Enhancing Network Security: Rogue Switch Detection and Prevention in Local Area Network

Vijay Bhuse, Yesaswini Vellaboina and Xinli Wang
School of Computing and Information Systems, Grand Valley State University, Allendale, MI, USA

bhusevij@gvsu.edu
vellaboy@mail.gvsu.edu
wangx@gvsu.edu

Abstract— Our paper comprehensively examines ways to detect and handle unauthorized switches in Local Area Networks (LANs) within today's intricate and interconnected network landscape. We demonstrate the utilization of PortFast and BPDU guard configurations to reinforce LAN security against unauthorized devices and potential complications arising from the spanning tree protocol. These measures not only enhance network performance but also function as robust protective mechanisms, safeguarding the integrity of the LAN infrastructure. Furthermore, this paper delves into advanced techniques for the proactive identification and prevention of rogue switches, fostering an overall enhanced security posture within LANs. By synergistically integrating PortFast, BPDU guard, and advanced rogue switch detection methods, the paper proposes a robust methodology to strengthen LAN security and maintain uninterrupted network operations. It equips organizations with crucial resources to establish a resilient, secure, and dependable digital infrastructure, addressing the evolving demands of network security.

Keywords: Rogue Switch, Portfast, BPDU Guard, Network Security, LAN, Detection

1. Introduction

In our interconnected digital realm, where the seamless flow of information is indispensable for businesses, institutions, and individuals, network security is most important. Local Area Networks (LANs) serve as the cornerstone of modern communication, safeguarding the integrity, availability, and confidentiality of sensitive data. As the intricacy of networked devices intensifies, bolstering LAN security becomes an absolute necessity in the face of increasing array of threats.

We comprehensively explore the intricate domain of LAN security, emphasizing three pivotal components that synergistically augment security: PortFast (PortFast 2018), Bridge Protocol Data Units (BPDU 2018) guard, and Rogue Switch Detection. PortFast and BPDU guard configurations optimize network performance and resilience, mitigating risks from unauthorized devices and alleviating risks associated with potential Spanning Tree Protocol (STP 2018) anomalies. These configurations embody proactive measures shielding LANs from disruptions and unauthorized intrusions.

Notwithstanding, in the face of a constantly evolving threat landscape, a more in-depth examination of rogue switch identification and mitigation is warranted. Rogue switches can introduce instability and security vulnerabilities, underlining the criticality of advanced detection mechanisms. The research rigorously investigates and implements these techniques to empower organizations with the capability to proactively counter potential threats.

Rogue switches can infiltrate the network through physical connections, where unauthorized individuals directly connect them to open network ports, mimicking legitimate equipment. This can be accomplished by plugging the rogue switch into an open wall jack or by connecting it to a network switch that is not properly secured. Employee errors, stemming from a lack of security awareness, can also contribute to rogue switch introductions. For example, an employee may accidentally connect a rogue switch to the network if they are not aware of the potential security risks. Insiders with malicious intent pose a substantial threat, as they may intentionally introduce rogue switches to the network to steal data or disrupt operations.

BPDU guard and PortFast stand as two critical components, working in tandem to safeguard Local Area Networks (LANs) from unauthorized access and potential disruptions. BPDU guard, a feature developed by Cisco, complements PortFast by actively monitoring ports for Bridge Protocol Data Units (BPDUs). These BPDUs serve as signals indicating the presence of unauthorized switches or misconfigurations within the network. By continuously monitoring for these BPDU signals, BPDU guard effectively identifies and neutralizes potential threats before they can compromise network integrity. On the other hand, PortFast expedites the transition process for access ports, eliminating the delays often encountered in traditional implementations. This rapid

transition ensures that end-user communication remains uninterrupted and efficient. By streamlining the access port transition process, PortFast contributes to a seamless and responsive network environment.

The integration of BPDU guard with PortFast proves to be a pivotal combination for network security. BPDU guard's active monitoring capabilities, coupled with PortFast's efficiency enhancements, provide a comprehensive approach to safeguarding LANs. This synergy ensures that both network efficiency and security are maintained on access ports, fostering a robust and reliable network infrastructure.

2. Related Work

The challenge of identifying rogue devices in network environments is a critical concern for network administrators aiming to maintain network security and stability. While existing methods have been established for detecting rogue wireless access points, the distinctive characteristics of wired networks necessitate separate approaches (Bhuse *et al.*, 2019 and Bhuse *et al.*, 2020).

