Global Knowledge®

Expert Reference Series of White Papers

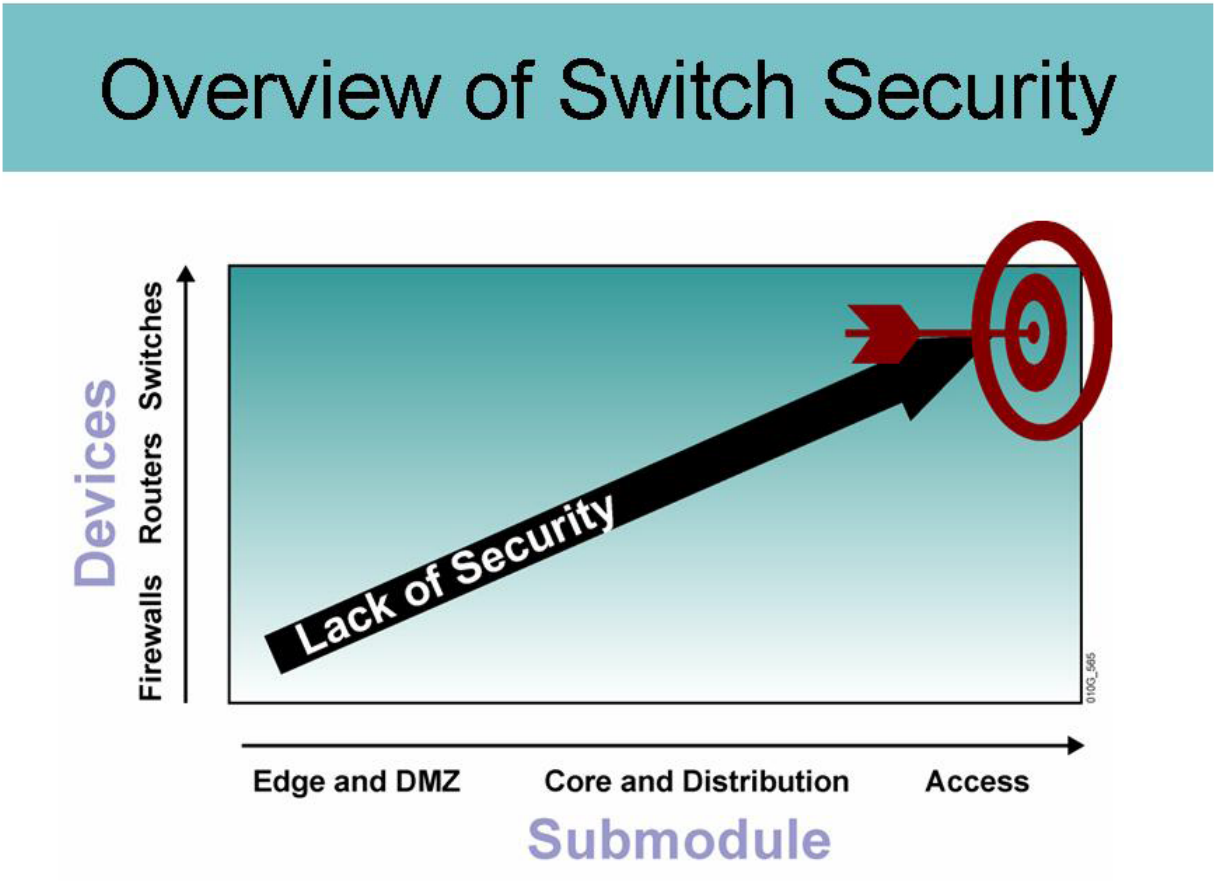
Securing Layer 2

Securing Layer 2

Carol Kavalla, Global Knowledge Instructor

Introduction

For many years network administrators have expected security breaches to come from outside an organization or at the upper layers of the OSI model. For this purpose, firewalls are implemented at the edge of a network. While the default state of a firewall does not allow communication between an organization and networks beyond the organizational borders, routers and switches were designed to enable communication.



