INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Mestrado em Engenharia de Segurança Informática
Análise de Comunicações em Rede

Relatório sobre SNMP

Martinho José Novo Caeiro - 23917
Paulo António Tavares Abade - 23919

Beja, janeiro de 2026

INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Mestrado em Engenharia de Segurança Informática
Análise de Comunicações em Rede

Relatório sobre SNMP

Martinho José Novo Caeiro - 23917
Paulo António Tavares Abade - 23919

Orientador: Daniel José Da Graça Peceguinha Franco

Beja, janeiro de 2026

Resumo

Este relatório apresenta um estudo detalhado sobre o protocolo SNMP (*Simple Network Management Protocol*), um protocolo fundamental para a gestão e monitorização de dispositivos de rede. O trabalho aborda a evolução histórica do protocolo, desde a sua criação nos anos 80 até às versões mais recentes, explorando a arquitetura, componentes e funcionamento do SNMP. São analisadas em detalhe as três principais versões do protocolo – SNMPv1, SNMPv2 e SNMPv3 – comparando as suas características técnicas, mecanismos de segurança, vantagens e limitações. Particular ênfase é dada à evolução dos mecanismos de segurança, desde a autenticação baseada em comunidades simples nas versões iniciais até aos robustos mecanismos criptográficos da versão 3. O relatório também discute os principais desafios na implementação do protocolo e as suas aplicações práticas em ambientes empresariais modernos. Este relatório foi realizado no âmbito da unidade curricular de Análise de Comunicações em Rede, do Mestrado em Engenharia de Segurança Informática (IPBeja, 2026), e o modelo LaTeX está disponivel no repositório do Github (Martinho Caeiro & Paulo Abade, 2026).

Palavras-chave: SNMP, gestão de redes, protocolos de rede, segurança de redes, SNMPv1, SNMPv2, SNMPv3

Abstract

This report presents a detailed study of the SNMP (Simple Network Management Protocol), a fundamental protocol for network device management and monitoring. The work addresses the historical evolution of the protocol, from its creation in the 1980s to the most recent versions, exploring the architecture, components, and operation of SNMP. The three main versions of the protocol – SNMPv1, SNMPv2, and SNMPv3 – are analyzed in detail, comparing their technical characteristics, security mechanisms, advantages, and limitations. Particular emphasis is given to the evolution of security mechanisms, from simple community-based authentication in early versions to the robust cryptographic mechanisms of version 3. The report also discusses the main challenges in protocol implementation and its practical applications in modern enterprise environments. This report was carried out within the scope of the Network Communications Analysis course, of the Master's in Computer Security Engineering (IPBeja, 2026), and the LaTeX model is available in the Github repository (Martinho Caeiro & Paulo Abade, 2026).

Keywords: SNMP, network management, network protocols, network security, SNMPv1, SNMPv2, SNMPv3

Índice

Índice de Figuras

1 Introdução

Com o crescimento exponencial das redes de computadores nas últimas décadas, a necessidade de ferramentas eficazes para a gestão e monitorização de dispositivos de rede tornou-se imperativa. O SNMP (*Simple Network Management Protocol*) emergiu como a solução padronizada para responder a esta necessidade, estabelecendo-se como o protocolo de gestão de rede mais amplamente utilizado na atualidade Harrington et al., 2002.

Desenvolvido inicialmente nos finais da década de 1980 como parte da arquitetura de protocolos TCP/IP, o SNMP foi concebido com o objetivo de proporcionar um mecanismo simples e eficiente para a monitorização e controlo de dispositivos de rede, tais como routers, switches, servidores, impressoras e outros equipamentos conectados Stallings, 2007. A simplicidade conceptual do protocolo foi um dos fatores que contribuiu para a sua rápida adoção pela indústria.

Ao longo de mais de três décadas de evolução, o SNMP passou por diversas revisões significativas, resultando em três versões principais: SNMPv1, SNMPv2 e SNMPv3. Cada versão trouxe melhorias em termos de funcionalidade, eficiência e, particularmente importante, segurança. A versão mais recente, SNMPv3, introduziu mecanismos robustos de autenticação e encriptação, respondendo às crescentes preocupações com a segurança das infraestruturas de rede Blumenthal e Wijnen, 2002.

