuários
- Criptografia das mensagens
- Controle de acesso baseado em permissões
- Garantia de integridade dos dados transmitidos

Por esse motivo, ambientes corporativos modernos recomendam a utilização do SNMPv3 sempre que possível, reduzindo riscos e aumentando a proteção da rede.



Portas E Transporte No SNMP

O protocolo SNMP utiliza o modelo cliente-servidor baseado na comunicação entre gerente e agente. Para realizar essa troca de informações, o protocolo normalmente opera sobre o **UDP (User Datagram Protocol)**.

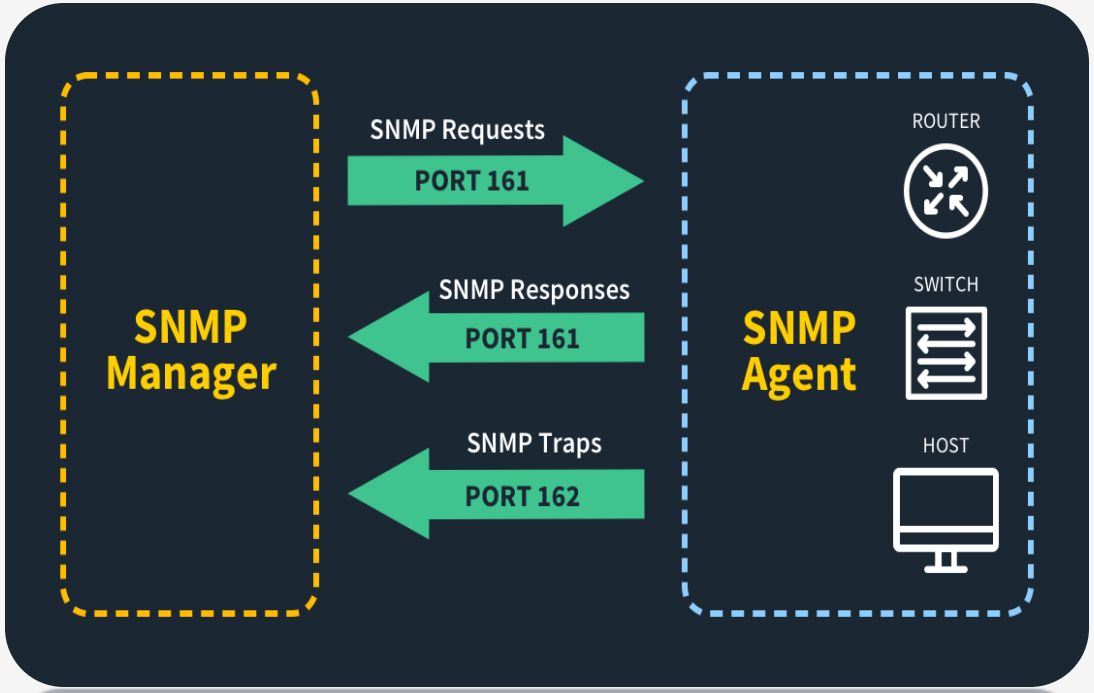
O UDP foi escolhido por ser um protocolo leve, rápido e com baixo consumo de recursos, características importantes em ambientes de monitoramento contínuo.

Uso do protocolo UDP

Diferente do TCP, o UDP não estabelece conexão antes da transmissão dos dados. Isso reduz o overhead da comunicação e torna o monitoramento mais eficiente, principalmente em grandes redes.

As principais vantagens do uso do UDP no SNMP incluem:

- Menor consumo de largura de banda
- Comunicação mais rápida
- Redução de processamento nos dispositivos
- Maior eficiência em consultas frequentes