A firewall needs to be configured specifically to allow IP packets to traverse it. By default, routers do not filter traffic; however, they can be configured to filter traffic based on inspecting values in layer 3 and layer 4 IP headers. Switches can also be configured to thwart attacks launched at the LAN layer.

In recent years, Cisco has expanded its focus beyond a perimeter type of security that is obtained through firewalls and Intrusion Detection (or Prevention) Systems (IDS or IPS) at the edge of the network. In addition to the Enterprise Edge, the access, distribution, and core layers of the enterprise campus or WAN need to be secured. Cisco calls this the self-defending network, where each piece of the network is secured independently as well as at the Enterprise Edge. This change of focus is because many attacks originate from the inside of the enterprise infrastructure. This paper will focus on securing layer 2 switching at the access layer through port security and preventing denial of service (DoS) attacks at layer 2.

Risk Assessment

Security implementation should start with a risk assessment and those risks need to be weighed against the need for data or information to be able to flow through a network. For example, for security reasons some organizations make a decision to disable unused switch ports. For other organizations that might not be an appropriate choice. A large news organization like CNN may choose to not disable unused ports. Sometimes a story needs to get to air at the last minute and it would be disastrous for a reporter to be unable to feed the news report to those newscasters already on air.

Another aspect of security evaluated during the risk assessment is physical security. An example of physical security could be a badge reader. Each employee would have to swipe his or her badge before entering the building and would be required to wear the badge at all times. To enforce this, physical security could include guards at the entrance to the building and guards on every floor. The choices about how to secure layer 2 are all driven by the business objectives defined in an enterprise's security policy.

Port Security

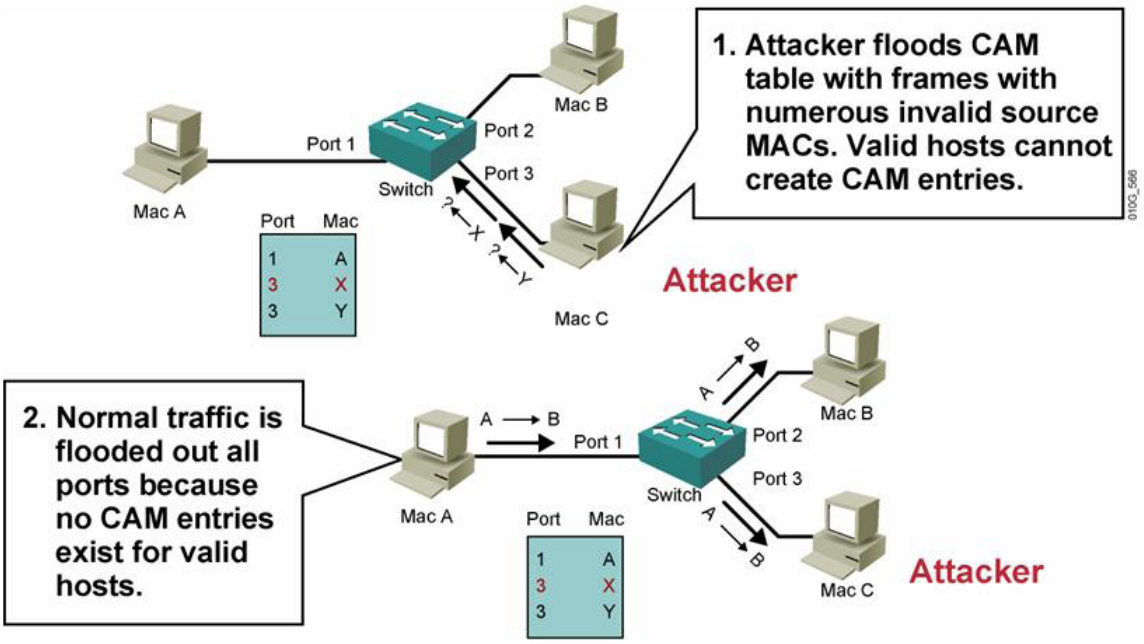
Port security allows a network administrator to limit the number of MAC addresses that are learned per switch port. A network administrator may further limit port access to a particular MAC address or set of MAC addresses.