Este relatório tem como objetivo apresentar um estudo aprofundado do protocolo SNMP, explorando a sua arquitetura fundamental, os componentes que o constituem, e o seu funcionamento operacional. Serão analisadas detalhadamente as características técnicas de cada versão, bem como as suas vantagens e limitações. A análise comparativa entre versões permitirá compreender a evolução do protocolo e as razões que motivaram as alterações introduzidas. Por fim, serão discutidos os desafios atuais na implementação e utilização do SNMP em ambientes de rede modernos.

2 Fundamentos do SNMP

2.1 Definição e Propósito

O SNMP (*Simple Network Management Protocol*) é um protocolo da camada de aplicação, definido pela IETF (*Internet Engineering Task Force*), que permite a gestão e monitorização de dispositivos numa rede IP. O protocolo fornece um conjunto padronizado de operações para coletar informações sobre o estado dos dispositivos, modificar configurações e receber notificações sobre eventos significativos Case et al., 1990.

O principal objetivo do SNMP é facilitar a troca de informações de gestão entre dispositivos de rede, permitindo que administradores monitorizem o desempenho da rede, detetem problemas rapidamente e ajustem configurações remotamente. Esta capacidade é essencial em redes de grande dimensão, onde a gestão manual de cada dispositivo seria impraticável.

2.2 Arquitetura do SNMP

A arquitetura do SNMP baseia-se no modelo gestor-agente (*manager-agent*), composto por quatro elementos principais Mauro e Schmidt, 2005:

a) **Gestor SNMP (*Manager*)**: Sistema responsável por comunicar com os agentes SNMP instalados nos dispositivos geridos. O gestor envia pedidos de informação, processa as respostas recebidas e apresenta os dados numa interface compreensível para o administrador. Pode também enviar comandos para modificar configurações nos dispositivos remotos.

b) **Agente SNMP (*Agent*)**: Software que executa nos dispositivos geridos e responde aos pedidos do gestor. O agente mantém uma base de dados local com informações sobre o dispositivo e pode enviar notificações (*traps*) ao gestor quando ocorrem eventos significativos.

c) **MIB (*Management Information Base*)**: Base de dados hierárquica que define as variáveis (objetos) que podem ser consultadas ou modificadas num dispositivo. A MIB é estruturada como uma árvore, onde cada objeto é identificado por um OID (*Object Identifier*) único. Existem MIBs standard, definidas pela IETF, e MIBs proprietárias, desenvolvidas por fabricantes específicos.

d) **Protocolo de Rede**: O SNMP utiliza normalmente UDP (*User Datagram Protocol*) como protocolo de transporte, usando as portas 161 para pedidos do gestor e 162 para *traps* dos agentes. A escolha do UDP deve-se à sua simplicidade e baixo overhead, características alinhadas com a filosofia de simplicidade do SNMP.

2.3 Funcionamento e Operações

O SNMP define um conjunto limitado de operações básicas, mantendo a simplicidade que caracteriza o protocolo. As principais operações são Presuhn, 2002:

- **GET**: Permite ao gestor obter o valor de uma ou mais variáveis específicas da MIB. Esta é a operação mais comum, utilizada para consultar informações sobre o estado do dispositivo.
- **GET-NEXT**: Obtém o valor do próximo objeto na hierarquia da MIB. Esta operação é útil para percorrer sequencialmente a MIB sem conhecimento prévio de todos os OIDs disponíveis.
- **GET-BULK**: Introduzida no SNMPv2, permite obter múltiplos valores numa única operação, melhorando significativamente a eficiência na recuperação de grandes quantidades de dados.
- **SET**: Permite ao gestor modificar o valor de variáveis na MIB do agente, possibilitando a alteração de configurações remotamente.
- **TRAP**: Notificação assíncrona enviada pelo agente ao gestor quando ocorre um evento significativo (por exemplo, reinicialização do dispositivo, falha de interface, ultrapassagem de limites). Ao contrário das outras operações, o TRAP é iniciado pelo agente, não pelo gestor.

- **INFORM**: Semelhante ao TRAP, mas com confirmação de receção. Introduzida no SNMPv2, garante maior fiabilidade na entrega de notificações.

3 Versões do SNMP

3.1 SNMPv1

3.1.1 Características

O SNMPv1, definido nas RFC 1155, 1157 e 1212, foi a primeira versão do protocolo, publicada em 1988 Case et al., 1990. Esta versão estabeleceu os fundamentos conceptuais que persistem em todas as versões subsequentes do protocolo.