Portas E Transporte No SNMP

Portas padrão do SNMP

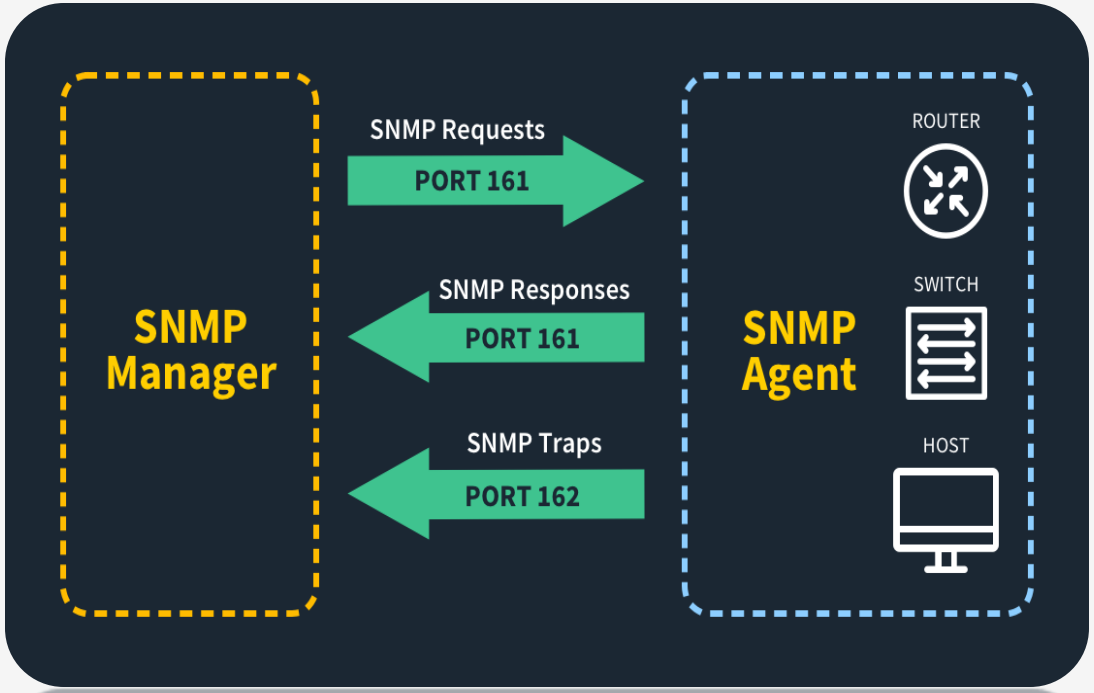
O protocolo utiliza duas portas principais:

- **Porta UDP 161:** utilizada para consultas e respostas entre gerente e agente
- **Porta UDP 162:** utilizada para envio de traps e notificações automáticas

Na prática:

- O gerente envia requisições pela porta 161
- O agente responde utilizando a mesma porta
- As traps são enviadas automaticamente para a porta 162 do gerente

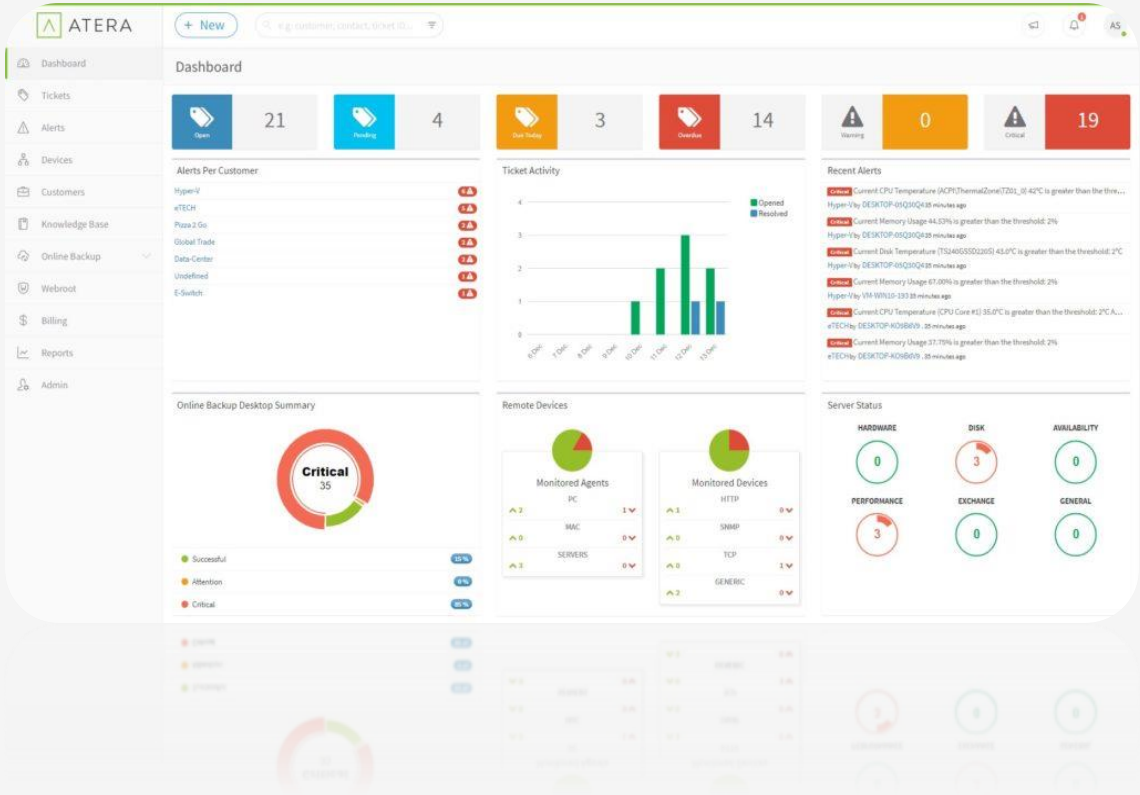
Embora o UDP ofereça maior desempenho, ele não possui mecanismos próprios de confiabilidade, tornando importante o uso de boas práticas de monitoramento e segurança na rede.