This serves two functions:

- Ensures sure end users don't turn their cubicles into a network world by plugging in a switch or wireless device and adding multiple end devices in their cubicle.
- Prevents certain reconnaissance and denial-of-service (DoS) attacks.

A **reconnaissance attack** is one where the intruder searches for information about the network; it's similar to a military reconnaissance mission. The actual attack will take place later. A **DoS attack** is renders either a link or host unreachable.

MAC Flooding Attack

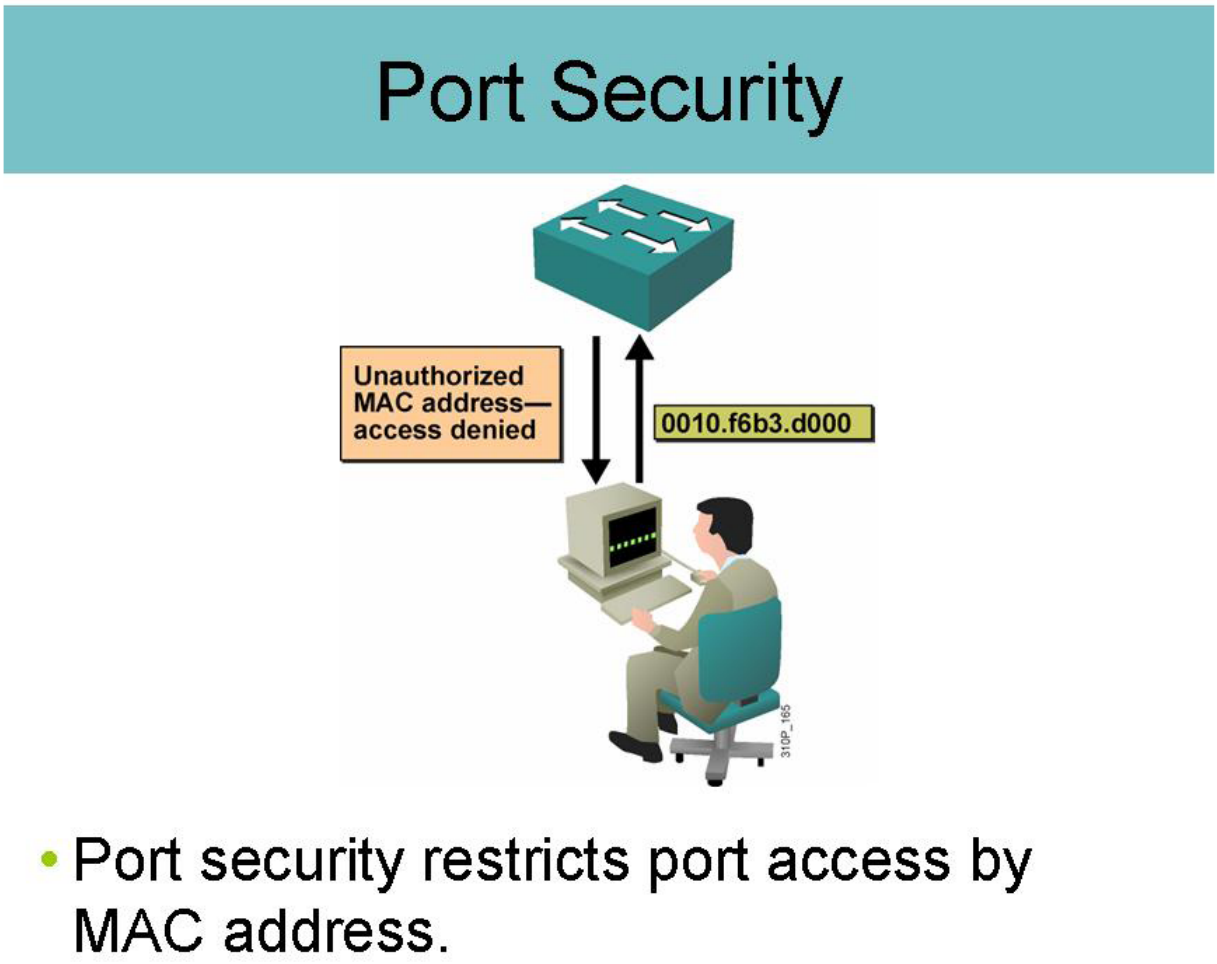


A **MAC flooding attack** is a type of reconnaissance attack. The attacker examines at the types of traffic on the LAN and may also looks for other information, such as details about default gateways. A MAC flooding attack may also be used as a DoS attack.

Before looking at the MAC flooding attack, a review of how a switch populates the MAC-Address-Table (or CAM Table) and forwards traffic would be helpful. When an Ethernet frame travels through the switch there is both a Destination MAC Address and Source MAC Address field in the Ethernet header. The switch will populate the MAC-Address-Table based on the source MAC address and its associated port. It will make forwarding decisions based on the destination MAC address. By default, if a switch does not have the destination MAC in its MAC-Address-Table, it will flood the frame out all ports—except the port it came in on. It's this behavior that the MAC flooding attack exploits.

The attacking PC floods the switch with a large number of frames, each with an invalid source MAC address. Switches have a limited amount of memory for the MAC-address-table and eventually it will be populated with all of the invalid MAC addresses from the malicious PC. When legitimate traffic is forwarded through the switch, the destination MAC addresses will not reside in the MAC-address-table and will, therefore, be forwarded out all ports, except the port it came in on. The result is that the intruder will have the opportunity to capture a considerable amount of data from the network by using a protocol analyzer on one port of the switch and record the flooded frames. In addition, if enough legitimate traffic has to be flooded out of all ports, there is a possibility that the links could become saturated, leading to a denial of service for those hosts.

One possible solution to this problem is port security.