As principais características do SNMPv1 incluem:

- **Simplicidade**: Desenho minimalista com operações básicas (GET, GET-NEXT, SET, TRAP).
- **Estrutura de dados**: Utiliza SMI (*Structure of Management Information*) baseada em ASN.1 (*Abstract Syntax Notation One*) para definir a estrutura dos dados.
- **Autenticação por comunidade**: Sistema simples baseado em strings de comunidade que funcionam como passwords partilhadas.
- **Transporte UDP**: Utiliza UDP para comunicação, minimizando o overhead de rede.
- **Tipos de mensagens**: Define cinco tipos de PDUs (*Protocol Data Units*): GetRequest, GetNextRequest, SetRequest, GetResponse e Trap.

3.1.2 Vantagens

O SNMPv1 apresenta várias vantagens que justificaram a sua ampla adoção:

1. **Simplicidade de implementação**: O protocolo é suficientemente simples para ser implementado em dispositivos com recursos limitados, como switches de baixo custo e dispositivos IoT básicos.
2. **Baixo consumo de recursos**: A utilização de UDP e a estrutura simples das mensagens resultam em overhead mínimo, tanto em termos de processamento como de largura de banda.
3. **Interoperabilidade**: A standardização pela IETF garantiu que dispositivos de diferentes fabricantes pudessem comunicar usando o mesmo protocolo.
4. **Facilidade de configuração**: A configuração básica do SNMPv1 é relativamente simples, requerendo apenas a definição das strings de comunidade.

3.1.3 Desvantagens

Apesar das suas vantagens, o SNMPv1 apresenta limitações significativas:

1. **Segurança fraca**: As strings de comunidade são transmitidas em texto claro, tornando o protocolo vulnerável a ataques de *sniffing*. Qualquer pessoa com acesso à rede pode capturar e utilizar estas credenciais.
2. **Ausência de encriptação**: Toda a comunicação é transmitida sem encriptação, expondo informações potencialmente sensíveis sobre a configuração e estado da rede.
3. **Falta de mecanismos de integridade**: Não existem verificações para garantir que as mensagens não foram alteradas durante a transmissão.
4. **Tratamento de erros limitado**: O SNMPv1 possui capacidades limitadas de tratamento e reporte de erros, dificultando o diagnóstico de problemas.
5. **Operações limitadas**: A ausência de operações como GET-BULK resulta em ineficiência quando é necessário obter grandes quantidades de dados.
6. **Sem confirmação de TRAPs**: Os TRAPs são enviados sem confirmação, podendo perder-se sem que o agente tenha conhecimento.

3.2 SNMPv2

3.2.1 Características

O SNMPv2, inicialmente publicado em 1993 e posteriormente revisto (SNMPv2c definido na RFC 1901), foi desenvolvido para endereçar algumas das limitações funcionais do SNMPv1 Case et al., 1996. A versão "c"(*community-based*) tornou-se a mais amplamente utilizada.

As principais características do SNMPv2 incluem:

- **Novos tipos de dados**: Introdução de novos tipos como Counter64 para contadores de 64 bits, essencial para interfaces de alta velocidade.
- **GET-BULK**: Nova operação que permite obter múltiplas variáveis numa única mensagem, melhorando significativamente a eficiência.
- **INFORM**: Novo tipo de notificação com confirmação de receção, aumentando a fiabilidade.
- **Tratamento de erros melhorado**: Códigos de erro mais detalhados facilitam o diagnóstico de problemas.
- **Comunicação gestor-gestor**: Capacidade de comunicação entre sistemas gestores, permitindo arquiteturas distribuídas.

3.2.2 Vantagens

O SNMPv2 trouxe melhorias significativas em relação à versão anterior:

1. **Maior eficiência**: A operação GET-BULK permite obter múltiplos valores numa única transação, reduzindo drasticamente o número de mensagens necessárias para operações de descoberta e monitorização.
2. **Melhor desempenho**: O suporte a contadores de 64 bits é essencial para interfaces de rede modernas (Gigabit e superior), evitando problemas de *wrap-around* de contadores de 32 bits.
3. **Fiabilidade melhorada**: As mensagens INFORM com confirmação garantem que notificações críticas não se percam.
4. **Tratamento de erros superior**: Mensagens de erro mais descritivas facilitam a identificação e resolução de problemas.
5. **Compatibilidade**: O SNMPv2c mantém compatibilidade com o modelo de segurança baseado em comunidades, facilitando a migração desde o SNMPv1.

