



# SNMP

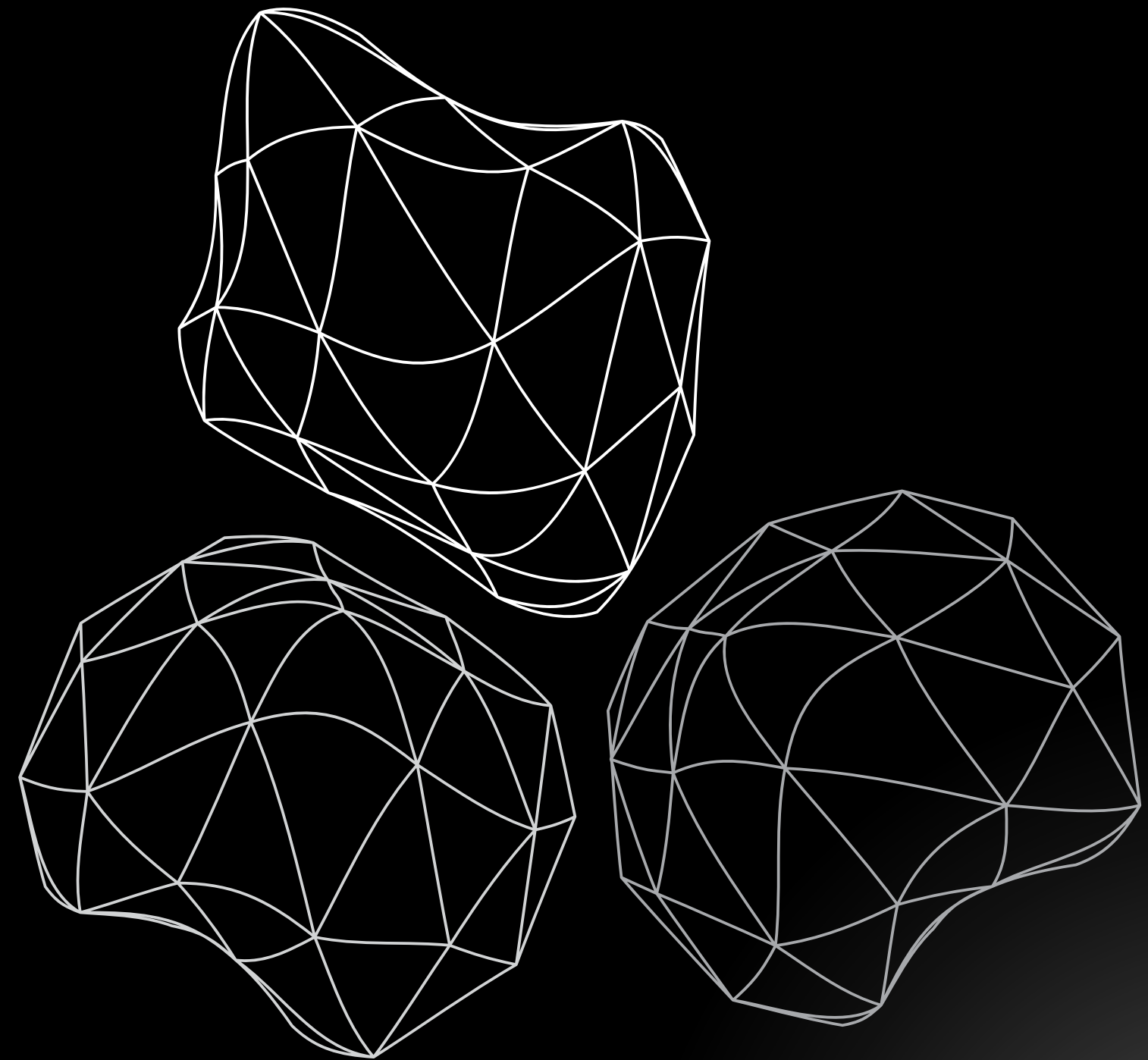
SIMPLE NETWORK MANAGEMENT PROTOCOL

MAIARA TORRES  
MARIA VITÓRIA PAIVA  
VICTOR SANTOS  
VINÍCIUS CAVALCANTE  
ZHIHANG LIN

# O QUE É O SNMP?

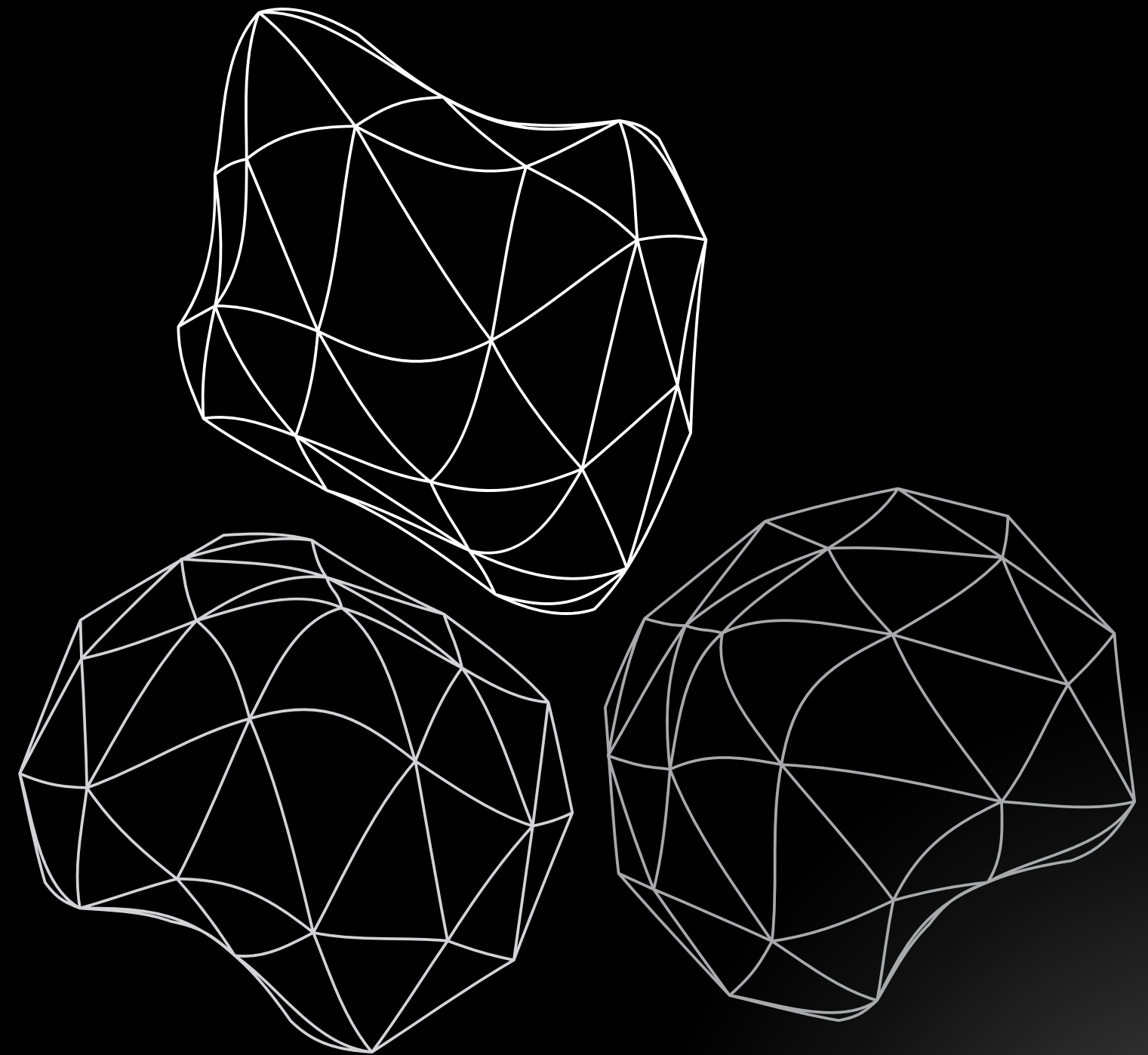
## PROTOCOLO DE MONITORAMENTO IP

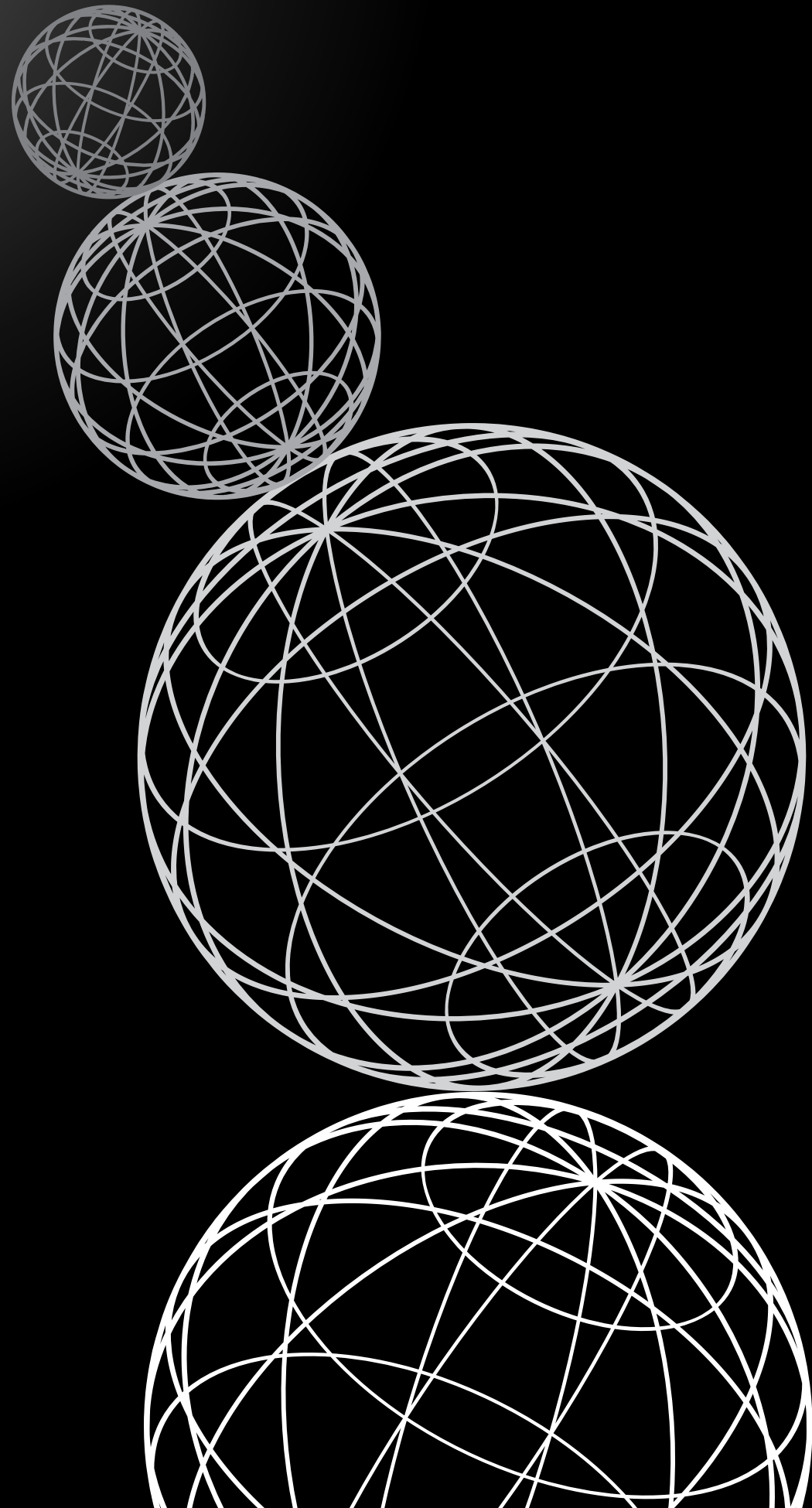
- Monitorar e controlar dispositivos de rede, como roteadores, switches, servidores...
- Permite a comunicação entre dispositivos de uma rede para fins monitoramento de status, coleta de informações e configuração de parâmetros.



# O QUE PODE SER MONITORADO?

- Quantidade de Processos
- Estatísticas de Tráfego
- Uso de Memória





# COMO FUNCIONA O SNMP?

- Gerente
- Agente
- Dispositivos Gerenciados
- MIB




# GERENTE

- É o cliente no modelo SNMP
- É geralmente um software ou sistema central usado para gerenciar e monitorar dispositivos da rede
- Exemplos de softwares SNMP incluem o Zabbix, Nagios e SolarWinds
- Ele coleta informações dos dispositivos gerenciados e pode enviar comandos para eles