The methods typically employed for identifying rogue wireless access points, such as wireless traffic analysis, site survey software, and tools like NetSpot (NetSpot, 2011), face limitations in the context of wired networks. These solutions are primarily reliant on monitoring wireless traffic patterns to identify suspicious activities, rendering them inapplicable for wired network infrastructures (Solarwinds, 2019) (Cisco Packet Tracer, 2023). Confronted with the challenge of detecting rogue switches in wired networks, network administrators have sometimes turned to IP sweep tools like Nmap (Nmap, 1997). However, these tools, while useful for IP address-based scanning, exhibit limited effectiveness. In wired networks, unmanaged Layer 2 switches are prevalent, often lacking IP addresses and support for neighbor discovery protocols. This limitation makes it difficult to accurately identify and locate rogue switches using traditional IP sweep.

Cisco's proprietary PortFast protocol provides an effective solution to address the challenge of rogue switches in wired networks. PortFast allows switches to expedite the activation of access ports by assuming that the connected device is a non-Spanning Tree Protocol (STP) device. As a result, the port is immediately transitioned to the forwarding mode. This streamlined approach significantly reduces network convergence time and, despite its proprietary nature, PortFast has become a standard feature in Cisco's switch offerings, facilitating the rapid provisioning of access ports (Cisco, 2018).

Complementing PortFast, Cisco's BPDU Guard serves as a vital security feature in wired network environments. BPDU Guard prevents unauthorized devices from transmitting Bridge Protocol Data Units (BPDUs) on access ports. When BPDU Guard is enabled on an access port and an unauthorized device attempts to send a BPDU, the port is promptly shut down. This proactive approach safeguards the network's integrity by swiftly blocking potentially harmful devices.

Numerous research efforts have been undertaken to determine the optimal configuration of PortFast and BPDU Guard for various types of local area networks (LANs) (Cisco, 2018). Cisco's PortFast and BPDU Guard protocols offer effective solutions to enhance network performance and security in wired environments. Ongoing research efforts aim to optimize the configuration of these protocols, tailoring them to diverse LAN topologies and security requirements.

3. Problem Definition

The existence of unauthorized rogue switches in Local Area Networks (LANs) poses a substantial threat to both the security and reliability of the network. These rogue switches, which are not authorized network devices, have the potential to disrupt normal network operations, compromise the security of data, and introduce anomalies into the spanning tree protocol. Regardless of whether they infiltrate the network with malicious intent or unintentionally, these devices introduce various risks such as network congestion, unauthorized access, data breaches, and potential network outages. The increasing number of connected devices in LANs further complicates the task of identifying and mitigating rogue switches.

To tackle this issue effectively, it is essential to use PortFast and BPDU guards. PortFast facilitates swift access for authorized end-user devices, ensuring efficient network operations. On the other hand, the BPDU guard acts as a protective measure against unauthorized switches by promptly disabling the corresponding port, thereby preventing network disruptions, and bolstering overall security. This configuration is crucial in environments where network reliability is a top priority, including critical infrastructure, guest networks, and remote office

setups. By employing PortFast and BPDU guards, organizations can establish a robust defense against the threats posed by rogue switches, ensuring both efficiency and security in LAN operations.

4. Experimental Analysis

Through a series of four experiments simulated with Cisco Packet Tracer, the application of PortFast and BPDU guard configurations was systematically explored to address network security concerns. The initial experiment highlighted security vulnerabilities in a baseline network topology without these configurations. Subsequent experiments demonstrated the collaborative impact of PortFast and BPDU guard in facilitating swift network access for authorized devices while effectively guarding against potential security threats, including the introduction of a rogue switch.

The final experiment, conducted in a complex network topology, emphasized the crucial role of BPDU guard in preventing unauthorized devices from disrupting the network's stability. Collectively, these experiments underscored the critical importance of implementing PortFast and BPDU guard configurations to enhance network performance, secure authorized access, and mitigate potential threats from unauthorized devices, ensuring the overall integrity and security of network infrastructures.

4.1 Experiment 1:

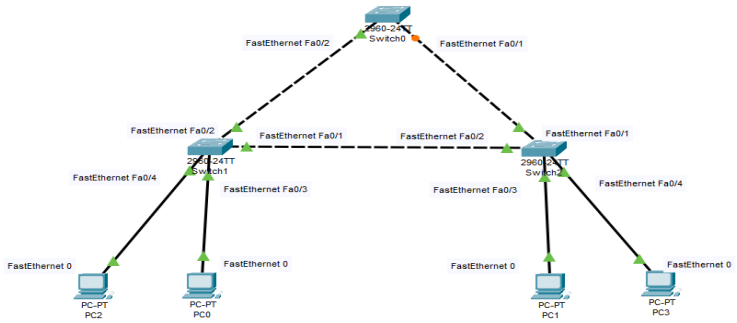

Figure 1: Network with STP enabled.

