|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DATOS DE LA ACTIVIDAD | | | | | | | |
| No. de Actividad: | **2.5** | **Práctica 3** | Configurar IP ACL para mitigar ataques | | | | |
| Unidad: | 2: Configuración de seguridad en firewall, Switches, Routers y Access point | | | | | | |
| Carrera: | Tgo. en Desarrollo de Software | | | | | | |
| Materia | **SEGURIDAD EN ITI** | | | | | Clave | MPF3608DSO |
| Profesor: | Andrés Figueroa Flores | | | | | | |
| Alumno: | David Alejandro López Torres | | | | | Registro: | 17300155 |
| Institución: | **Centro de Enseñanza Técnica Industrial plantel Colomos** | | | | | | |
| Semestre: | 8 | Grupo: | D1 | Período: | Feb-Jun 2021 | Fecha: | 23/04/2021 |
| Compet. Genéricas | | 4.1, 4.5, 5.2, 5.5 | | Compet. Profesional | | CP1-1 | |

**1. Objetivo(s) de la actividad**

* Aplicar los tipos de listas de control de acceso.

**2. Introducción**

Los controles de acceso son soluciones de hardware y software que se utilizan para administrar el acceso a recursos y a los sistemas, las listas de control de acceso (ACL) definen el tipo de tráfico permitido en una red informática.

**3. Objetivos**

* Verificar la conectividad entre los dispositivos antes de la configuración del firewall.
* Utilizar las ACL para garantizar que el acceso remoto al router está disponible sólo desde la estación de administración de PC-C.
* Configurar ACL en Router 1 y Router 3 para mitigar los ataques.
* Verificar las funciones ACL en esta página.

**4. Instrucciones (Descripción) de la actividad**

1. Usar el archivo de ejemplo de prácticas para realizar el reporte esta actividad.
2. Tomar impresiones de pantalla completa de la actividad, (recuerda ir haciendo las impresiones conforme vas realizando la práctica en el simulador) , con tu nombre en la impresión.
3. Subir el reporte terminado de WORD y el archivo de PACKET TRACERT, dar clic para marcar como entregada la actividad.

**4. Resumen**

**Listas de acceso estándar**

Las listas de acceso IP estándar comprueban las direcciones de origen de los paquetes que solicitan enrutamiento. El resultado es el permiso o la denegación de la salida del paquete por parte del protocolo, basándose en la dirección IP de la red-subred-host de origen.

**Listas de acceso extendidas**

Las listas de acceso extendidas controlan el tráfico por la comparación de las direcciones de origen y de destino de los paquetes IP a las direcciones configuradas en la ACL.

**Listas de acceso reflexivas**

Permiten que se filtren los paquetes IP según la información de sesión de capa superior. Generalmente, se utilizan para permitir el tráfico saliente y para limitar el tráfico entrante en respuesta a las sesiones que se originan dentro del router. Solo se pueden definir con ACL con nombre IP extendidas.

**Listas de acceso dinámicas**

La configuración de cerradura y llave comienza con la aplicación de una ACL extendida para bloquear el tráfico a través del router. Los usuarios que desean atravesar el router son bloqueados por la ACL extendida hasta que realicen una conexión Telnet al router y sean autenticados. Luego, la conexión Telnet se pierde y se agrega una ACL dinámica de una única entrada a la ACL extendida existente. Esto permite el tráfico por un período de tiempo determinado; son posibles los tiempos de espera inactivo y absoluto

**Listas de acceso basadas en tiempo**

Se crea un intervalo de tiempo que define las horas específicas del día y de la semana para implementar las ACL basadas en El intervalo de tiempo se identifica con un nombre y luego se remite a él a través de una función. Por lo tanto, las restricciones de tiempo se imponen en la misma función. El intervalo de tiempo depende del reloj del sistema del router. Se puede utilizar el reloj del router, pero la función funciona mejor con la sincronización de Network TimeProtocol (NTP).

**Referencias**

Configuración de Listas de Acceso IP. Recuperado el 22/04/2021 de: <https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.pdf>

