

Simple Network Management Protocol (SNMPv2 and SNMPv3)



Stephen Wenn

Network Engineer



SNMP Versions (SNMPv1)

1ST

SNMPv1, introduced in 1988, is the first version of SNMP.

It enables basic monitoring and management of network devices, including status queries and alerts.

SNMPv1 uses plaintext community strings for authentication, making it insecure.

The protocol defines five key operations: Get, GetNext, Set, Trap, and GetResponse.

SNMPv1 is outdated due to weak security but laid the foundation for later versions.



SNMP Versions (SNMPv2c)

2ND

SNMPv2c, introduced in 1993, improves SNMPv1's performance and functionality.

Adds GetBulk operation for efficient data retrieval in large networks.

Relies on plaintext community strings for authentication, leaving it vulnerable.

Enhances error handling with more detailed feedback between manager and agent.

Despite improvements, it is still considered insecure due to weak authentication.



SNMP Versions (SNMPv3)



SNMPv3 adds robust security features like authentication, encryption, and message integrity.

Supports three security levels: noAuthNoPriv, authNoPriv, and authPriv, for secure environments.

Retains SNMPv2's performance but adds User-Based Security Model (USM) and View-Based Access Control Model (VACM).

USM and VACM provide detailed control over access to MIB data and actions.

SNMPv3 is preferred for modern network management due to its enhanced security and flexibility.



SNMP Message Types (Part 1)

Get Request
(v1, v2c and v3)

Get Next Request
(v2c and v3)

Set Request
(v1, v2c and v3)

Get Response
(v1, v2c and v3)



SNMP Message Types (Part 2)

Trap
(v1, v2c and v3)

Inform Request
(v2c and v3)

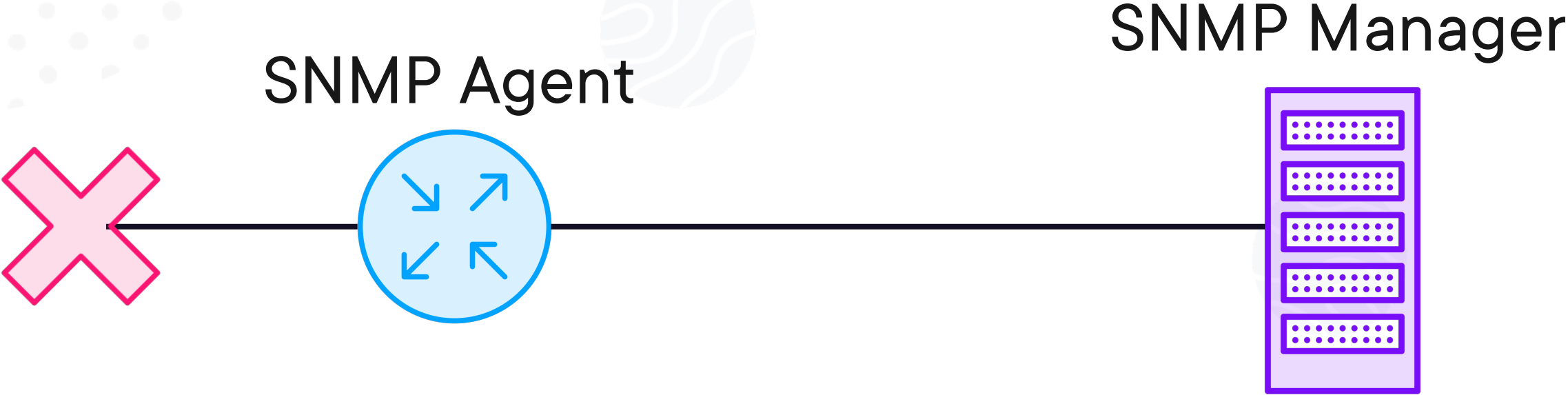
Get Bulk Request
(v2c and v3)