With port security a network administrator can limit the number of MAC addresses learned on a switch port. For example: if there were one PC per port the MAC addresses count would be limited to one. If there were an IP phone and PC, the MAC address count would be limited to two. Optionally, an administrator could restrict the port to a specific MAC address.

When an administrator chooses to restrict the number of MAC addresses per port, the results of a violation can be:

Protect Frames from a non-allowed address are dropped, but there is no log of the violation.

Restrict Frames from a non-allowed address are dropped and a log message is created.

Shut Down If any frames from a non-allowed address are seen, the interface is errdisabled (shutdown). Manual intervention or errdisable recovery must be used to make the interface operational.

Configuring Port Security on a switch enables port security and specifies the maximum number of MAC addresses that can be supported by this port. It also specifies allowable MAC addresses and defines violation actions.

```
Switch(config-if)#switchport port-security [maximum value]
violation {protect | restrict | shutdown}
```

Conclusion

Port security is just one way to help secure switches at the access layer. There are other security vulnerabities such as VLAN hopping, DHCP spoofing, Address Resolution Protocol (ARP) spoofing, Secure Shell Protocol (SSH) and Telnet attacks that also need to be addressed to more completely secure layer two. But those are subjects for another white paper or a network-security class.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses.

IINS – Implementing Cisco IOS Network Security

Security+ Prep Course

Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 1,200 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and business training needs.

For more information or to register, visit www.globalknowledge.com or call 1-800-COURSES to speak with a sales representative.

About the Author

Carol Kavalla's background includes teaching at Rockland Community College in New York, managing networks and being a consultant for the NYS small business development center. For the last eight-and-a-half years, Carol has taught for Global Knowledge and is certified to teach nine Cisco Courses: ICND1; ICND2; CCDA; BSCI; BCMSN; TCN; ICMI; BGP; and ARCH. She also has a consulting firm in Charleston, South Carolina, where she works with small companies (100-200 nodes) installing, configuring routers and switches, and troubleshooting network problems.