ISSN 2181-3187

ANALYSIS OF METHODS OF ENSURING PORT SECURITY IN SWITCHES

Rajabboyeva Surayyo Baxrom qizi
Urgench branch of Tashkent University of Information Technologies named After Muhammad al-Khwarizmi, Head of the Department Information Security Technologies
researchersurayyo@proton.me

Abstract — This article analyzes how to enable port security on the switch, how to prevent port security violations, and how to protect against attacks.

Switches are basic network devices that are mainly responsible for forwarding packets from one port to another. Although they are busy performing this important function, modern switches are capable of inspecting packet headers to enforce security policies at the network level. Port security is a network security feature that operates at layer 2 of the OSI model. It is mainly used to control and restrict access to the Ethernet ports of the switch. By implementing port security, network administrators can allow only authorized devices to connect to specific switch ports.

Today, port security is an important aspect of network infrastructure, not only focused on port protection, but also used to enhance features such as PortFast and Bridge Protocol Data Unit (BPDU) protection, Loop Prevention, DHCP Snooping and MAC filtering.

Keywords — Port Security, STP, PortFast, BPDU, DHCP Snooping, Loop, ARP, MAC filtering.

Introduction

Secure MAC addresses can be entered into the switch in 3 different ways:

1. static – secure MAC addresses are manually entered into the switch to allow the port.

2. dynamic - allows switching to MAC address learning when devices are connected and automatically updates the MAC address table. This is suitable for situations where the device changes frequently, but can be dangerous if unauthorized devices are connected.

3. sticky - learns MAC addresses dynamically and then stores them in the configuration.

The following example shows how to enable port security.