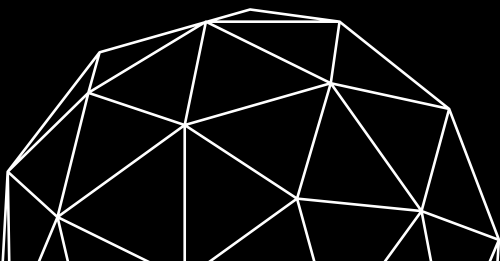
# AGENTE

- É o servidor SNMP que roda em cada dispositivo gerenciado
  - O agente é responsável por coletar as informações locais do dispositivo (por exemplo, uso da CPU, tráfego de rede, etc.) e disponibilizá-las ao gerente SNMP
- 



# DISPOSITIVOS GERENCIADOS

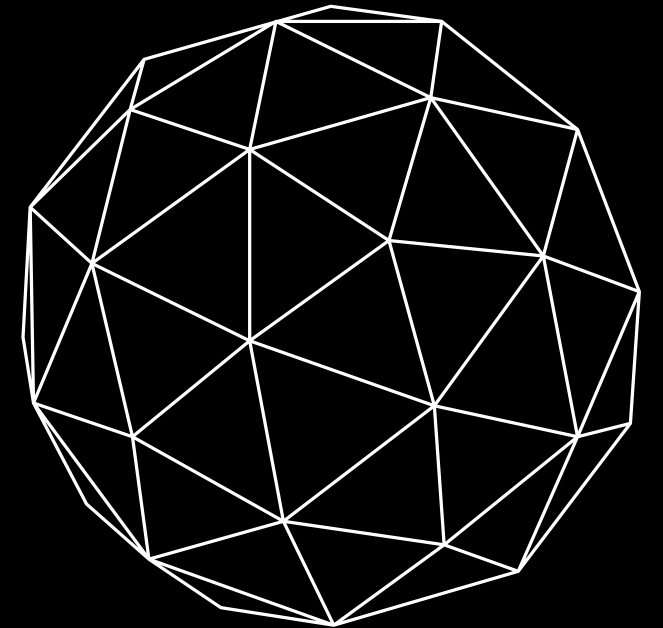


- São os dispositivos que possuem agentes SNMP instalados, como roteadores, switches, servidores, impressoras, entre outros.
- 

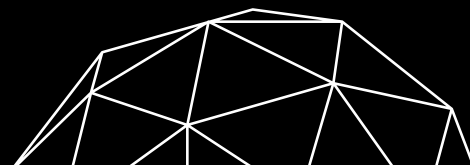


# MIBS

(Base de Informações Gerenciais)

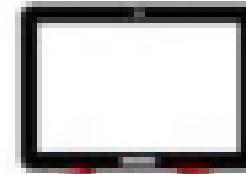


- É a “base de dados” do dispositivo gerenciado
- Contém informações em uma estrutura hierárquica que descreve as variáveis que podem ser acessadas/alteradas no dispositivo
- Por exemplo, você pode acessar informações como:
  - Uso de CPU
  - Espaço em disco
  - Estado das portas de um switch