3.2.3 Desvantagens

Apesar das melhorias, o SNMPv2 mantém algumas limitações:

1. **Segurança inadequada**: O SNMPv2c mantém o modelo de segurança fraco baseado em comunidades do SNMPv1, sem encriptação ou autenticação robusta.
2. **Complexidade histórica**: As tentativas iniciais de criar um modelo de segurança robusto (SNMPv2u, SNMPv2*) resultaram em múltiplas variantes incompatíveis, causando confusão no mercado.
3. **Fragmentação**: A existência de várias variantes do SNMPv2 criou problemas de interoperabilidade e adoção lenta.
4. **Overhead adicional**: As novas funcionalidades, embora úteis, aumentam ligeiramente a complexidade e os requisitos de processamento.

3.3 SNMPv3

3.3.1 Características

O SNMPv3, definido nas RFC 3410-3415, foi publicado em 2002 e representa a evolução mais significativa do protocolo, focando-se primariamente em segurança Harrington et al., 2002. Esta versão não substitui o SNMPv2, mas adiciona capacidades de segurança robustas.

As características fundamentais do SNMPv3 incluem:

- **Modelo de segurança baseado em utilizadores (USM)**: Autenticação baseada em utilizadores individuais em vez de comunidades partilhadas.

- **Autenticação**: Suporte para protocolos de autenticação HMAC-MD5-96 e HMAC-SHA-96, garantindo a verificação da identidade do remetente.
- **Encriptação**: Suporte para encriptação usando DES, 3DES e AES, protegendo a confidencialidade dos dados transmitidos.
- **Controlo de acesso (VACM)**: Modelo baseado em visualizações (*View-based Access Control Model*) que permite definir permissões granulares sobre que objetos cada utilizador pode aceder.
- **Proteção contra replay**: Utilização de *timestamps* e números de sequência para prevenir ataques de repetição.
- **Modularidade**: Arquitetura modular que permite a adição de novos modelos de segurança sem alterar a estrutura base.

3.3.2 Vantagens

O SNMPv3 oferece vantagens significativas, especialmente em ambientes que requerem segurança:

1. **Segurança robusta**: A implementação de autenticação, encriptação e controlo de acesso torna o SNMPv3 adequado para ambientes onde a segurança é crítica.
2. **Autenticação forte**: Os mecanismos HMAC garantem que as mensagens provêm de fontes legítimas e não foram alteradas.
3. **Confidencialidade**: A encriptação protege informações sensíveis sobre a configuração e estado da rede contra interceptação.
4. **Controlo de acesso granular**: O VACM permite definir políticas de acesso detalhadas, limitando o que cada utilizador pode visualizar ou modificar.
5. **Conformidade**: Atende aos requisitos de segurança de standards como PCI-DSS, HIPAA e outros regulamentos de segurança da informação.
6. **Proteção contra ataques**: Mecanismos de proteção contra ataques de repetição, modificação e mascaramento.
7. **Flexibilidade**: Permite configurar diferentes níveis de segurança (sem autenticação, com autenticação, com autenticação e encriptação) conforme as necessidades.

3.3.3 Desvantagens

Apesar das suas capacidades avançadas, o SNMPv3 apresenta alguns desafios:

1. **Complexidade de configuração**: A configuração do SNMPv3 é significativamente mais complexa que as versões anteriores, requerendo a definição de utilizadores, contextos, visualizações e políticas de acesso.

2. **Overhead computacional**: Os processos de autenticação e encriptação consomem mais recursos de CPU, o que pode ser problemático em dispositivos com capacidades limitadas.

3. **Dificuldade de implementação**: A implementação correta de todos os mecanismos de segurança requer conhecimento especializado e atenção aos detalhes.

4. **Compatibilidade**: Dispositivos mais antigos podem não suportar SNMPv3, limitando a sua utilização em redes heterogéneas.

5. **Desempenho**: A encriptação e autenticação introduzem latência adicional, embora geralmente aceitável para a maioria das aplicações.

6. **Gestão de chaves**: A gestão segura de credenciais e chaves criptográficas adiciona complexidade administrativa.

7. **Curva de aprendizagem**: Administradores familiarizados com SNMPv1/v2c necessitam de formação adicional para utilizar eficazmente o SNMPv3.

4 Análise Comparativa das Versões

A tabela 1 apresenta uma comparação sintética das três versões principais do SNMP, destacando as principais diferenças em termos de funcionalidades e características de segurança.

