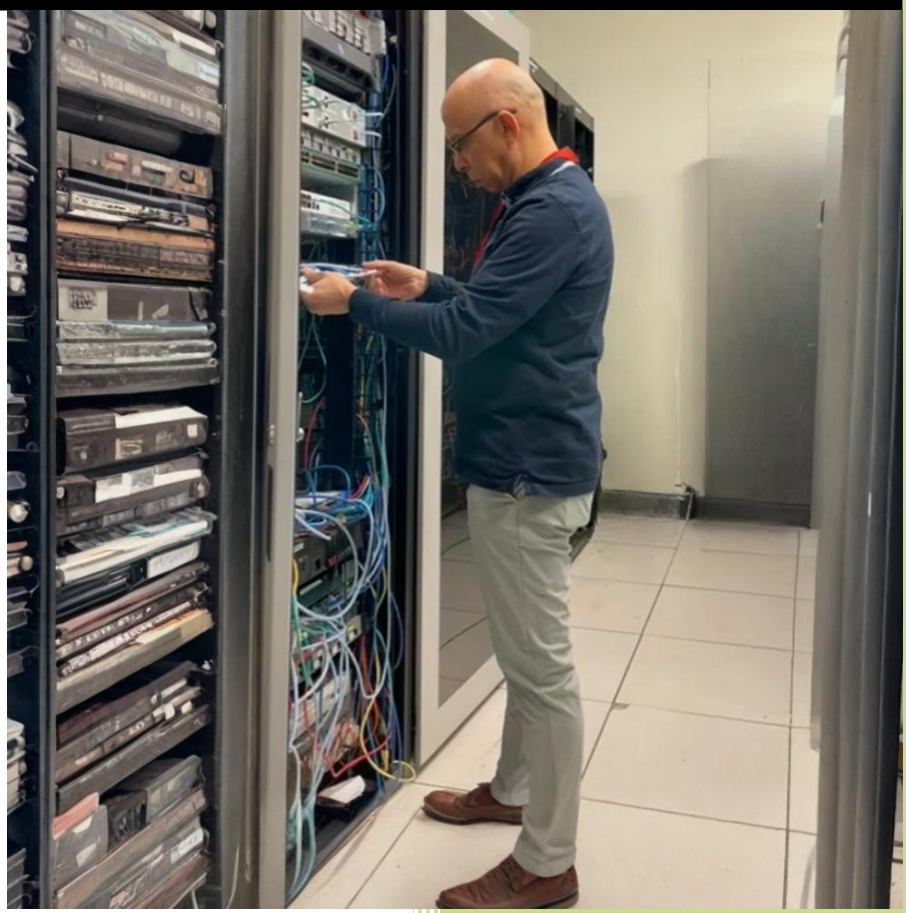
CYBERSECURITY NOTES

Ethernet Security Techniques



leonel pedroza

Contents

Protecting your physical wired access

Introduction

In today's interconnected world, every organization relies on networks to conduct business, communicate, and store sensitive information. Yet one of the most overlooked vulnerabilities lies hidden in plain sight: the physical network ports scattered throughout our offices, conference rooms, and public spaces.

Imagine walking into your building's lobby and noticing an electrical outlet. You wouldn't plug in a stranger's device without questioning it. Network ports—those small ethernet jacks in walls and switches—deserve the same caution. When left unsecured, they become open doors that bypass expensive firewalls and sophisticated security software.

An unprotected network port is like leaving your office building with no locks on the doors. Anyone with a laptop and a cable can potentially access confidential data, install malicious software, or monitor private communications. The consequences range from stolen customer information and intellectual property theft to complete network shutdowns that paralyze operations.

While cybersecurity often focuses on complex digital threats, physical security remains fundamental. A single unsecured port can undo millions of dollars in digital defenses. Whether it's a disgruntled employee, a visitor with ill intentions, or simply someone plugging in an infected device, the risks are real and immediate.

This book will guide you through practical steps to secure your network's physical access points, helping you close these often-ignored gaps in your security infrastructure. By understanding and addressing these vulnerabilities, you protect not just your data, but your organization's reputation and future.

Port Security

Port Security allows the restriction of the number of MAC addresses learned on a switch port, preventing MAC flooding attacks.

Advantages:

- Limits access to the network at the switch port level.
- Helps mitigate MAC address table overflow attacks.

Disadvantages:

- Static configuration may block legitimate devices.
- Requires constant monitoring and adjustment.

