Network Assessment Report

RHLABS
HQ
Version 1.1
December 22, 2020

Disclaimers

The information contained in this document is the proprietary and exclusive property of RouteHub Group and RH Example except as otherwise indicated. No part of this document, in whole or in part, may be reproduced, stored, transmitted, or used for design purposes outside of RHLabs infrastructure.

Privacy Information

This document may contain information of a sensitive nature. This information should not be given to persons other than those who are involved in the project or who will become involved during the project's lifecycle.

Document Owner

Author:	Michel Thomatis, CCIE #6778
Company:	RouteHub Group, LLC
Business:	RH Example
Location:	HQ1
Project Name:	Network Assessment Report v1.1
Email:	sales@routehub.com
Website:	www.routehub.net

Table of Contents

1 Introduction

This **Network Assessment Report** will provide a breakdown of your network environment in regard to its overall topology, configuration, and the hardware used for the network devices. The structure of the assessment will break up the network into different parts based on its solution type.

The network will have one or more **network frameworks** (e.g., LAN, WAN, Internet) which serves as the backbone for the network environment. From there you will have several **network solutions** that depend on the framework such as Wireless and Voice to provide a specific function to the network. Lastly, several **network services** would be configured on the framework and/or solutions as needed such as Routing and Switching.

Each of these network types will be broken down into different sections in this report. Based on our assessment (in this reduced sample report), we have determined the following network frameworks, solutions, and services from your network topology:

- **Network Frameworks**: LAN
- **Network Solutions**: Wireless
- **Network Services**: Switching

For each of these solutions, we will provide an outline of the current configuration based on the service, technology, and/or hardware device. But we will also provide an outline of the configuration and/or hardware recommendations for that solution on your network. This will include any caveats and considerations that should be addressed.

2 Network Frameworks

In this section, we will provide assessments for all **network frameworks** discovered in the environment.

2.1 Local Area Network (LAN) / Campus

The **LAN** is the main framework in the network topology where all other solutions are connected to. Below reflects how this framework is currently configured in the topology. Then we will provide our list of recommendations and considerations of changes that should be performed within this framework based on best practices including any issues discovered.

Current
- The network consists of a medium-sized 2-Tier LAN topology with a core and access layer all located in the same wiring closet with the other equipment
- The core switch consists of a Cisco Catalyst 2970G
- The access switch consists of a series of NETGEAR PoE switches configured in a cluster where all user endpoints and NEC IP phones are connected
- The switches are using EOL hardware with outdated software and non-standardized configuration
- All other major network solutions (WAN, Remote Access, Internet Perimeter, etc.) including server endpoints are connected directly into the Core switch
- There are other network devices with different functions that are connected among the core and access switches with undetermined purposes nor access
- The customer has reported connectivity issues with user endpoints (connected to the access switches) accessing the Internet and servers

Recommendations
- Based on the EOL hardware, network issues, and business requirements, it is recommended to replace the hardware for the core and access switches to use a single chassis-based switch, Cisco Catalyst 4500E Series which would provide increased performance, scalability, reliability, and flexibility to the environment
- The LAN topology would be considered as Tier-1 LAN Topology
- All of the major network solutions would still be connected to the new core switch
- It is recommended for each network device providing a different function be removed if it is no longer be used or to be integrated with the new core switch to avoid multiple devices to be managed. Any network device that is managed by a different vendor should be connected to an isolated VLAN on the Core switch with ACL restrictions.

3 Network Solutions

In this section, we will provide assessments for all **network solutions** discovered in the environment.

3.1 Wireless Network

The existing network consist of a **Wireless solution** which is considered as a supplemental network that is connected to the LAN. Below reflects how this solution is currently configured in the topology. Then we will provide our list of recommendations and considerations of changes that should be performed within this solution based on best practices including any issues discovered.

Current
- There are two consumer brand access points (different hardware models) at the main building advertising a single SSID
- One of the access points is a Cisco Linksys Access Point configured for WEP 128-bit security. The other access point is a D-Link Access Point configured for WPA/TKIP security
- Access Points are not Power over Ethernet (PoE) supported
- The two access points are plugged into the NETGEAR access switch
- The wireless SSID network is used by both employee and guest users
- Business wants to implement separate wireless networks for the employee and guest users
- There are several issues reported by the users related to wireless coverage, performance, and connectivity.

Recommendations
- It is recommended for the wireless network to use hardware intended for business networks. It is recommended to replace the consumer access points with a mesh of access points controlled by a single Wireless controller. One of the recommended hardware options would be Ubiquiti's UniFi solution for the Access Points and Wireless Centralized Controller.
- Completing a site survey to determine the best location and the estimated number of access points with the best signal to noise ratio (SNR) in the building
- The access points will be PoE supported and would be plugged into a PoE port on the recommended Cisco Catalyst 4500E core switch replacement
- The recommended wireless solution supports adding additional wireless SSIDs. One for employees with full access and another SSID for guests and contractors with limited access.
- Wireless security for employee SSID should be configured for WPA2. And wireless security for the guest SSID should be configured for either WPA2 or web portal.

4 Network Services

In this section, we will provide assessments for all **network services** discovered in the environment.

4.1 Switching

The existing network has **Switching services** configured among the framework and network solutions. Below reflects how this service is currently configured in the topology. Then we will provide our list of recommendations and considerations of changes that should be performed based on best practices including any issues discovered.

Current
- Mixed spanning tree configuration among the switches for RSTP and PVST
- Default Cisco VLAN Trunking Protocol (VTP) configuration using VTP server mode
- Mixed number of VLANs configured among the core and access switches. Most of the added VLANs are not in use nor assigned to a switch port
- Root Bridge for the VLANs are selected automatically among the switches on the LAN with a high number for Topology Change Notifications (TCN)
- 802.1Q Trunking is configured on some ports, but not matched on the connected switch device
- There is a high amount of CRC and output errors found on several switch ports
- Inconsistent configuration among the access switches that are configured as a stack
- Low port capacity on all switches

Recommendations
- The recommended switch replacement would allow for increased port capacity and performance as needed for the environment
- Rapid Spanning Tree (RSTP) configured for all switches
- VTP should be configured for VTP Transparent mode on all switches
- Define VLANs for each solution and endpoint network. A VLAN should be added for Users, Servers, Voice, Wireless, and Management to start with based on the current topology. Future VLANs can be added as needed.
- The core switch should be manually configured to be the root bridge for all VLANs using a low priority value assignment
- Perform switch clean-up of all unused configuration and services
- Ensure that all endpoint switchport's speed and duplex are configured for auto-negotiation including the endpoint systems themselves