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config)#interface fa0/1
Switch(config-if)#switchport port-security mac-address aaaa.bbbb.cccc
```

ISSN 2181-3187

Here we have configured port security to allow only one MAC address on the port and specified that this MAC address should be aaaa.bbbb.cccc.

If the MAC address of the device connected to the port is different from the list of safe addresses, then a port violation occurs. By default, the port is in the error-disabled state.

Security breach mode descriptions are as follows:

shutdown (default) - the port immediately switches to the error-disabled state, turns off the port LED and sends a syslog message. This increases the damage counter. If the secure port error is disabled, the administrator must re-enable it by entering the disable and no disable commands.restrict - The port will drop packets with unknown source addresses until you remove enough safe MAC addresses to drop below the maximum value or increase the maximum value. This mode causes the Security Violation counter to increment and generates a system message.

protect - is the least secure of the security breach modes. The port will drop packets with unknown source MAC addresses until you remove enough safe MAC addresses to drop below the maximum value or increase the maximum value. No syslog message is sent.

There are also several alternative approaches to port security, some of which could be combined for better defence in depth.

802.1X Port-Based Authentication

802.1X Port-Based Authentication mandates devices to authenticate before gaining network access, significantly enhancing security by validating user or device identities through mechanisms like RADIUS (Remote Authentication Dial-In User Service). It’s possible to connect an 802.1X system to an LDAP directory which can be an excellent approach in an enterprise environment.

Network Access Control (NAC)

More generically, Network access control solutions enforce security policies based on device health, identity, and compliance. 802.1X Port-Based Authentication may also be a step in a broader NAC system. This approach offers dynamic and context-aware network access, making it adaptable to diverse network environments.

VLAN Segmentation

Isolating network traffic into separate VLANs restricts communication between segments, limiting the potential impact of security breaches or unauthorized access within a particular VLAN. This approach combines very well with traditional port security to provide an additional layer of defence.

Physical Port Security

Physical port security is also an essential aspect of overall network protection, focusing on securing the physical access points through which devices connect to a network. It involves strategies, technologies, and practices aimed at preventing

ISSN 2181-3187

unauthorized physical access to network ports and ensuring the integrity of the network infrastructure. Physical port security is often overlooked, but, if done right, physical port security can make life very hard for a would be attacker!

Importance of Physical Port Security

Physical access to network ports can provide unauthorized individuals with the opportunity to compromise network security, potentially leading to data breaches, network disruptions, and unauthorized data access. Usually, we think about normal access ports in a wall which are eventually connected to a switch port – but in poorly secured environments and attacker might even be able to access a network cabinet and the all-important console port of the switch itself. As security professionals, it's very easy to focus entirely on technical solutions – however physical access to a device is critical to consider.

The Main Part

Let's explore how to prevent several attacks on the switch.

Broadcast Storm Prevention

A broadcast storm is a disruptive network phenomenon where an excessive volume of broadcast (and sometimes multicast) traffic floods the network, overwhelming its capacity and impeding normal communication. Broadcast storms occur when a network device, such as a switch or router, continuously forwards broadcast frames - causing each device on the network to repeat and propagate these broadcasts. As the cycle repeats, network resources become saturated, leading to degraded performance, slowed data transmission, and even network outages. Broadcast storms often result from misconfigurations, network loops, or malfunctioning devices. If you study networking in any depth, you'll certainly learn more about avoiding Broadcast storms!

Port security addresses this concern by limiting the number of MAC addresses permitted on a given port. This limitation curbs the propagation of broadcast traffic that could lead to storms. By setting a maximum limit, network administrators ensure that a malicious or malfunctioning device cannot overwhelm the network with an excessive number of broadcasts. More advanced systems, such as storm control can also drop a specific type of traffic when more than a certain number of any one type of packet are seen on a link.

Flood attack prevention

In the same way that broadcast storms can disrupt a network, malicious actors can also send excessive traffic onto a network as part of a deliberate denial of service attack. There are numerous types of flooding attacks which could be attempted - ping floods, SYN floods, ICMP floods (Smurf attacks), and traffic flooding can all be mitigated in part by using port security and storm control.

ISSN 2181-3187

Preventing STP attacks

Network attackers can manipulate Spanning Tree Protocol (STP) to perform an attack by spoofing the root bridge and changing the network topology. We should use PortFast and Bridge Protocol Data Unit (BPDU) Guard to mitigate Spanning Tree Protocol (STP) manipulation attacks.

PortFast

PortFast – PortFast takes an interface configured as an ingress or trunk port from a blocking state to a forwarding state, bypassing the listening and learning states. Apply to all end-user ports. PortFast should only be configured on ports connected to end devices. PortFast access ports bypass STP listen and learn states to minimize STP association wait times. If PortFast is enabled on a port that connects to another switch, there is a risk of creating an extension chain.

Bridge Protocol Data Unit (BPDU) Guard

A Bridge Protocol Data Unit (BPDU) is a fundamental element of the Spanning Tree Protocol (STP) and its variants, which are used to prevent network loops in Ethernet networks. A BPDU is a special type of frame that network switches exchange to exchange information about the network's topology and to collectively determine the best path for forwarding traffic. BPDU frames contain information such as the sending switch's identity, priority, cost to reach the root switch, and the path cost from the sending switch to the root switch.