**5. Material y Equipo**

• Computadora

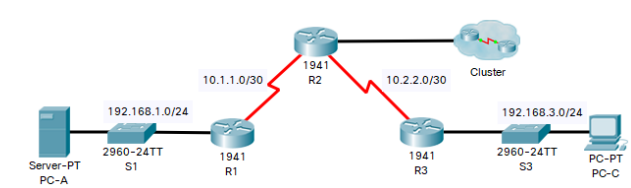
• Acceso a Packet Tracer

**6. Desarrollo**

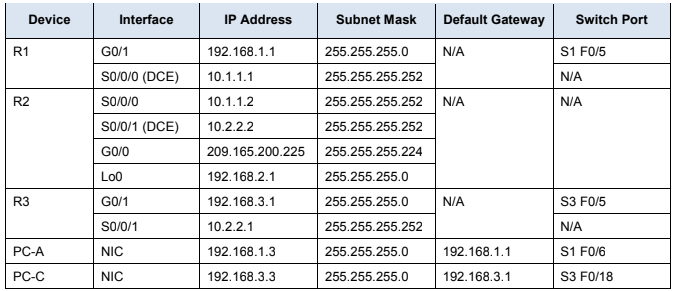
• Tabla de Comandos

|  |
| --- |
| **Tabla de Comandos** |
| access-list access-list-number {permit|deny} {host|source source-wildcard|any} |
| ip access-group nº in|out |
| access-list nº permit|deny origen [wild-mask] |
| access-list nº permit|deny protocolo origen [wild-mask][operación] [puerto origen] destino [wild-mask][operación] [puerto destino][established] |
| ip access-group nº in|out |
| **ip access-list[standard|extended][nombre]** |
| **[permit|deny][condiciones de prueba]** |
| **no[permit|deny][condiciones de prueba]** |
| **Interfaz asociación de la ACL** |
| **ip access-group[nombre][in|out]** |
| ip access-list extended name permit protocol any any reflect name [timeoutseconds] |
| ip access-group {number|name} {in|out |
| ip access-list extended name evaluate name |
| username user-name password password interface <interface> ip access-group {number|name}{in|out} |
| access-list access-list-number dynamic name {permit|deny} [protocol] {source source-wildcard|any} {destination destination-wildcard|any} [precedence precedence][tostos][established] [log|log-input] [operator destination-port|destination port] |
| “Rango de tiempo”: time-range time-range-name  “Tiempo periódico”: periodic days-of-the-week hh:mm to [days-of-the-week] hh:mm  “Tiempo absoluto”: absolute [start time date] [end time date]  “Usado en la ACL”: ip access-list name|number <extended\_definition>time-rangename\_of\_time-range |
| access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny|permit} protocolsource source-wildcard destination destination-wildcard [precedence precedence] [tos tos][log|log-input] [time-range time-range-name] |
| access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny|permit} udp sourcesource-wildcard [operator [port]] destination destination-wildcard [operator [port]] [precedenceprecedence] [tos tos] [log|log-input] [time-range time-range-name] |
| access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny|permit} tcp sourcesource-wildcard [operator [port]] destination destination-wildcard [operator [port]][established] [precedence precedence] [tos tos] [log|log-input] [time-range time-range-name] |
| access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny|permit} protocolsource source-wildcard destination destination-wildcard [precedence precedence] [tos tos][log|log-input] [time-range time-range-name] |

