Basic Switch Security Concepts and Configuration

By Sean Wilkins

Date: Jan 24, 2012

Return to the article

A very important part of securing an organizational network involves the layer 2 parts of the network, specifically the switches. Many people can tend to ignore the security vulnerabilities that can be exploited at layer 2, but these devices are just as vulnerable as high layer devices but are just attacked in different ways. This article takes a look at these potential threats and at the different techniques and configurations that can be used to avoid them. It should be noted that this article is not intended to show all possible switch security methods but simply highlight the most commonly referenced.

A very important part of securing an organizational network involves the Layer 2 parts of the network, specifically the switches. Many people can tend to ignore the security vulnerabilities that can be exploited at Layer 2, but these devices are just as vulnerable as high layer devices—they are just attacked in different ways. This article takes a look at these potential threats and at the different techniques and configurations that can be used to avoid them. It should be noted that this article is not intended to show all possible switch security methods but simply highlight the most commonly referenced.

Switch Port Security

The simplest form of switch security is using port level security. When using port level security, the MAC address(es) and/or number of MAC addresses of the connected devices is controlled. There are three different ways that MAC addresses can be configured onto a port:

- Statically
- Dynamically
- Sticky

A statically-configured MAC address is rather simple; a single MAC address is configured to be allowed on a port:

```
router#configure terminal
router(config)#interface interface
router(config-if)#switchport port-security mac-address mac-address
```

A dynamic MAC address is one that is learned on an interface and is held in the Content-Addressable Memory (CAM) table until it times out (5 minutes); these are enabled by default.

A sticky address is dynamically learned and then immediately converted into a sticky secure MAC address; this “sticks” the specific MAC address to this port alone. Sticky MAC addresses are lost on reboot unless the running configuration is saved.

```
router#configure terminal
router(config)#interface interface
router(config-if)#switchport port-security mac-address sticky
```

Along with configuring these different types of MAC address, a port can also be configured with a maximum number of allowed learned MAC addresses (the default is one):

```
router#configure terminal
router(config)#interface interface
router(config-if)#switchport port-security maximum maximum
```

If a port security violation should occur, there are three different methods that can be configured based on the intended device reaction:

- Protect—When using this method, the packets from the unknown source addresses will be dropped.
- Restrict—When using this method, the packets from the unknown source addresses will be dropped, AND the security violation counter will be incremented and a management message will be sent.
- Shutdown—When using this method, the port will shut down upon receipt of packets from unknown addresses, AND the

security violation counter will be incremented, and a management message will be sent. (This is the default.)

```
router#configure terminal
router(config)#interface interface
router(config-if)#switchport port-security violation {protect | restrict | shutdown}
```

Switch Port Types

When deploying a switched network, one of the first things designed is how the different ports on the switch are connected. There are three main port types:

- Access ports are intended to be connected to a host or group of hosts (but not another switch).
- Trunk ports are intended to be connected to another switch.
- Dynamic ports are able to negotiate themselves as access or trunk ports.

The main difference between access and trunk ports is that access ports are only able to exist within a single Virtual LAN (VLAN) at a time while trunk ports are able to forward traffic from multiple VLANs at once. Access ports are the port type that is configured with the Portfast and BPDU Guard features as discussed above.

```
router#configure terminal
router(config)#interface interface
router(config-if)#switchport mode access
```

Many Cisco switches default to a dynamic port type. There are two different dynamic sub-types: auto and desirable. Ports configured as auto will not try to become a trunk port unless the device on the other side initiates it. Ports configured as desirable will actively attempt to become a trunk; these negotiations are done via Dynamic Inter-Switch Link Protocol (DISL) and Dynamic Trunking Protocol (DTP):

```
router#configure terminal
router(config)#interface interface
router(config-if)#switchport mode {trunk | dynamic {auto | desirable}}
```

One method used by many engineers to secure a switch is to manually configure each port to be an access or trunk port manually and disabling DISL/DTP:

```
router#configure terminal
router(config)#interface interface
router(config-if)#switchport nonegotiate
```

Spanning-Tree Protocol (STP)

One of the protocols (or its successors) that is run on almost every Layer 2 Ethernet network is STP. STP is responsible for providing a loop-free Layer 2 network, it does this by setting up a hierarchy where a root switch is elected and is used as the focal point for the entire switched network. There are some basic rules that are followed by STP:

1. All ports on the root switch will be forwarding.
2. All other non-root switches will calculate the best switchport to reach the root switch and this port will always be forwarding.
3. Switches that have a sole connection to a LAN segment will assign the connecting port as a designated port for that segment.
4. Switches that have redundant connections to a LAN segment (or multiple switches that have a connection into the same LAN segment) will calculate the port with the best cost (to the root switch) and assign it as designated port; all other connecting ports to the LAN segment will be put into blocking mode.

It is important to note that the switch with the highest priority will become the root switch. Without any security configured, anybody with physical access to the LAN cabling could insert a switch into the topology with a higher priority and have STP change the way all LAN traffic is forwarded. Obviously, this is not something that a network administrator or engineer wants to happen; to prevent this, there are a couple of features that can be used.

> **NOTE**
>
> For a more detailed description of STP check out the “Spanning Tree Protocol Concepts and Configuration” article.

Rootguard

One feature that Cisco has developed is Rootguard; when enabled on a port, no switch connected off this port will be allowed to become the root switch. It does this by listening for superior priority advertisements; if one is received, the port will enter into

root-inconsistent state and traffic is not forwarded until the superior priority advertisements stop. The Rootguard feature can be enabled on all ports that are facing away from the planned root switch:

```
router#configure terminal
router(config)#interface interface
router(config-if)#spanning-tree guard root
```

Portfast and BPDU Guard

One of the disadvantages of STP is that it can delay the forwarding of traffic on ports that have been recently connected. The amount of delay depends on the version of STP implemented; with IEEE 802.1D (standard STP) it would be ~30 seconds. This delay is necessary when the port is connected to another switch and is intended to be a trunk, but if the port is connected to a single host device, this delay is annoying and unnecessary. A feature to disable this delay is called Portfast. When a port is enabled with Portfast, it will immediately transition to a forwarding state.

A companion feature is called BPDU guard. Because a port that is intended to be connected to a single host should not receive Bridge Protocol Data Units (BPDUs) from another switch, the BPDU feature will automatically transition the port to an err-disabled state, and manual administrator intervention is required before traffic will be allowed to be forwarded again.

```
router#configure terminal
router(config)#interface interface
router(config-if)#spanning-tree bpduguard enable
```

Summary

The security of Layer 2 should not be overlooked in any organizational network. The potential is always there that an attacker is looking to obtain access to the information contained within the organizational network and exploiting Layer 2 is one of the methods that can be used. While it can be commonly overlooked, the security of Layer 2 is at least as important as higher level device security and is probably more important as they are generally less complex to exploit. Hopefully the information contained within this article has provided a basic understanding of these features and help in securing a future Layer 2 network.