The primary purpose of BPDU exchange is to establish a loop-free topology by electing a root bridge and logically blocking redundant paths. The root bridge becomes the central reference point, and switches exchange BPDUs to calculate the shortest path back to the root. This calculation helps the switches identify which ports should be designated as forwarding ports (ports that can pass traffic) and which should be placed in a blocking state (ports which will not forward traffic), thereby preventing the formation of network loops that can severely disrupt network operations.

BPDU guard is a safety mechanism which is instrumental in maintaining network integrity. When a port unexpectedly receives BPDU frames, it triggers BPDU guard to disable the port. This precautionary measure prevents the accidental introduction of rogue switches that could lead to network loops. BPDU guard operates on ports designated as access ports, providing a crucial safeguard against accidental misconfigurations or deliberate attacks on network stability.

DHCP Snooping

DHCP snooping plays a pivotal role in securing IP address allocation within a network. It operates by distinguishing between trusted and untrusted ports. Trusted ports are those connected to DHCP servers, while untrusted ports are those which should not be connected to a DHCP server. If a DHCP response is received on an untrusted port, the switch can assume that it is likely to connect to rogue DHCP server.

ISSN 2181-3187

By validating DHCP responses on trusted ports and discarding unauthorized ones, DHCP snooping prevents potential IP address conflicts, unauthorized access, and potential security breaches.

Loop Prevention

Loop prevention mechanisms are vital to preventing disruptions caused by network loops. Port security contributes to this objective by monitoring the movement of MAC addresses within the network. When a port detects a sudden surge in MAC address changes or an unusual pattern, it indicates a possible loop. To prevent such scenarios, the port can be shut down automatically, mitigating the loop's impact and maintaining network availability.

Media Access Control (MAC) Filtering

MAC filtering involves permitting only specific MAC addresses to access a port, mitigating the risk of unauthorized devices gaining network access. MAC filtering is an effective approach assuming that devices are using their true MAC address – the problem is that spoofing a mac address is easily done and indeed, this is the default action for many modern devices (Especially phones). MAC address filtering can still be effective – an administrator can stipulate that MAC address spoofing be turned off when connecting to a corporate network, and opt for a "whitelist" approach to allowing devices. This would continue to ensure that only devices with permitted MAC addresses could access the network, but requires quite a lot of manual configuration to maintain. An attacker who is able to spoof a legitimate "allowed" MAC address can also still bypass this control.

Benefits of Port Security

Port security offers several advantages that contribute to a more secure and stable network environment:

Enhanced Security: Port security prevents unauthorized devices from gaining network access, reducing the risk of unauthorized data access, information theft, or malicious activities.

Reduced Attack Surface: By limiting the number of active devices on a port, port security minimizes the potential targets available to attackers, making it more challenging for them to infiltrate the network.

Improved Network Performance: Port security helps prevent broadcast storms and network loops, ensuring better network performance and responsiveness by minimizing unnecessary traffic and disruptions.

Ease of Management: Port security provides network administrators with granular control over connected devices. This facilitates more efficient network administration, troubleshooting, and device management.

ISSN 2181-3187

Compliance and Regulatory Requirements: Many industries have regulatory standards that mandate strong security practices. Port security helps organizations meet these requirements by controlling access and mitigating risks.

Drawbacks of Port Security

While port security offers numerous benefits, it also comes with certain drawbacks that also need to be considered:

Complex Configuration: Implementing and managing port security on a large scale can be complex and time-consuming. Configuring and maintaining individual port settings, especially in dynamic environments, requires careful planning and continuous oversight.

Limited Flexibility: Port security's strict access controls can impede the flexibility needed in rapidly changing network environments. Frequent device changes or the addition of new devices may necessitate constant reconfiguration.

MAC Spoofing: Port security primarily relies on MAC addresses for authentication, which can be susceptible to MAC spoofing attacks. Skilled attackers can forge legitimate MAC addresses to bypass port security measures.

Potential False Positives: In certain scenarios, legitimate network changes or maintenance activities might trigger port security mechanisms, causing temporary disruptions or false alarms.

Complex Troubleshooting: When issues arise, diagnosing problems related to port security can be intricate and time-consuming, requiring a deep understanding of the configuration and potential interactions with other network components.

III Conclusion

Port security (including physical port security) remains a critical component of network security, offering protection against unauthorized access and network disruptions. By employing various techniques such as port security learning types, broadcast storm prevention, BPDU guard, loop prevention, DHCP snooping, and MAC filtering, organizations can bolster their network's security posture. While port security has its benefits and drawbacks, considering alternatives like 802.1X authentication and NAC can provide additional layers of security to meet evolving network demands.

References

[1] https://www.zenarmor.com/docs/network-security-tutorials/what-is-vlan-hopping#:~:text=Switch%20spoofing%20is%20a%20type,multiple%20VLANs%20within%20a%20network.
[2] https://www.vskills.in/certification/tutorial/switch-attacks/
[3] https://community.fs.com/article/basic-switch-security-concepts-explained.html
[4] https://library.mosse-institute.com/articles/2023/08/port-security.html
[5] https://www.crowdstrike.com/cybersecurity-101/spoofing-attacks/arp-spoofing/

ISSN 2181-3187

[6] Regulation (EC) No 725/2004 of the European Parliament and the Council on Enhancing Ship and Port Facility Security, 31 March 2004
[7] Directive 2005/65/EC of the European parliament and the Council on Enhancing Port Security, 26 Oct 2005
[8] I.Vakalis, B.Hosgood, P.Chawdry, "Biometrics for Border Security – An Overview", Technical Report EUR 22359 EN, European Communities 2006
[9] PortID Consortium, "Study for the Analysis and the Conceptual Development of an European port Access Identification Card (EPAIC)", Final Report, QINETIC/07/03289,19 Dec 2007
[10] F. Andritsos, M. Mosconi, "Port Security in EU: a Systemic Approach", 2nd International Conference on Waterside Security (WSS 2010), Marina di Carrara, Italy, November 2010 Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 14–15 December 2018.