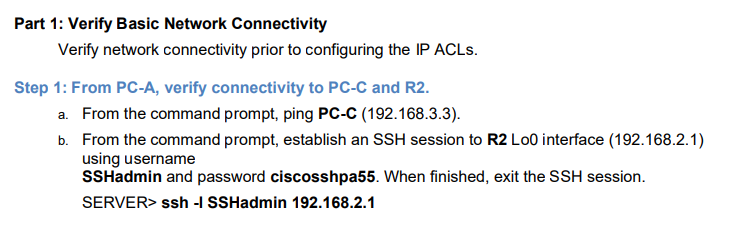
• Topología

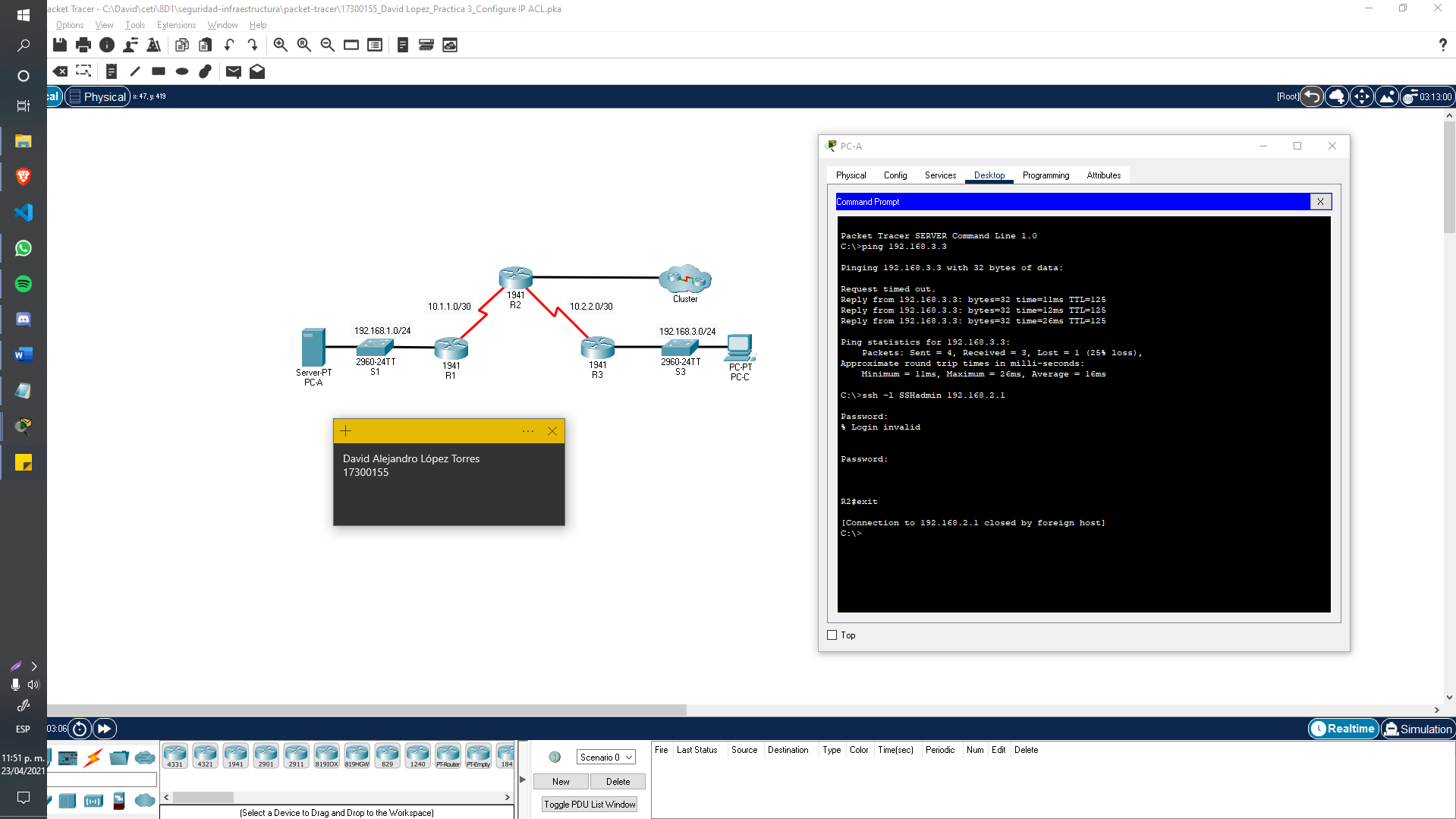
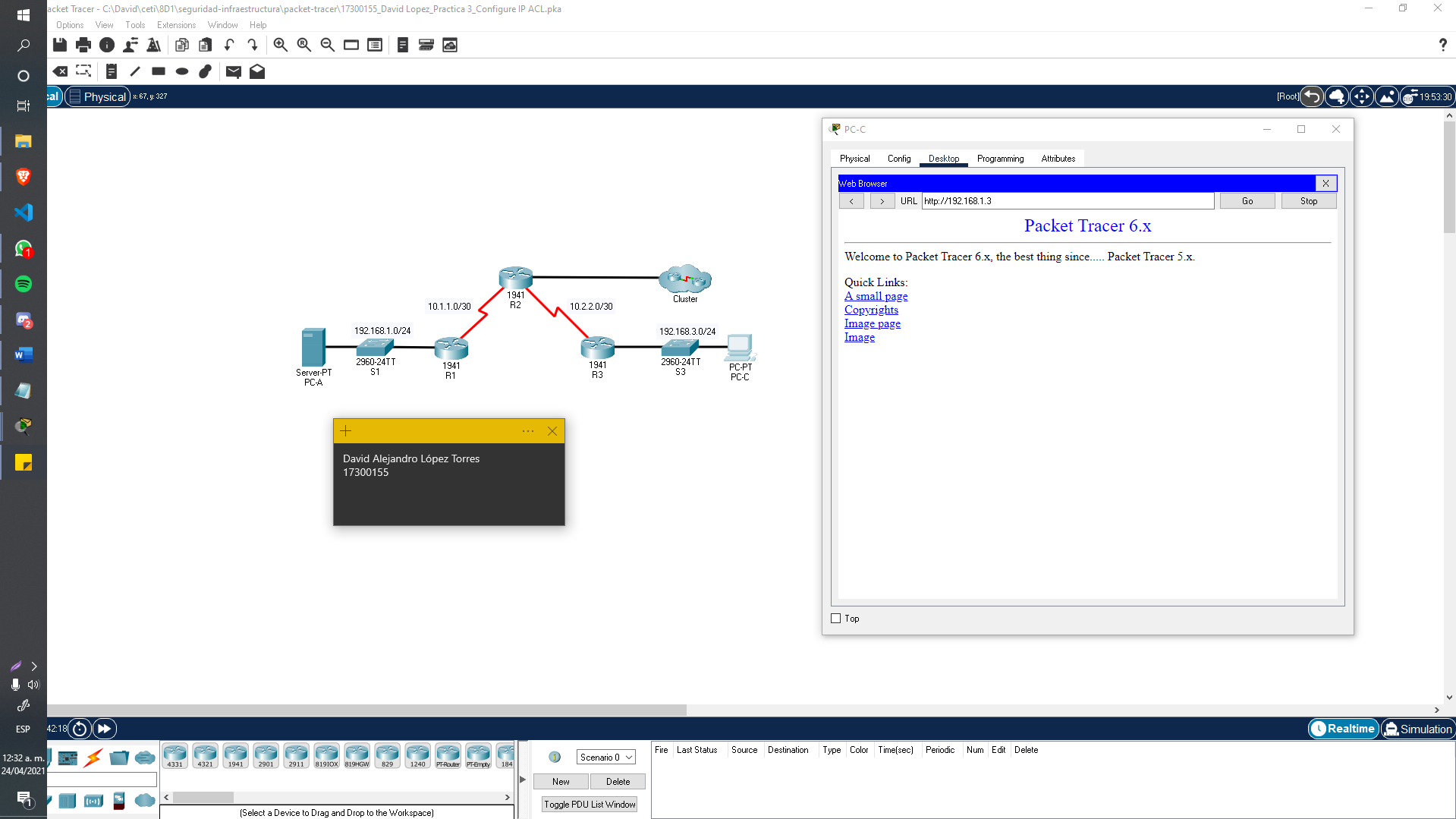