Ferramentas De Monitoramento Utilizando SNMP

O protocolo SNMP é amplamente utilizado por ferramentas de monitoramento e gerenciamento de redes. Esses sistemas permitem acompanhar o funcionamento da infraestrutura em tempo real, coletando informações de diversos dispositivos conectados à rede.

Por meio dessas ferramentas, administradores conseguem visualizar métricas, identificar falhas, gerar alertas e analisar o desempenho da rede de forma centralizada.



Principais funcionalidades dessas ferramentas

- Monitoramento contínuo de dispositivos
- Coleta automática de métricas da rede
- Geração de gráficos e relatórios
- Detecção de falhas e indisponibilidades
- Emissão de alertas em tempo real
- Controle e análise de desempenho da infraestrutura

Ferramentas De Monitoramento Utilizando SNMP

Exemplos de ferramentas que utilizam SNMP

- **Zabbix**
  - Plataforma de monitoramento open source bastante utilizada em ambientes corporativos para acompanhar servidores, redes e serviços.
- **PRTG Network Monitor**
  - Ferramenta voltada para monitoramento de redes e dispositivos, conhecida pela interface intuitiva e facilidade de configuração.
- **Nagios**
  - Sistema de monitoramento amplamente utilizado para supervisão de servidores, dispositivos de rede e serviços críticos.
- **SolarWinds**
  - Solução corporativa focada em gerenciamento avançado de redes, desempenho e análise de infraestrutura.

Vantagens E Limitações Do SNMP

Principais vantagens do SNMP

- **Padronização**
  - O protocolo é amplamente adotado por diferentes fabricantes, permitindo monitorar equipamentos distintos dentro da mesma infraestrutura.
- **Baixo consumo de recursos**
  - O SNMP utiliza comunicação leve baseada em UDP, reduzindo o impacto no desempenho da rede e dos dispositivos monitorados.
- **Facilidade de implementação**
  - Grande parte dos equipamentos de rede já possui suporte nativo ao protocolo.
- **Monitoramento centralizado**
  - Permite acompanhar diversos dispositivos a partir de uma única ferramenta de gerenciamento.
- **Automação de alertas**
  - Falhas e eventos importantes podem ser identificados rapidamente por meio das traps.

Vantagens E Limitações Do SNMP

Principais limitações do SNMP

- **Problemas de segurança nas versões antigas**
  - SNMPv1 e SNMPv2c utilizam mecanismos simples de autenticação, sem criptografia das mensagens.
- **Dependência de configuração adequada**
  - Configurações incorretas podem expor informações sensíveis da infraestrutura.
- **Limitações em ambientes muito complexos**
  - Grandes volumes de consultas podem gerar aumento de tráfego e sobrecarga em determinados cenários.
- **Informações limitadas em alguns dispositivos**
  - Nem todos os fabricantes disponibilizam o mesmo nível de detalhamento nas MIBs.