In a Cisco Packet Tracer simulation, a network topology was created to illustrate the practical application of network security. The network topology consists of three Cisco switches (Switch 0, Switch 1, and Switch 2) interconnected in a simple topology. Switch 0 is connected to Switch 1 via port 2, and Switch 0 is also linked to Switch 2 via port 1. Switch 1 is further connected to Switch 2 through port 2. This arrangement forms the foundation for demonstrating network configuration and security concepts. On Switch 1, two personal computers (PC 0 and PC 2) are connected to ports 3 and 4, respectively. Switch 2 has PC 1 and PC 3 connected to ports 3 and 4. These end-user devices represent practical network access points where network administrators must balance security and rapid connectivity.

In the current state of the network, PortFast and BPDU guard configurations have not been applied to the switch ports connecting to these end-user devices. Therefore, the network currently operates with standard spanning tree protocol settings. Significance of this scenario lies in the potential application of PortFast and BPDU guard configurations to enhance network performance and security. By configuring PortFast on the switch ports that connect to these end-user devices, network administrators can reduce the time required for devices to become operational, a critical requirement in environments where swift network access is essential.

Furthermore, the scenario highlights the potential security risks associated with swift port transitions when unauthorized devices, including rogue switches, exploit this rapid network access. Applying BPDU guard in conjunction with Port Fast can effectively monitor and prevent unauthorized network equipment from introducing disruptions or security breaches.

While the network in its current state does not employ PortFast and BPDU guard, the scenario sets the stage for the application of these configurations to strike a balance between network efficiency and security. By illustrating the impact of these configurations on a representative network topology, this research paper aims to enhance the understanding of how they can be applied to improve performance and safeguard against unauthorized network access and disruptions. It underscores the crucial role of network administrators in configuring and managing these features effectively to maintain network security and operational efficiency.

4.2 Experiment 2:

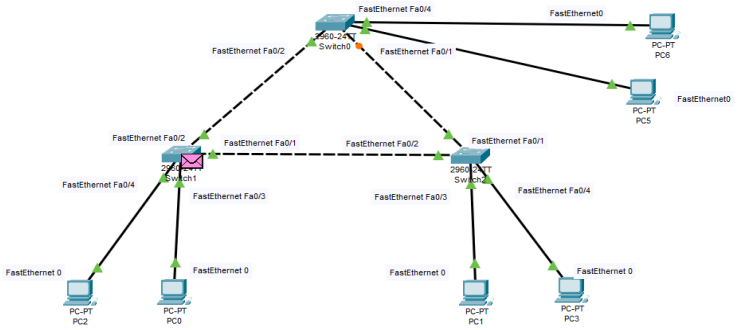

Figure 2: Network with PortFast and BPDU guard configured

In this Cisco Packet Tracer experiment, we have configured Switch 0, Port 4, with both PortFast and BPDU guard enabled, and introduced PC6 to the network, exemplifying the significance of these configurations in the realm of network security and efficient network access.

4.2.1 PortFast and BPDU Guard Configuration:

PortFast has been thoughtfully applied to Port 4 of Switch 0 to expedite network access for connected devices. Its primary objective is to reduce the time required for devices to transition to a fully operational state, significantly improving user experience. In scenarios where swift network access is paramount, Port Fast simplifies the process.

Complementing Port Fast, BPDU guard has been configured on the same port. BPDU guard plays a pivotal role in safeguarding the network from unauthorized or potentially disruptive devices. It continually monitors incoming traffic for Bridge Protocol Data Units (BPDUs), which are indicative of Spanning Tree Protocol (STP) messages typically generated by network switches. The presence of BPDUs suggests the potential connection of an unauthorized switch or a misconfigured device. In response to this security threat, BPDU guard is programmed to disable Port 4 promptly, protecting the network against potential disruptions and unauthorized access attempts.

4.2.2 Network Operation:

With PC6 connected to Port 4, the network operates smoothly. PC6 experiences rapid network access, and the network remains unaffected by any security actions triggered by BPDU guard. There are no disruptions or security concerns because PC6 is an authorized device and does not generate BPDUs.