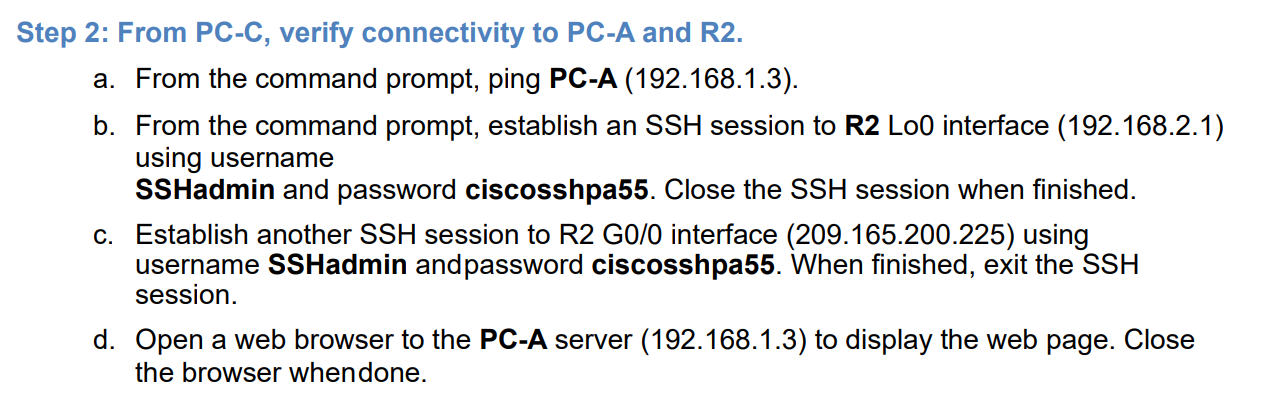
• Tabla de configuración básicas

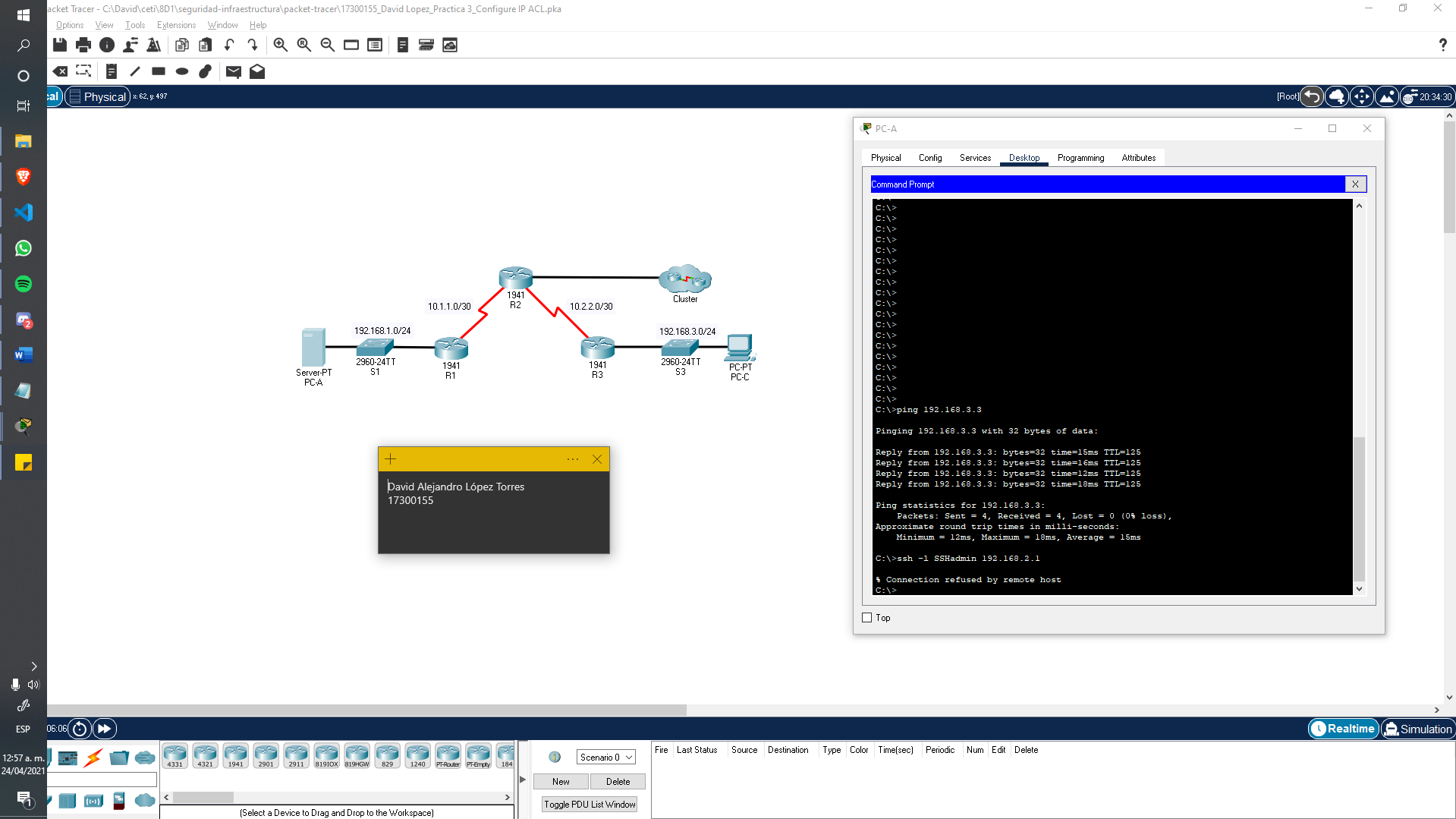
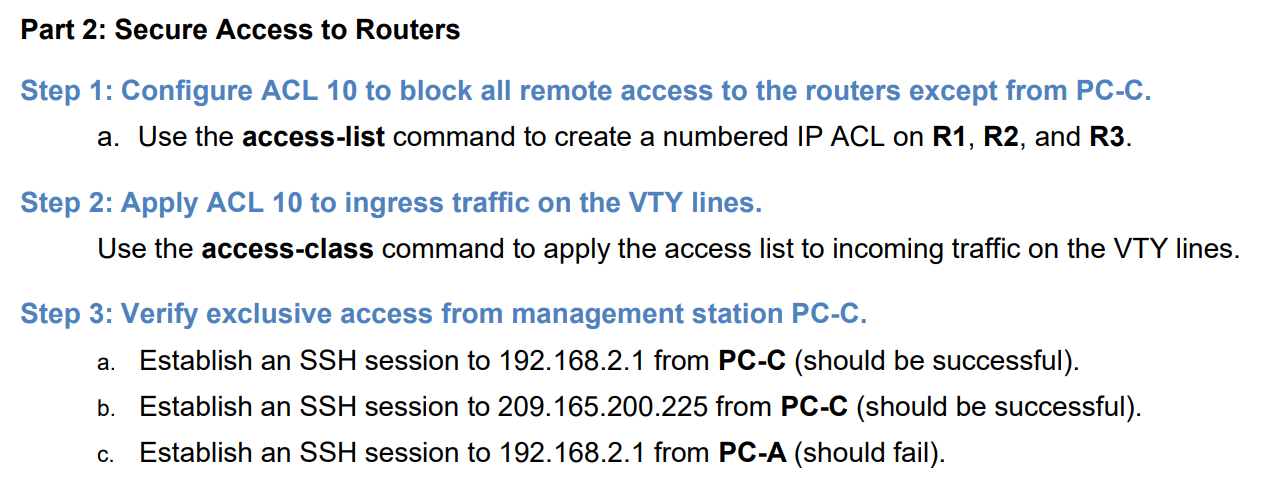