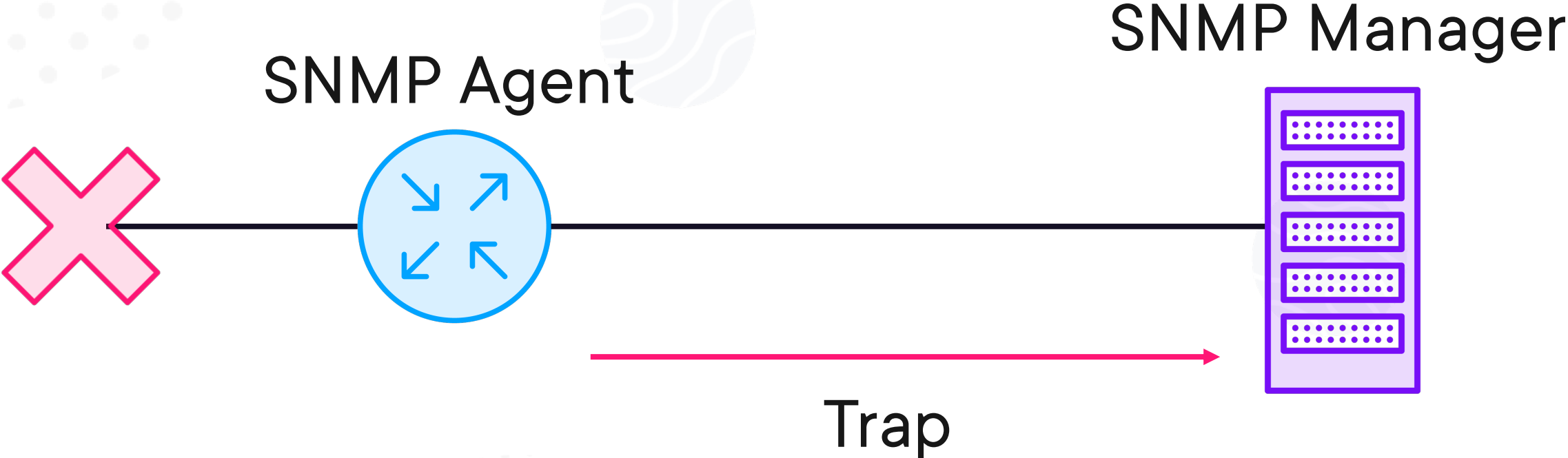
SNMP Inform vs. Trap



SNMP Inform vs. Trap



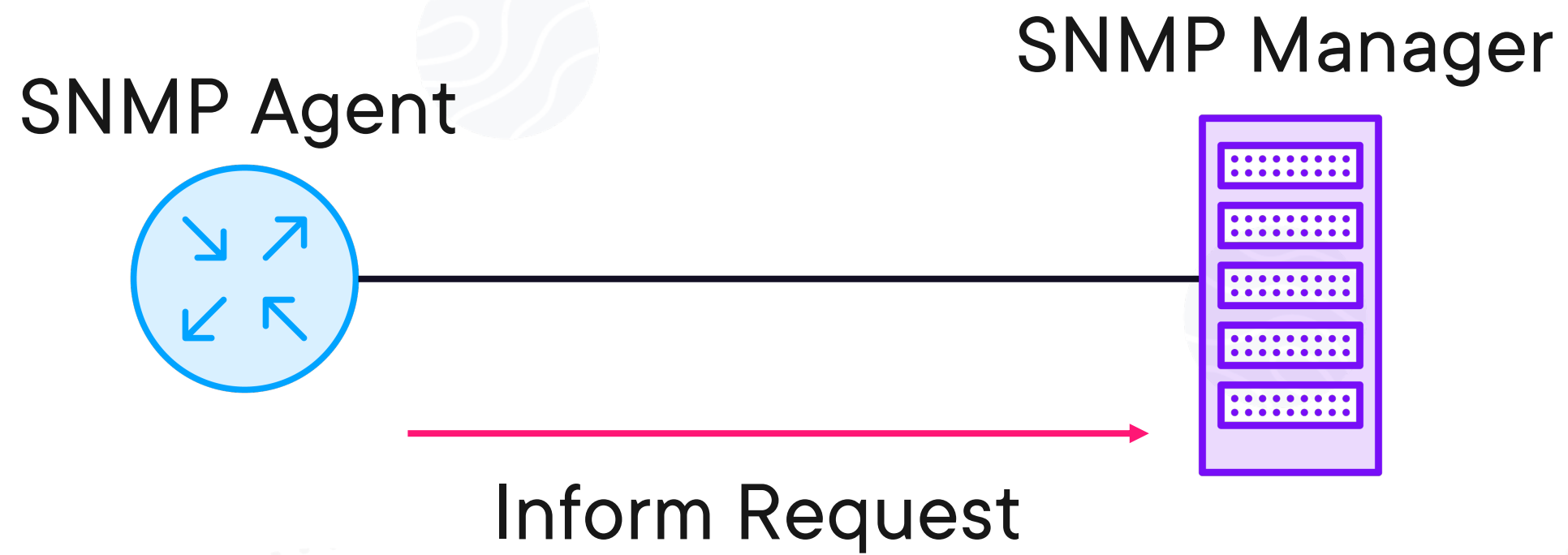
SNMP Inform vs. Trap



SNMP Inform vs. Trap



SNMP Inform vs. Trap



SNMP Inform vs. Trap