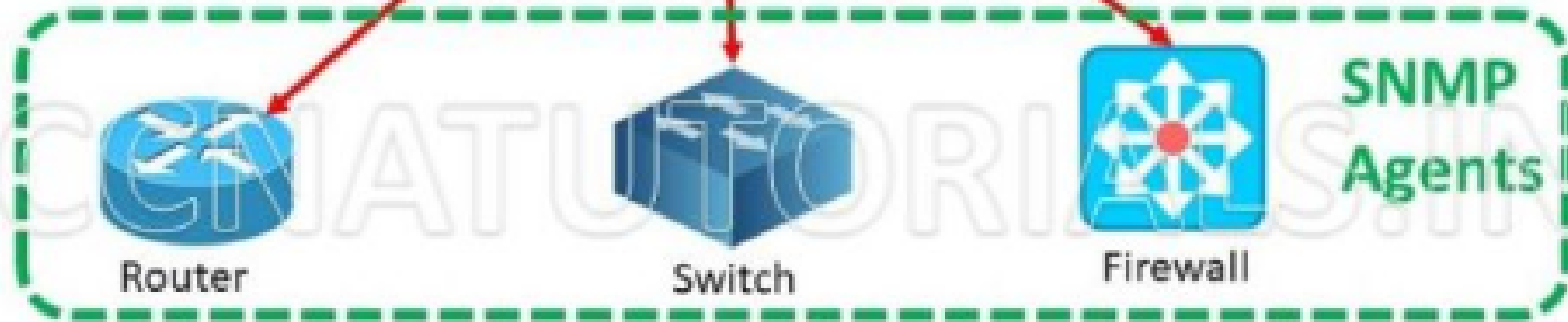




SNMP Manager



ccnatutorials.in



SNMP Simple Network Management Protocol



# COMANDOS BÁSICOS



GET: Recuperar informações de um dispositivo de rede

SET: Modificar a configuração de um dispositivo de rede

TRAPS: Notificações para alertar sobre eventos específicos





# VERSÕES DO SNMP



SNMPv1

SNMPv2c

SNMPv3





# SNMPV1

1980



- **Arquitetura simples:**

Modelo simples de cliente-servidor, onde o gestor consulta ou modifica dados em dispositivos de rede por meio de agentes SNMP instalados nesses dispositivos.

- **Operações básicas:**

Get, set e trap.

- **Segurança limitada:**

Conta apenas com senhas simples, sem criptografia.





# SNMPV1


1980

- **Uso de UDP:**

SNMPv1 opera sobre o protocolo UDP, utilizando a porta 161 para consultas e a 162 para traps. Isso o torna mais leve e rápido, porém pode causar perda de pacotes.

- **Estrutura MIB:**

Utilizada para organizar e estruturar as informações gerenciáveis. A MIB define variáveis que representam propriedades dos dispositivos de rede e permite a consulta e o controle desses parâmetros.







# SNMPV2C

1996

- **Arquitetura aprimorada:**

Baseado no modelo cliente-servidor com maior eficiência e novas funcionalidades.

- **Operações estendidas:**

Inclui operações GET, SET, GETNEXT, GETBULK e INFORM, otimizando a coleta de dados em massa.

- **Segurança limitada:**

Ainda utiliza “Community Strings” (ex.: “public”), sem autenticação ou criptografia robusta.





# SNMPV2C

1996

- **Uso de UDP:**

Similar ao v1, utiliza portas 161 (consultas) e 162 (traps), mantendo rapidez, mas com possíveis perdas de pacotes.

- **Estrutura MIB:**

Expansão das variáveis e tipos de dados (BitString, Counter64 e etc...) para maior flexibilidade no gerenciamento de dispositivos.





# SNMPV3

2002



- **Arquitetura aprimorada:**

Introduz autenticação, criptografia e controle de acesso, garantindo a proteção dos dados.

- **Principais funcionalidades:**

- Privacidade: Criptografia para proteger a comunicação.
  - Autenticação: Garante que a origem dos dados seja confiável.
  - Controle de Acesso: Define permissões específicas para cada usuário.
- 



# SNMPV3

2002



- **Uso de UDP:**

Opera nas portas 161 para consultas e 162 para traps, com foco em segurança e confiabilidade.

- **Estrutura MIB:**

Utiliza a estrutura de MIB das versões anteriores, com melhorias para suportar segurança avançada.





# VANTAGENS




## • SNMPv1

1. Simplicidade na implementação e uso.
2. Compatibilidade com a maioria dos dispositivos de rede, mesmo os mais antigos.

## • SNMPv2c

1. Introdução do comando **GETBULK**, permitindo a coleta eficiente de grandes volumes de dados.
2. Maior eficiência e suporte a novos tipos de dados e operações.

## • SNMPv3

1. Segurança robusta com suporte a autenticação e criptografia.
  2. Maior confiabilidade e proteção em ambientes sensíveis.
- 





# DESVANTAGENS




## • SNMPv1

1. Segurança muito limitada, com uso de “Community Strings” simples e sem criptografia.
2. Ineficiência no gerenciamento de grandes volumes de dados.

## • SNMPv2c

1. Segurança ainda baseada em “Community Strings”, sem criptografia ou autenticação robusta.
2. Problemas de interoperabilidade com o SNMPv1 em alguns casos.

## • SNMPv3

1. Maior complexidade de configuração e implementação.
  2. Pode exigir mais recursos computacionais nos dispositivos gerenciados.
- 

# ALGUNS SOFTWARES QUE UTILIZAM O SNMP



**PTRG**

**ZABBIX**

**ManageEngine  
OpManager**



**Datadog**

**Nagios**



**PRÁTICA**

**OBRIGADO!**