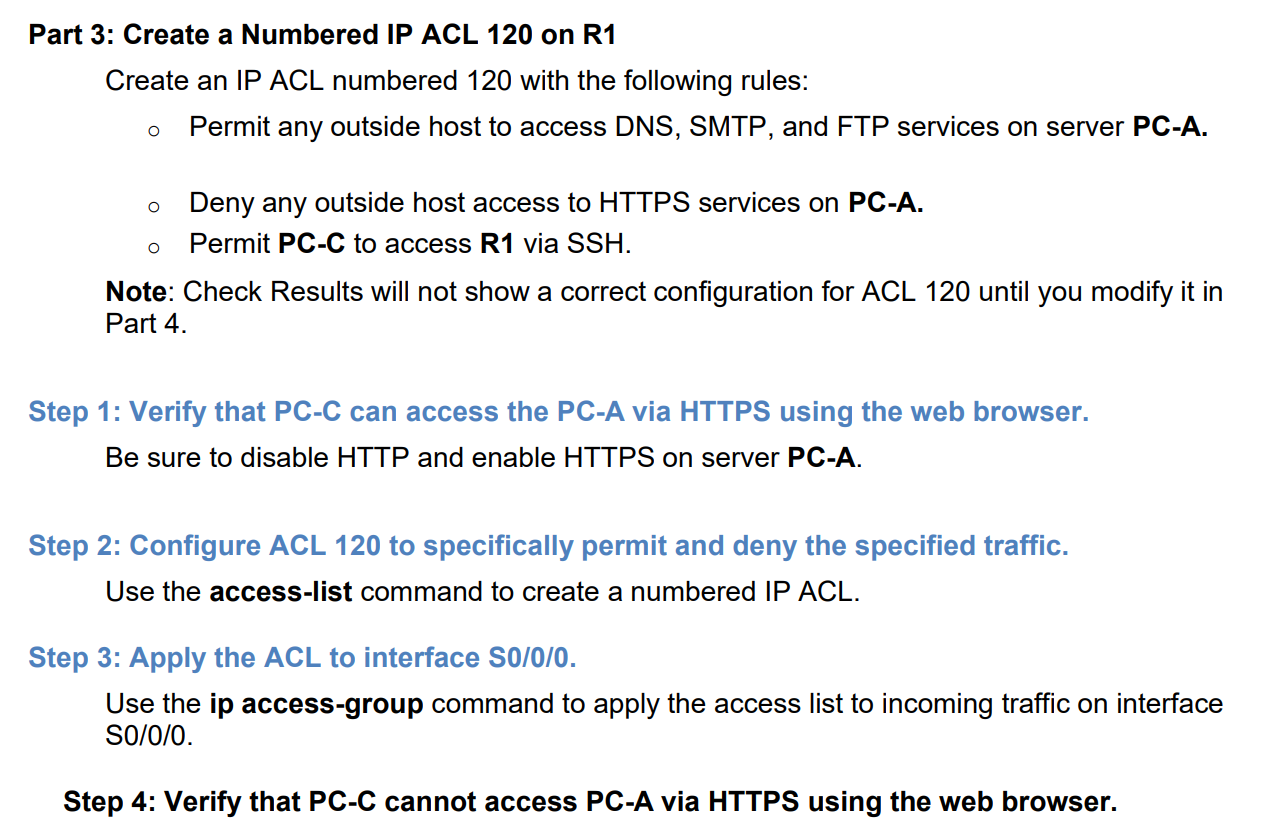
• Procedimiento

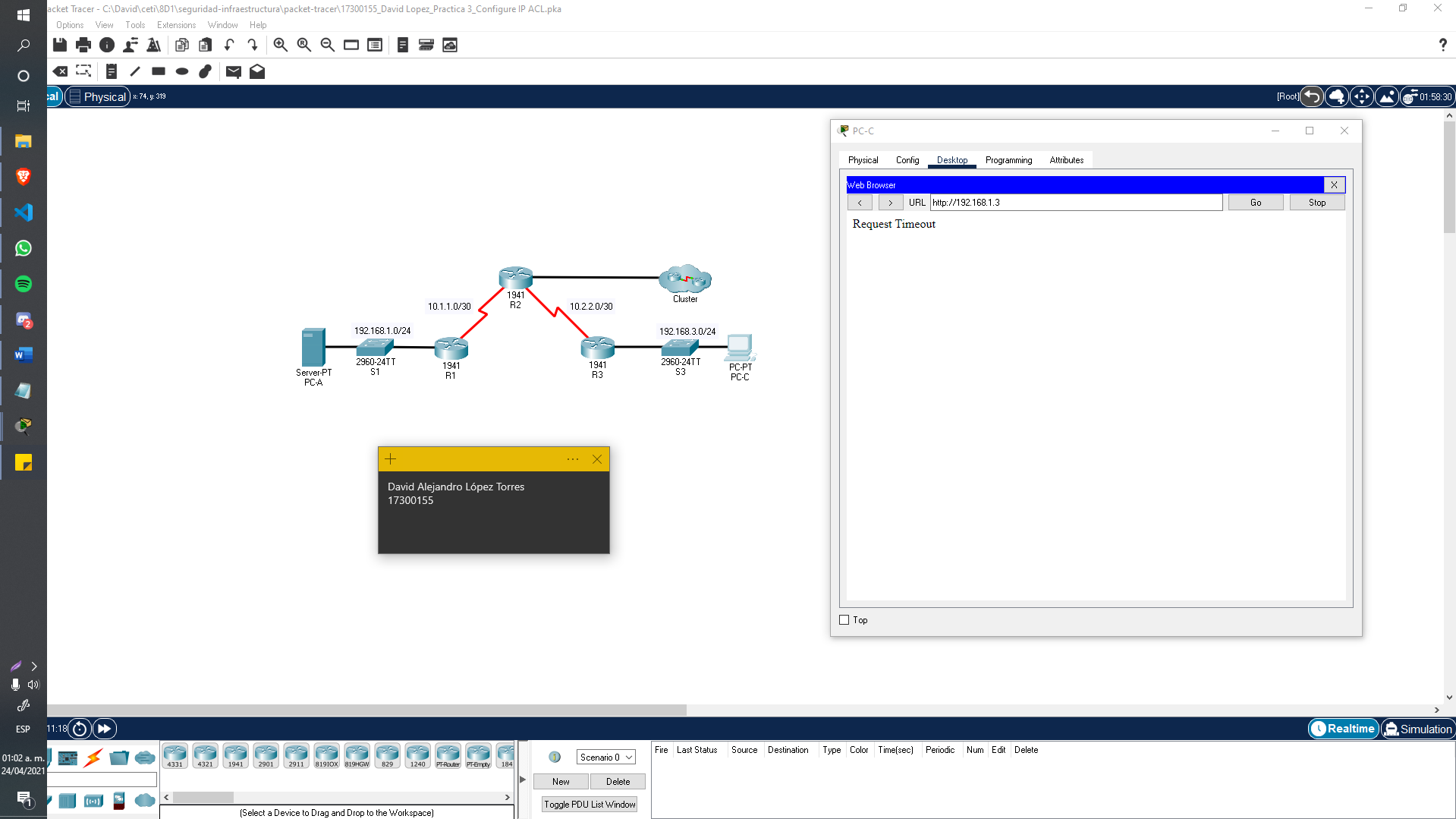