This scenario demonstrates the practical implications of PortFast and BPDU guard configurations in a security-sensitive environment. It highlights how these configurations, when properly employed, can strike a delicate balance between network efficiency and security. While PortFast expedites network access for authorized devices, BPDU guard acts as a vigilant guardian against rogue devices and unauthorized network access.

The experiment showcases the synergy between these configurations, safeguarding the network against unauthorized or potentially disruptive devices, while ensuring swift network access for authorized users. By illustrating the impact of these configurations on a tangible network setup, this research paper seeks to enhance the understanding of how PortFast and BPDU guard can be applied to improve network performance and security. It underscores the critical role of network administrators in configuring and managing these features effectively to maintain network security and operational efficiency, ensuring that authorized devices can access the network swiftly without compromising its integrity.

4.3 Experiment 3:

In a controlled Cisco Packet Tracer experiment, we implemented PortFast and BPDU guard configurations on Switch 0, Port 4, and introduced a rogue switch to the network, providing valuable insights into the practical application of these security features. This scenario elucidates the significance of PortFast and BPDU guard in network security by addressing real-world vulnerabilities. Switch 0, a key component of the network topology,

is equipped with Port 4, which has been configured with PortFast and BPDU guard settings. These settings are crucial for enhancing network efficiency while concurrently bolstering security.

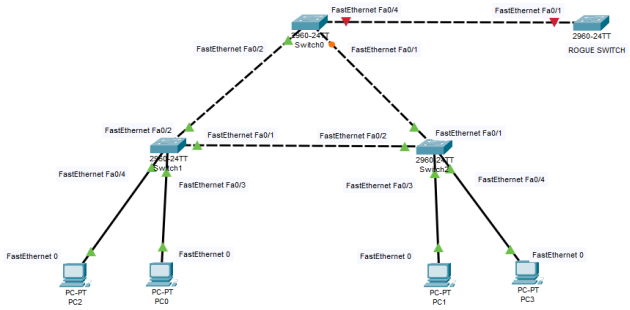

Figure 3: BPDU guard implemented

Port Fast Configuration: Port Fast is applied to Port 4 of Switch 0 to expedite network access for devices connected to this port. The primary goal is to reduce the time required for devices to become fully operational. In scenarios where swift network access is imperative, Port Fast streamlines the process.

BPDU guard Configuration: BPDU guard, implemented in tandem with PortFast on Port 4, serves as the network's first line of defense against unauthorized or rogue devices. BPDU guard vigilantly monitors incoming traffic for Bridge Protocol Data Units (BPDUs), typically indicative of spanning tree protocol messages generated by network switches. The presence of BPDUs suggests the potential connection of an unauthorized switch or a misconfigured device. In response to this security threat, BPDU guard automatically disables Port 4 to safeguard the network against potential disruptions and unauthorized access attempts.

Introducing the Rogue Switch: In the experiment, a rogue switch is introduced and connected to Port 4 of Switch 0, impersonating an authorized network device. Rogue switches are a potential security concern as they can inadvertently or maliciously introduce network loops or disrupt network operations. Rogue switches often remain undetected until they compromise network stability.

This controlled experiment demonstrates the real-world implications of PortFast and BPDU guard configurations in a security-sensitive environment. The deployment of PortFast expedites network access, enhancing the user experience, while the implementation of BPDU guard offers immediate protection against rogue devices.

The presence of the rogue switch on Port 4 initiates a critical response from the network. BPDU guard, diligently monitoring the port, detects the unauthorized BPDUs originating from the rogue switch. In response, BPDU guard promptly disables Port 4, neutralizing the potential security threat and preventing network disruptions.

This scenario underscores the essential role of PortFast and BPDU guard in securing network access points. It provides a tangible demonstration of the critical security implications and efficiency enhancements brought about by the simultaneous use of these features, protecting the network against rogue devices while ensuring rapid network access for authorized users. The experiment showcases how these configurations are pivotal in maintaining network security and operational efficiency in the face of evolving network threats.

4.3.1 Detection of Rogue Switch:

Ensuring the security and stability of a local area network is of paramount importance. Rogue switches, unauthorized devices that can disrupt network operations and compromise security, pose a significant threat. In this scenario, we explore the use of PortFast and BPDU Guard to detect and respond to rogue switches effectively.

4.3.2 Experimental Analysis:

Step 1: Configuration

Port 4 on Switch 0 is configured with PortFast, ensuring that it transitions to the forwarding state without the usual spanning-tree checks and timers. Additionally, BPDU Guard is enabled on Port 4 of Switch 0.

