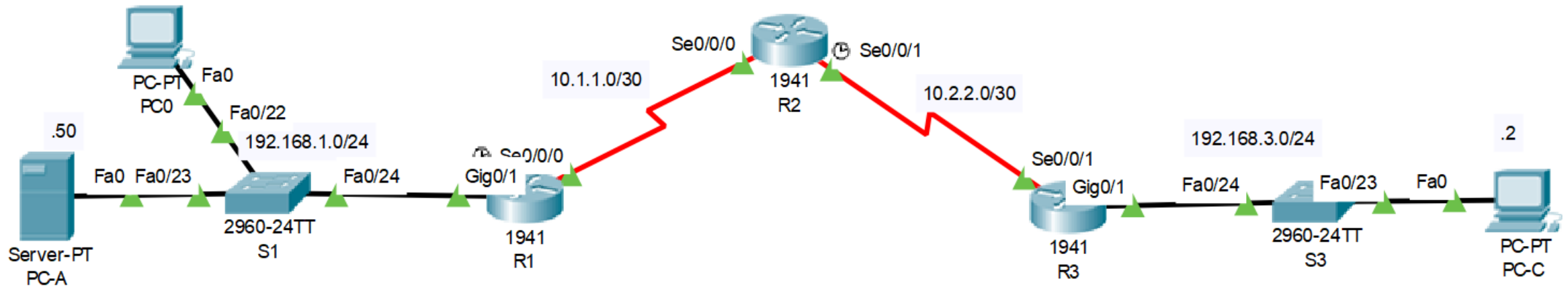
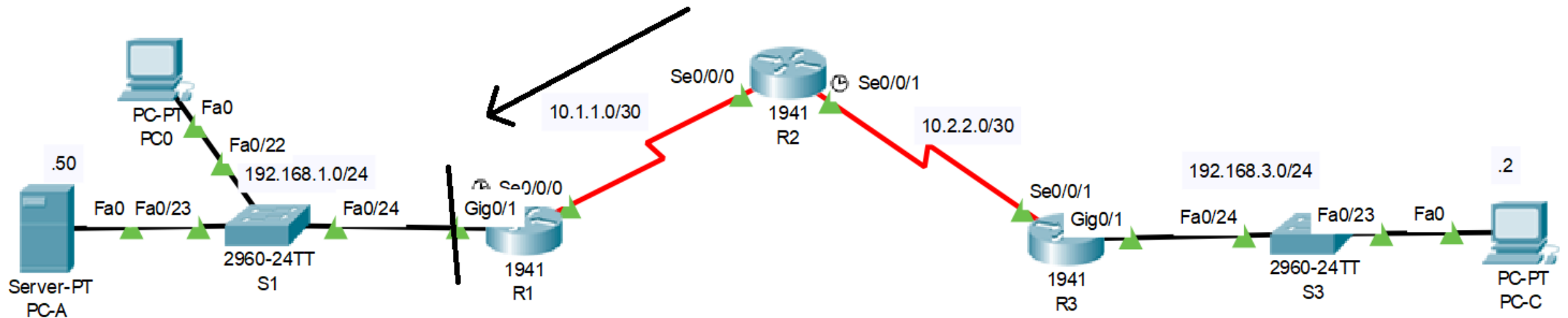


Lab 8 IOS IPS usando CLI



R1(config)# license boot module c1900 technology-package securityk9



Crear directorio de configuración y regla

Directorio

- **R1# mkdir ipsdir**
- **R1(config)# ip ips config location flash:ipsdir**

Regla

- **R1(config)# ip ips name iosips**

Habilitar logs

- **R1(config)# ip ips notify log**
- **R1# clock set 10:20:00 16 july 2019**
- **R1(config)# service timestamps log datetime msec**
- **R1(config)# logging host 192.168.1.50**

Categorías de firmas

“Cisco IPS contiene más de 10,000 firmas predeterminadas incorporadas.

No puede renombrar o eliminar firmas de la lista de firmas incorporadas, pero puede retirar firmas para eliminarlas del motor de detección.”

Configurar categoría de firmas

- **R1(config)# ip ips signature-category**

Retirar todas las categorías

- **R1(config-ips-category)# category all**
- **R1(config-ips-category-action)# retired true**
- **R1(config-ips-category-action)# exit**

Agregar solamente la categoría básica

- **R1(config-ips-category)# category ios_ips basic**
- **R1(config-ips-category-action)# retired false**
- **R1(config-ips-category-action)# exit**

Aplicar regla a la interfaz

- **R1(config)# interface g0/1**
- **R1(config-if)# ip ips iosips out**

Cambiar acción de la firma

- **R1(config)# ip ips signature-definition**
- **R1(config-sigdef)# signature 2004 0**
- **R1(config-sigdef-sig)# status**
- **R1(config-sigdef-sig-status)# retired false**
- **R1(config-sigdef-sig-status)# enabled true**
- **R1(config-sigdef-sig-status)# exit**
- **R1(config-sigdef-sig)# engine**
- **R1(config-sigdef-sig-engine)# event-action produce-alert**
- **R1(config-sigdef-sig-engine)# event-action deny-packet-inline**
- **R1(config-sigdef-sig-engine)# exit**
- **R1(config-sigdef-sig)# exit**




Search bar with magnifying glass icon

Home / Cisco Security / Latest Threat Information / Search Cisco Intrusion Prevention System Signatures

Cisco Security

ICMP Echo Request

Signature ID: 2004/0
 Original Release: S1
 Release: [S666 \(download\)](#)
 Original Release Date: 2000 November 27
 Latest Release Date: 2012 September 11
 Default Enabled: False
 Default Retired: False

Alarm Severity: Informational 
 Fidelity: 100

Powered by **IntelliShield**

Related Links

Solutions

- [Security Solutions](#)
- [E-mail Security](#)
- [Threat Control for Endpoints](#)
- [Threat Control for Infrastructure](#)

Products & Services

- [Security Services](#)
- [Security Products](#)
- [Cisco IntelliShield Alert Manager](#)

Description

Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 8 (Echo Request).ICMP Echo Requests are commonly used to perform reconnaissance sweeps of networks. These sweeps often are a prelude to attack. Additionally they may be used to perform denial of service attacks.

Recommended Filter