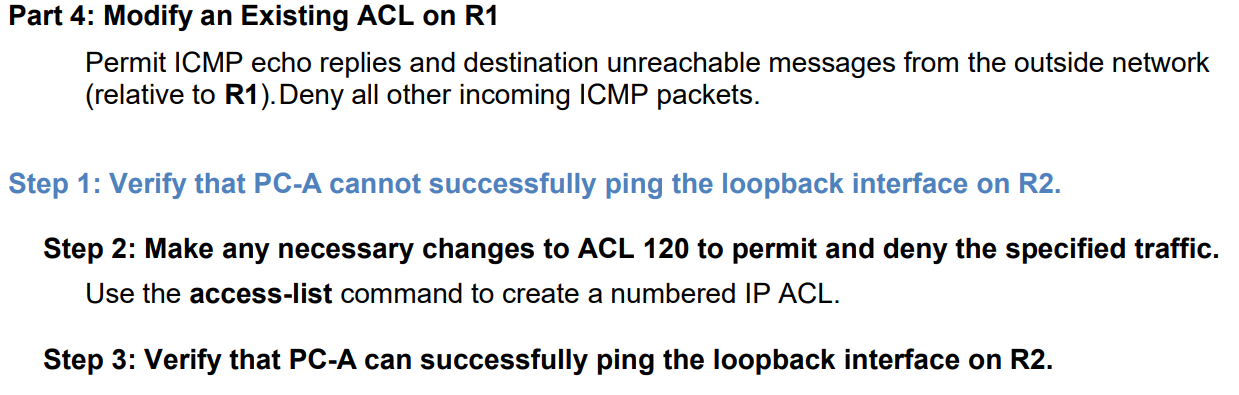
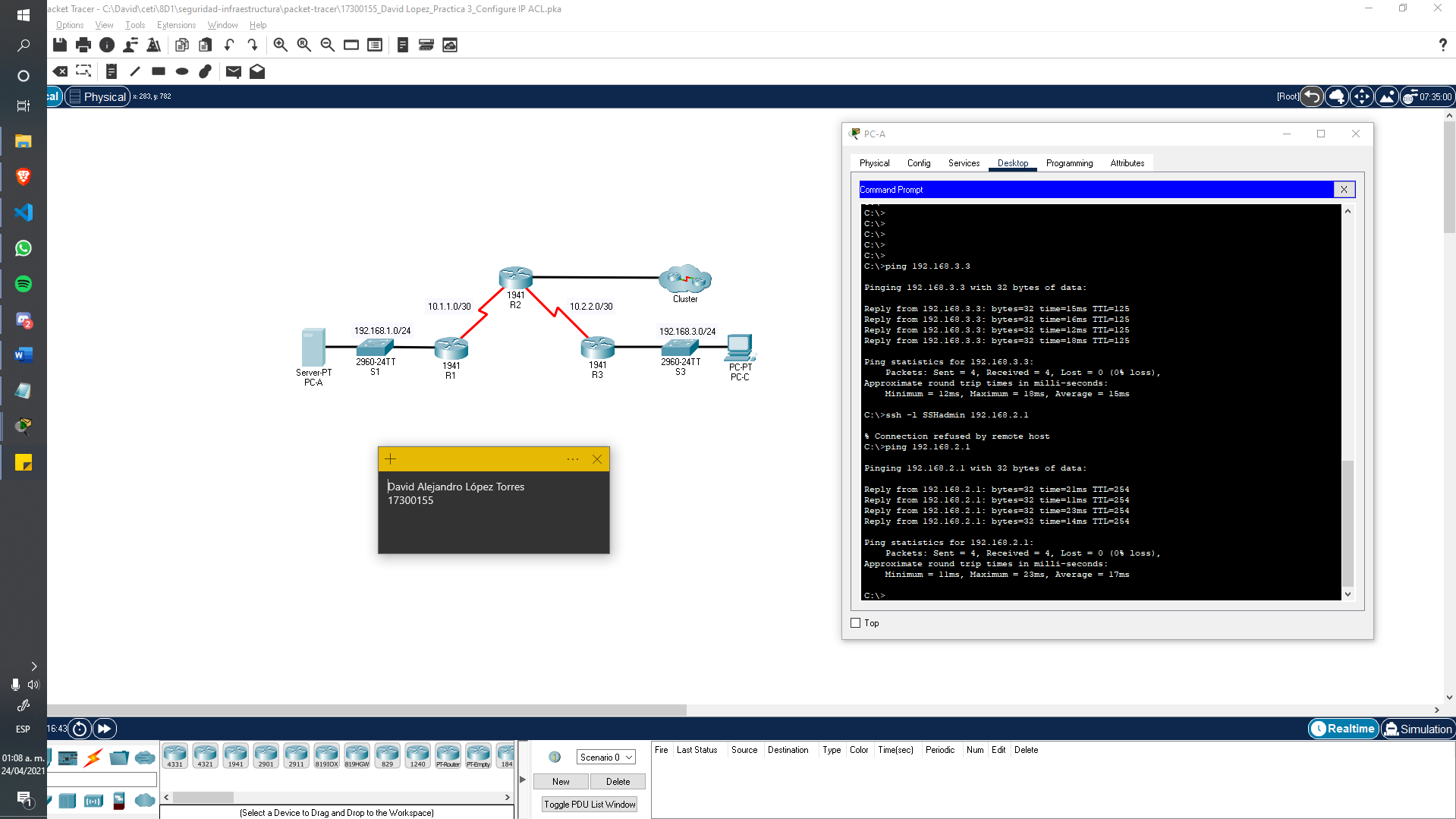