Step 2: Rogue Switch Connection

A rogue switch attempts to connect to Port 4 of Switch 0. When the rogue switch is powered on, it begins sending BPDUs due to its lack of proper network configuration.

Step 3: BPDU Guard Activation

As the rogue switch sends BPDUs, BPDU Guard on Port 4 of Switch 0 detects these unexpected BPDUs.

Step 4: Error Detection

The command-line interface (CLI) of Switch 0 displays a BPDU Guard error message indicating the detection of unexpected BPDUs on Port 4. This message is a critical alert for network administrators.

Step 5: Port Shutdown

In response to the BPDU Guard error, Switch 0 takes action to safeguard the network. Port 4 is placed into an error-disabled state, effectively disconnecting the rogue switch from the network.

Upon detecting the error, the network administrator is alerted to the situation. They can investigate and resolve the rogue switch issue, ensuring network security and integrity. Port 4 can be manually re-enabled once the rogue switch is removed.

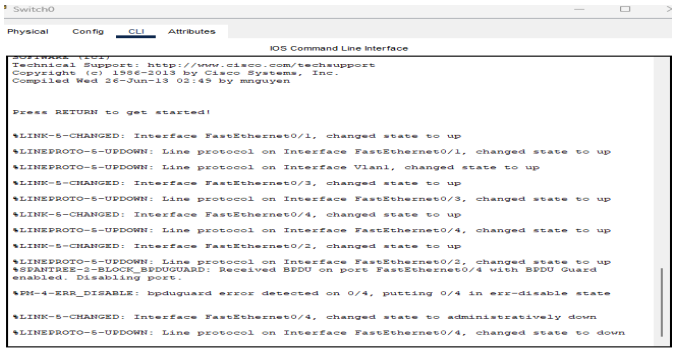

Figure 4: Detection of Rogue Switch

The scenario illustrates the significance of employing features like PortFast and BPDU Guard to protect a network from rogue devices. Rapid detection and response to unexpected BPDUs contribute to network stability and security, safeguarding the network from potential disruptions.

4.4 Experiment 4:

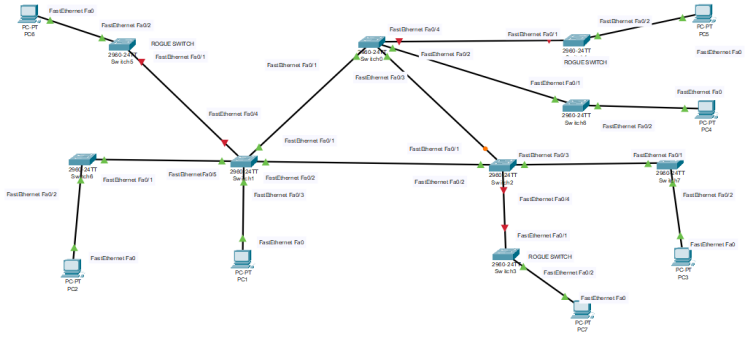

Figure 5: Network Infrastructure with Rogue Switches

For our research, we have configured a BPDU guard on three switches (Switch 0, Switch 1, and Switch 2), specifically on Port 4 of each switch. These switches are part of a network infrastructure, and Port 4 is strategically selected for this experiment. In our setup, rogue switches are introduced and connected to Port 4 of each of the three switches to evaluate the BPDU guard's effectiveness. BPDU guard operates by monitoring incoming BPDU frames on a switch port. If it detects a BPDU frame, the port is immediately placed in an error-disabled state.

In this network topology, Switch 0 serves as the central hub, connecting various switches and devices. Port 1 of Switch 0 links to Switch 1, while Port 2 connects to Switch 8, subsequently connecting to PC4. Port 3 is directed towards Switch 2, and Port 4 establishes a connection with Switch 4, which, in turn, connects to PC5. The network branching out from Switch 0 forms the core of the infrastructure, facilitating data flow between the switches and connected devices.

Switch 1 plays a pivotal role in the network by connecting to Switch 0 and various devices. It has links to Switch 2 via Port 2, connects directly to PC1 through Port 3, and establishes connections with Switch 5 and Switch 6 via Ports 4 and 5, respectively. These interconnections create a hierarchical structure, allowing for the distribution of data and resources efficiently. Switch 2, in turn, further expands the network, connecting to Switch 7 and Switch 3, which in turn connect to PC3 and PC7, respectively. This intricate design provides a comprehensive framework for the network's operations.

