How Barracuda RMM identifies the network role of SNMP devices

https://campus.barracuda.com/doc/98217217/

Under certain circumstances, some devices may have an unusual network role assigned to them by Barracuda RMM. This article explains the logic used in this classification, clarifying why this occurs.

Barracuda RMM's logic for classifying the network roles of SNMP devices can be expressed simply as, "if it looks like X, and is acting like X, classify is as X".

More specifically, network roles are classified as follows:

A Router

A device is classified as a Router if the Gateway address of the Onsite Manager is that of the device ***or*** if all of the following are applicable:

- The device has SNMP enabled.
- It has IPForwarding (OID 1.3.6.1.2.1.4.1.0) set to 1 (acting as a gateway).
- There is more than one network adapter.

A Switch

A device is classified as a Switch if ***all*** of the following are applicable:

- SNMP is enabled.
- IPForwarding (OID 1.3.6.1.2.1.4.1.0) is set to 2 (not acting as a gateway).
- It implements the Bridge Management Information Base (we check for the existence of OID_DOT1BASENUMPORTS [OID1.3.6.1.2.1.17.1.2.0]).

Cisco Devices

There is additional logic applied for Cisco devices. If SNMP is enabled and its SysObjectID is in Barracuda RMM's table of SysObjectIds, then the device will be assigned a role according to the mapping table.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.