Configuration Examples:

- Cisco:

```
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation restrict
 switchport port-security mac-address sticky
```

- HP/Aruba:

```
interface 1
 port-security
 port-security max-mac-count 1
 port-security learn-mode sticky
 port-security action restrict
```

- Juniper:

```
set ethernet-switching-options secure-access-port interface ge-
0/0/1 allowed-mac 00:11:22:33:44:55
set ethernet-switching-options secure-access-port interface ge-
0/0/1 restrict
```

802.1X Authentication

802.1X is a network access control protocol that enforces authentication before granting access to the network. 802.1X is a protocol that requires authentication before allowing network access.

Advantages:

- Provides user-level access control via RADIUS.
- Integrates with existing identity management solutions.

Disadvantages:

- Requires an authentication server (RADIUS) and configuration.
- Complex deployment, especially in legacy environments.

Configuration Examples:

- Cisco:

```
interface FastEthernet0/1
 switchport mode access
 authentication port-control auto
 dot1x pae authenticator
 dot1x timeout quiet-period 5
```

- HP/Aruba:

```
aaa port-access authenticator 1
aaa port-access authenticator active
aaa port-access authenticator unauth-vid 999
aaa port-access authenticator auth-vid 10
```

- Juniper:

```
set interfaces ge-0/0/1 unit 0 family ethernet-switching port-
mode access
set protocols dot1x authenticator interface ge-0/0/1 supplicant
multiple
```

DHCP Snooping

DHCP Snooping filters untrusted DHCP messages and builds a database of valid IP-to-MAC bindings to prevent rogue DHCP servers.

Advantages:

- Protects against DHCP spoofing attacks.
- Creates a trusted binding database for other features (e.g., IP Source Guard).

Disadvantages:

- May block legitimate servers if misconfigured.
- Binding database requires proper maintenance.

Configuration Examples:

- Cisco:

```
ip dhcp snooping
ip dhcp snooping vlan 10
interface FastEthernet0/1
 ip dhcp snooping trust
interface FastEthernet0/2
 ip dhcp snooping limit rate 15
```

- HP/Aruba:

```
dhcp-snooping
dhcp-snooping vlan 10
interface 1
 dhcp-snooping trust
```

- Juniper:

```
set ethernet-switching-options secure-access-port interface ge-
0/0/1 dhcp-trusted
```

BPDU Guard

BPDU Guard disables a port if a Bridge Protocol Data Unit (BPDU) is received, protecting the STP topology.

Advantages:

- Prevents STP manipulation on edge/access ports.
- Protects the network from loops caused by user devices.

Disadvantages:

- May block ports unintentionally if BPDUs are received.
- Should only be used on access ports.

Configuration Examples:

- Cisco:

```
interface FastEthernet0/1
 spanning-tree bpduguard enable
```

- HP/Aruba:

```
spanning-tree bpdu-protection
interface 1
 spanning-tree bpdu-protection
```

- Juniper:

```
set protocols rstp interface ge-0/0/1 no-root-port
```

Storm Control

Storm Control prevents traffic storms (broadcast, multicast, or unknown unicast) by applying traffic thresholds on switch ports.

Advantages:

- Protects against denial-of-service from broadcast storms.
- Improves overall network reliability.

Disadvantages:

- Misconfiguration can drop legitimate traffic.
- Threshold tuning is environment-specific.

Configuration Examples:

- Cisco:

```
interface FastEthernet0/1
 storm-control broadcast level 30.00
 storm-control multicast level 30.00
```

- HP/Aruba:

```
interface 1
 broadcast-limit 30
```

- Juniper:

```
set interfaces ge-0/0/1 unit 0 family ethernet-switching storm-
control broadcast level 30
```

Private VLANs

Private VLANs provide layer 2 isolation between ports in the same VLAN, often used in shared environments like data centers.

Advantages:

- Increases network segmentation without increasing VLAN count.
- Useful in ISP and hosting provider scenarios.

Disadvantages:

- Complicated to configure and troubleshoot.
- Not universally supported across all vendors.

Configuration Examples:

- Cisco:

```
vlan 100
 private-vlan primary
vlan 101
 private-vlan isolated
vlan 102
 private-vlan community
interface FastEthernet0/1
 switchport mode private-vlan host
 switchport private-vlan host-association 100 101
```

- HP/Aruba:

  Not natively supported on all models; similar functionality requires traffic filters or ACLs.