Tabela 1: Comparação entre as versões do SNMP

Característica	**SNMPv1**	**SNMPv2c**	**SNMPv3**
Ano de publicação	1988	1993/1996	2002
Autenticação	Comunidade (texto claro)	Comunidade (texto claro)	USM com HMAC
Encriptação	Não	Não	Sim (DES/AES)
Integridade	Não	Não	Sim
Controlo de acesso	Básico	Básico	VACM (granular)
Operação GET-BULK	Não	Sim	Sim
INFORM	Não	Sim	Sim
Contadores 64-bit	Não	Sim	Sim
Complexidade	Baixa	Média	Alta
Segurança	Muito fraca	Muito fraca	Forte
Desempenho	Excelente	Muito bom	Bom
Compatibilidade	Universal	Universal	Limitada

4.1 Evolução da Segurança

A evolução mais significativa entre as versões do SNMP relaciona-se com a segurança. Enquanto o SNMPv1 e SNMPv2c utilizam um modelo de segurança extremamente simples baseado em strings de comunidade transmitidas em texto claro, o SNMPv3 introduz um modelo de segurança completo com múltiplas camadas de proteção.

O modelo de segurança do SNMPv3 define três níveis de segurança Blumenthal e Wijnen, 2002:

1. **noAuthNoPriv**: Sem autenticação nem encriptação (equivalente a SNMPv1/v2c).

2. **authNoPriv**: Com autenticação mas sem encriptação.

3. **authPriv**: Com autenticação e encriptação (nível recomendado).

4.2 Considerações de Desempenho

Em termos de desempenho, existe uma relação inversa entre segurança e eficiência. O SNMPv1 oferece o melhor desempenho devido à sua simplicidade, enquanto o SNMPv3 com encriptação e autenticação apresenta maior overhead. No entanto, em redes modernas, este overhead é geralmente insignificante face aos benefícios de segurança obtidos.

4.3 Adoção e Uso Atual

Apesar das vulnerabilidades conhecidas, o SNMPv1 e SNMPv2c continuam a ser amplamente utilizados, especialmente em ambientes internos considerados seguros. No entanto, a crescente preocupação com segurança e os requisitos regulamentares estão a impulsionar a migração para SNMPv3, particularmente em setores como banca, saúde e infraestruturas críticas Cisco Systems, 2020.

5 Desafios e Considerações de Implementação

A implementação eficaz do SNMP em ambientes de produção apresenta diversos desafios que os administradores de rede devem considerar:

5.1 Segurança

A segurança constitui o principal desafio na implementação do SNMP. Mesmo com a disponibilidade do SNMPv3, muitas organizações continuam a utilizar versões anteriores devido à compatibilidade com equipamentos legados. Quando a utilização de SNMPv1/v2c é inevitável, devem ser implementadas medidas compensatórias, tais como:

- Segregação da rede de gestão em VLANs dedicadas
- Utilização de ACLs (*Access Control Lists*) para restringir acesso aos agentes SNMP
- Escolha de strings de comunidade complexas e únicas
- Desativação do acesso SNMP em interfaces públicas
- Monitorização de tentativas de acesso não autorizado

5.2 Escalabilidade

Em redes de grande dimensão com milhares de dispositivos, a gestão via SNMP pode apresentar desafios de escalabilidade. O polling frequente de múltiplos dispositivos pode gerar tráfego significativo e sobrecarregar sistemas gestores. Estratégias para mitigar estes problemas incluem:

- Ajuste dos intervalos de polling conforme a criticidade das métricas
- Utilização de múltiplos servidores gestores com distribuição de carga
- Implementação de sistemas de caching para reduzir queries repetitivas
- Aproveitamento de TRAPs e INFORMs para notificações em vez de polling constante

5.3 Interoperabilidade

A diversidade de implementações de SNMP entre fabricantes pode causar problemas de interoperabilidade. MIBs proprietárias e interpretações diferentes dos standards podem resultar em comportamentos inconsistentes. A validação cuidadosa e testes de integração são essenciais.

6 Conclusão

O SNMP estabeleceu-se como o standard de facto para gestão de redes IP, mantendo-se relevante após mais de três décadas desde a sua criação inicial. A evolução do protocolo através de três versões principais reflete tanto a adaptação às necessidades crescentes de funcionalidade e segurança, como o compromisso com a retrocompatibilidade e simplicidade que caracterizaram a sua conceção original.

A análise detalhada das três versões principais – SNMPv1, SNMPv2c e SNMPv3 – revela uma progressão clara nas capacidades do protocolo. O SNMPv1 estabeleceu os fundamentos conceptuais e demonstrou a viabilidade de um protocolo de gestão simples e eficiente. O SNMPv2 trouxe melhorias funcionais importantes, particularmente a operação GET-BULK e o suporte a contadores de 64 bits, essenciais para redes modernas de alta velocidade. O SNMPv3 representou um salto qualitativo significativo ao introduzir mecanismos robustos de segurança, tornando o protocolo adequado para ambientes onde a proteção de informação é crítica.

