

Week 7 – L2 Security

In this lab, you will gain familiarity with some of the security features available on Cisco switches.

What you will do:

- Part 1. Set up basic end-to-end connectivity (exact repeat from previous labs)
- Part 2. Configure SSH (exact repeat from previous labs)
- Part 3. Configure security features on (1) VLAN trunk ports and (2) access ports; disable unused ports.
- Part 4. Configure SPAN (Switched Port Analyser; ie. traffic mirroring)

Things that you will need to know or learn:

1. How VLANs work
2. How STP works; how a root bridge is elected
3. How to set up SSH on both PC and switch/router
4. How to configure, modify, and verify L2 security features for both trunk and VLAN ports using CLI

What you need to submit and when:

1. Sign your name on the board when you reach any of the checkpoints listed below in “Marks”. The lab professor will then assign each mark at that moment.
2. The post-lab quiz on BB must be completed before your next lab period.

Marks:

In order to receive the marks shown below, all network devices must have a hostname which prepends **your network id** to the hostname!

- 1 mark: Correct configuration of L2 security features on S1
- 1 mark: Correct display of SPAN activity on PC-A

15% of your final mark is for labs done during the semester. Although the number of marks will vary from lab to lab, each lab is weighted equally in the final lab total.

References and Resources:

- Harddrive and network cables (crossover, straight-thru)
- Cisco CCNAS Chapter 6 Lab (available on Blackboard)
- putty SSH client: www.chiark.greenend.org.uk/~gtatham/putty/download.html
- SuperScan: <http://www.foundstone.com>

General Comments

- This lab consists of working only on switches (the router is just a target). Decide what will help you learn the most: working individually on a set of switches or as a pilot & co-pilot team (repeating the lab once for each partner).
- Make sure you have **all the software you need for this lab** before disconnecting from the main college network!
- We have a variety of switches available in T108: only one of your switches may be a 2950/2960! The other should be a 3550 or a 3560.
- Note that the ethernet ports on Cisco 2950 and 3950 switches are **not** auto MDI/MDI-X. You need to use the correct type of cables to get them to work! (Ref: <http://cisco-network.com/do-you-know/cisco-auto-mdi-mdix-switch-support-matrix/>)
- I can't guarantee that the switches in T108 will have the required IOS version to support SSH. If you confirm that your switch doesn't support SSH, skip the remainder of Part 2 and continue with telnet.
- There is only one lab period scheduled for this lab. Fortunately you can use Packet Tracer to practice this lab.
- It is highly recommended that you keep a log book of all (new) commands that you use (in this and every subsequent lab) along with a brief 1-line description of what each command does.

Some commands required for this lab

Global config:

```
ip domain-name {domain_name}
username admin privilege {0..15} secret {pswd}
crypto key generate rsa general-keys modulus 1024
ip ssh time-out {secs}
ip ssh authentication-retries {num}
spanning-tree vlan {1-4094} priority {priority}
show spanning-tree inconsistentports
default interface {interface}
interface range {i/f} - {last_val}          [eg.fa0/2-4]
monitor session {num} source interface {i/f} [both]
monitor session {num} destination interface {i/f}
```

Specific config mode (applied to an interface)

```
switchport mode {access | trunk}
switchport trunk native vlan {1-4094}
switchport nonegotiate
storm-control broadcast level {percentage}
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree guard root
switchport access vlan {vlan_num}
switchport port-security
switchport port-security maximum {num}
switchport port-security violation {action}
switchport port-security mac-address {MAC_addr}
switchport port-security mac-address sticky
switchport port-security aging time 120
mac-address {MAC_addr}
```