- Juniper:

```
set vlans private-vlan vlan-id 100
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan
members private-vlan
```

MACsec

MACsec provides point-to-point encryption at Layer 2 to ensure data confidentiality and integrity over the LAN.

Advantages:

- Encrypts Ethernet frames to protect from snooping and tampering.
- Adds security without changing Layer 3 configurations.

Disadvantages:

- Requires hardware and software support.
- May introduce latency and processing overhead.

Configuration Examples:

- Cisco:

```
interface GigabitEthernet0/1
 macsec
 mka policy default
 mka pre-shared-key key-chain MACSEC-KEY
```

- HP/Aruba:

```
interface 1
 macsec enable
 macsec policy secure-policy
```

- Juniper:

```
set interfaces xe-0/0/1 gigether-options macsec enable
```

IP Source Guard

IP Source Guard prevents IP spoofing by filtering traffic based on valid IP-MAC bindings derived from DHCP Snooping.

Advantages:

- Mitigates spoofing and man-in-the-middle attacks.
- Automatically applies binding-based filters.

Disadvantages:

- Relies on accurate DHCP Snooping data.
- Static IPs require manual binding entries.

Configuration Examples:

- Cisco:

```
ip dhcp snooping
interface FastEthernet0/2
 ip verify source
```

- HP/Aruba:

```
interface 1
 ip verify source
```

- Juniper:

```
set ethernet-switching-options secure-access-port interface ge-0/0/1 ip-source-guard
```

Dynamic ARP Inspection

DAI inspects ARP packets and compares them against trusted DHCP Snooping bindings to prevent ARP spoofing.

Advantages:

- Blocks malicious ARP packets.
- Prevents man-in-the-middle attacks on LANs.

Disadvantages:

- Consumes switch CPU resources.
- Can block valid ARP if DHCP Snooping is not configured properly.

Configuration Examples:

- Cisco:

```
ip arp inspection vlan 10
interface FastEthernet0/2
 ip arp inspection trust
```

- HP/Aruba:

```
arp-protect vlan 10
interface 1
 arp-protect trust
```

- Juniper:

```
set ethernet-switching-options secure-access-port interface ge-
0/0/1 arp-inspection
```

VLAN Segmentation

VLANs logically separate network traffic, reducing broadcast domains and improving security by isolating user groups.

Advantages:

- Improves network performance and security.
- Allows policy enforcement per segment.

Disadvantages:

- Requires VLAN-aware infrastructure.
- Complexity increases with scale and misconfiguration.

Configuration Examples:

- Cisco:

```
vlan 10
 name HR
interface FastEthernet0/1
 switchport access vlan 10
```

- HP/Aruba:

```
vlan 10
 name HR
interface 1
 untagged vlan 10
```

- Juniper:

```
set vlans HR vlan-id 10
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan
members HR
```

MAC Address Filtering

MAC Filtering restricts network access to specific MAC addresses, enforcing a basic access control at the switch port.

Advantages:

- Simple access control method for small networks.
- Can prevent casual unauthorized device connections.

Disadvantages:

- MAC addresses can be spoofed.
- Not scalable for large networks with dynamic devices.

Configuration Examples:

- Cisco:

```
interface FastEthernet0/1
 switchport port-security mac-address 00:11:22:33:44:55
```

- HP/Aruba:

```
interface 1
 mac-address 0011.2233.4455 mask ffff.ffff.ffff
 port-security
```

- Juniper:

```
set ethernet-switching-options secure-access-port interface ge-
0/0/1 allowed-mac 00:11:22:33:44:55
```

Final Thoughts: Securing Your Enterprise Network

In today's modern enterprises, Ethernet networks and his many flavors form the backbone of communication, data access, and operations. While Wi-Fi and firewalls often dominate security discussions, physical Ethernet ports and Layer 2 technologies present critical vulnerabilities if left unmanaged.

Corporate environments must adopt a zero-trust mindset even at the switch port level. Port Security, 802.1X authentication, and MACsec encryption should be enforced by policy, particularly in workspaces, data centers, and shared areas. Technologies such as DHCP Snooping, IP Source Guard, and Dynamic ARP Inspection can prevent spoofing and rogue DHCP servers that threaten service integrity.

Furthermore, VLAN segmentation must be strategically planned to isolate critical systems such as finance, HR, or production environments. This reduces lateral movement in case of a breach. Private VLANs are ideal in co-located facilities or environments with high multi-tenancy, such as ISPs or hosting providers.