Switches 5, 6, 7, and 8 are responsible for connecting to individual devices: PC6, PC2, PC3, and PC4, respectively. The network design is structured to optimize data traffic and facilitate communication between the devices, ensuring seamless data transfer and efficient resource allocation. Understanding this network topology is crucial for network management, troubleshooting, and planning for scalability. It forms the backbone of a robust communication infrastructure, with each switch acting as a critical node in the network's overall functionality.

This action helps safeguard the network by preventing unauthorized devices from participating in the STP process, thus minimizing the potential for loops and other network disruptions. In our experiment, when rogue switches were introduced and connected to Port 4 of the switches (Switch 0, Switch 1, and Switch 2), the BPDU guard was triggered as expected. Upon receiving unauthorized BPDUs from the rogue switches, all three switches promptly disabled Port 4. This action successfully prevented the rogue switches from interfering with the network topology and maintained network stability.

The results of our study emphasize the vital role of BPDU guard in securing network infrastructure. By effectively disabling ports in response to unauthorized BPDU frames, it acts as a robust line of defense against rogue switches and other potential threats.

This security feature ensures that the network topology remains intact and operates without disruptions caused by unauthorized devices. In this research paper, we have explored the effectiveness of BPDU guard in mitigating network vulnerabilities introduced by rogue switches.

Our case study demonstrates that BPDU guard successfully identifies and responds to unauthorized BPDU frames, promptly disabling the affected ports and preventing rogue switches from compromising network stability. As such, we conclude that BPDU guard is a valuable feature for enhancing network security and ensuring the smooth operation of network infrastructure.

5. Conclusion

In conclusion, this research paper has delved into the critical realm of network security within Local Area Networks (LANs), with a specific focus on the prevention of rogue switches. The investigation has centered around the strategic implementation of PortFast and BPDU guard configurations as essential measures to fortify LANs against unauthorized devices and potential disruptions to the spanning tree protocol.

Through meticulously designed experiments simulated with the Cisco Packet Tracer, the practical implications of PortFast and BPDU guard configurations have been elucidated. These configurations, when appropriately deployed, showcase a synergistic relationship, enhancing both network efficiency and security. The experiments have underscored the importance of striking a delicate balance between rapid network access and safeguarding against unauthorized devices, particularly rogue switches.

Beyond the technical configurations, this research has addressed the multifaceted challenges associated with the introduction of rogue switches, considering various avenues such as physical connections, employee errors, and insider threats. The emphasis on proactive measures, including robust identity and access management, heightened employee awareness, and regular assessments, underscores the holistic approach required to mitigate security risks comprehensively.

This case study proves the critical role PortFast and BPDU guard play in preventing the introduction of rogue network switches. The insights derived from the experiments and analysis, empower network administrators with practical methodologies to enhance both the security posture and operational efficiency of LANs. By

understanding and implementing the findings presented herein, organizations can foster resilient, secure, and trustworthy digital infrastructures in the face of evolving threats within interconnected environments.

References

Bhuse, V., Kalafut, A., & Dohn L. (2019). “Detection of a Rogue Switch in a Local Area Network”. International Conference on Internet Monitoring and Protection, Nice, France.

Bhuse, V., James V. (2020). “Detecting a Rogue Switch using Network Automation”. ECCWS 2020 19th European Conference on Cyber Warfare and Security.

BPDU (2018) "Configuring BPDU Guard" Cisco.

Catalyst 3560 Software Configuration Guide, https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swstpopt.html#wp1203191

Cisco (2018). "Configuring Spanning Tree Protocol", https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9200/software/release/16-10/configuration_guide/lyr2/b_1610_lyr2_9200_cg/configuring_spanning___tree_protocol.html

Cisco Packet Tracer (2024) “Cisco Packet Tracer.” https://www.netacad.com/courses/packet-tracer.

NetSpot (2011). “Wi-Fi Network Planning and Site Survey.” https://www.netspotapp.com

Nmap (1997). “Nmap: the Network Mapper - Free Security Scanner.” https://nmap.org

fInNUcastPkts (2018) Available at: http://oid-info.com/get/1.3.6.1.2.1.2.2.1.12.

STP (2018). "Understanding Spanning Tree Protocol (STP)" https://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfa.shtml

Solarwinds (2019) "Detecting and Preventing Rogue Devices." https://www.solarwinds.com.

PortFast (2018) "Configuring PortFast"

Quitiquit, T., and Bhuse, V. (2022) "Utilizing Switch Port Link State to Detect Rogue Switches." Grand Valley State University, Allendale, MI, USA.