A comparação entre versões evidencia os *trade-offs* inerentes ao design de protocolos de rede. O SNMPv1 e SNMPv2c oferecem simplicidade e desempenho excelente, mas à custa de segurança inadequada. O SNMPv3 fornece segurança robusta, mas introduz complexidade de configuração e overhead computacional. A escolha da versão apropriada deve considerar cuidadosamente o contexto específico de implementação, balançando requisitos de segurança, compatibilidade com equipamento existente, recursos disponíveis e expertise da equipa de administração.

Apesar das suas limitações, particularmente as vulnerabilidades de segurança das versões iniciais, o SNMP continua a ser amplamente utilizado em praticamente todas as redes empresariais modernas. A sua ubiquidade, simplicidade conceptual e amplo suporte por fabricantes garantem que o protocolo permanecerá relevante no futuro próximo. No entanto, a crescente adoção de SNMPv3 e o desenvolvimento de protocolos alternativos como NETCONF e RESTCONF sugerem uma evolução contínua no panorama da gestão de redes.

Para organizações que planeiam implementar ou migrar sistemas de gestão SNMP, recomenda-se fortemente a adoção do SNMPv3 sempre que possível, particularmente em ambientes onde a segurança é uma preocupação. Quando a utilização de versões anteriores for inevitável devido a limitações de equipamento legado, devem ser implementadas medidas de segurança compensatórias rigorosas.

Em conclusão, o SNMP representa um exemplo notável de um protocolo que, apesar das suas limitações iniciais, conseguiu adaptar-se e evoluir para responder às necessidades em constante mudança das redes de computadores modernas, mantendo simultaneamente os princípios de simplicidade que motivaram a sua criação.

7 Notas finais

Este trabalho foi desenvolvido no âmbito da unidade curricular de Análise de Comunicações em Rede do Mestrado em Engenharia de Segurança Informática do Instituto Politécnico de Beja, sob orientação do Professor Daniel José Da Graça Peceguinha Franco.

A elaboração deste relatório permitiu aprofundar o conhecimento sobre um dos protocolos mais fundamentais

em gestão de redes, compreendendo não apenas os seus aspetos técnicos, mas também a evolução histórica e as considerações práticas de implementação que afetam as decisões tecnológicas em ambientes reais.

Bibliografia

Blumenthal, U., & Wijnen, B. (2002). *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)* [Internet Requests for Comments, RFC 3414]. Obtido janeiro 15, 2026, de https://www.rfc-editor.org/rfc/rfc3414

Case, J., Fedor, M., Schoffstall, M., & Davin, J. (1990). *Simple Network Management Protocol (SNMP)* [Internet Requests for Comments, RFC 1157]. Obtido janeiro 15, 2026, de https://www.rfc-editor.org/rfc/rfc1157

Case, J., McCloghrie, K., Rose, M., & Waldbusser, S. (1996). *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)* [Internet Requests for Comments, RFC 1905]. Obtido janeiro 15, 2026, de https://www.rfc-editor.org/rfc/rfc1905

Cisco Systems. (2020). *Simple Network Management Protocol* [Documentação Cisco sobre SNMP]. Obtido janeiro 15, 2026, de https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/

Harrington, D., Presuhn, R., & Wijnen, B. (2002). *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks* [Internet Requests for Comments, RFC 3411]. Obtido janeiro 15, 2026, de https://www.rfc-editor.org/rfc/rfc3411

IPBeja. (2026). *Disciplina: Análise de Comunicações em Rede | IPBeja* [Página ACR]. Obtido janeiro 15, 2026, de https://cms.ipbeja.pt/course/view.php?id=529

Martinho Caeiro & Paulo Abade. (2026). *SNMP-Research - Repositório de Código* [Repositório do SNMP Research]. Obtido janeiro 15, 2026, de https://github.com/MartinhoCaeiro/SNMP-Research

Mauro, D. R., & Schmidt, K. J. (2005). *Essential SNMP* (2nd). O'Reilly Media.

Presuhn, R. (2002). *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)* [Internet Requests for Comments, RFC 3416]. Obtido janeiro 15, 2026, de https://www.rfc-editor.org/rfc/rfc3416

Stallings, W. (2007). *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2* (3rd). Addison-Wesley Professional.