Physical access controls combined with stringent switch-level policies create layered security defenses. Regular audits must be practiced along with a strong regimen to update firmware and enhance dynamic monitoring tools in order to detect anomalies and ensure compliance with internal and external cybersecurity standards.

Layer 2 foundation protection is paramount. The best of perimeter defenses are nothing if an attacker gains physical access to an Unmanaged Port. By combining Ethernet security into any enterprise architecture, an organization protects not merely its infrastructure but also its business continuity and reputation.

Glossary

802.1X Authentication – Protocol used for port-based network access control.

BPDU Guard – Feature that disables ports receiving STP BPDUs to avoid topology attacks.

Broadcast Storm – Excessive broadcast traffic that can degrade or bring down a network.

DHCP Snooping – Security feature that filters DHCP messages to prevent rogue servers.

Dynamic ARP Inspection (DAI) – Validates ARP packets using DHCP Snooping database.

IP Source Guard – Blocks spoofed packets using IP/MAC binding information.

MAC Filtering – Restricts access to devices with approved MAC addresses.

MAC Flooding – Attack targeting the switch's MAC address table to intercept traffic.

MACsec – Layer 2 encryption standard for Ethernet security.

Man-in-the-Middle Attack – An attacker intercepts or modifies communications.

Port Security – Limits access to switch ports based on MAC address learning.

Private VLANs – Allows isolation of devices within the same VLAN.

Spanning Tree Protocol (STP) – Protocol to prevent loops in Ethernet networks.

VLAN Segmentation – Logical separation of devices within a network to improve security.

Extra Goodies: Appendices

Appendix A: Which Security Method / Switch When? A Quick Guide

Security Method	Best Use Case	Switch Type
Port Security	Small networks to prevent MAC flooding	Cisco, HP, Juniper
802.1X Authentication	Enterprise environments with identity servers	Cisco, HP, Juniper
DHCP Snooping	Networks with DHCP and risk of rogue servers	All major vendors
BPDU Guard	Office edge ports to protect STP	Cisco, HP
Storm Control	LANs at risk of traffic floods	All vendors
Private VLANs	Shared hosting, ISPs, multi-tenant setups	Mostly Cisco
MACsec	Sites requiring encrypted Ethernet	Cisco, HP, some Juniper
IP Source Guard	Networks using DHCP Snooping	Cisco, Juniper
Dynamic ARP Inspection	LANs with DHCP and ARP poisoning risk	Cisco, HP
VLAN Segmentation	Isolate departments or devices	All vendors

Appendix B: Vendors to Check Out

1. **Arista Networks** – https://www.arista.com/
   Powerful switching solution.
2. **Cisco Systems** – https://www.cisco.com
   World leader in enterprise network security and switching.
3. **Hewlett Packard Enterprise (Aruba)** – https://www.arubanetworks.com
   Offers powerful edge and access switching solutions.
4. **Juniper Networks** – https://www.juniper.net
   Known for high-performance switching and security integration.

References

- Cisco Networking Docs – https://www.cisco.com/c/en/us/support/docs
- Aruba Networks Documentation – https://www.arubanetworks.com/techdocs
- Juniper TechLibrary – https://www.juniper.net/documentation
- IEEE 802.1X Standard – https://standards.ieee.org/
- NetworkLessons.com – https://networklessons.com/
- PacketLife.net Cheat Sheets – https://packetlife.net/library/cheat-sheets/
- GitHub - Community Security Scripts – https://github.com/leonelpedroza

A Little About Me & Why I Do This

BSc. Electronic engineer

Senior Network Analyst | Cybersecurity Engineer | Telecommunications Specialist

So, what's my deal? I've got this personal mission, you could call it a challenge: to explain how cybersecurity works in plain English, or as I like to say, in "muggle" language. For over 12 years, I was a technical instructor for big corporate clients, and I can't even count the number of internal training sessions I ran for colleagues across Latin America. I've also had the privilege of being a university professor, teaching systems engineering to both undergrads and graduate students.

If there's one thing all those years have taught me, it's this: not everyone speaks "geek." And that's perfectly okay! My goal here, and with other stuff I create, is to cut through the dense technical jargon without losing the important stuff. I genuinely hope that if you're reading this, you feel a bit more confident and can speak up about why understanding cybersecurity is so important these days. It's not just for the IT crowd anymore; it's for everyone.

→ Want to learn more or find some tools? Check out my stuff on GitHub:

github.com/leonelpedroza