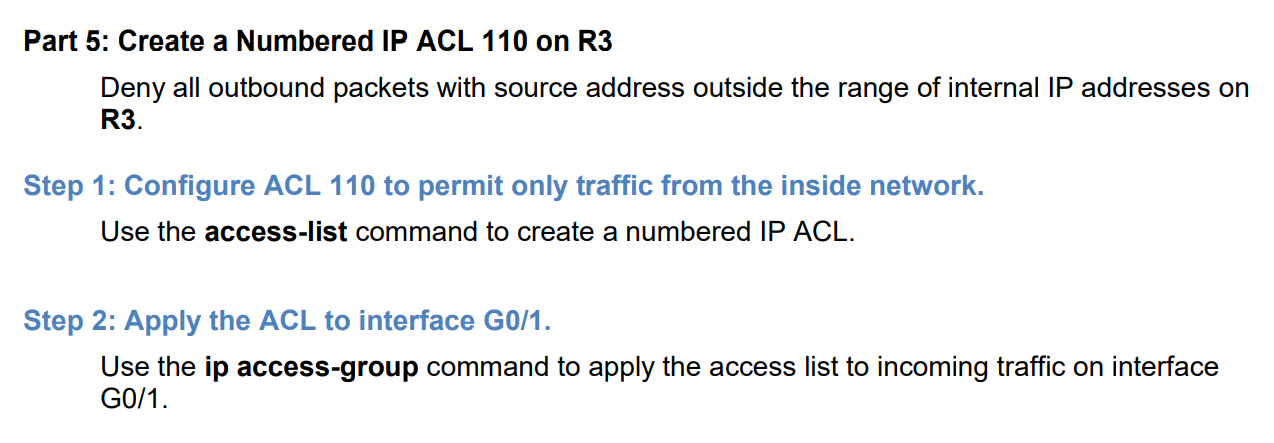
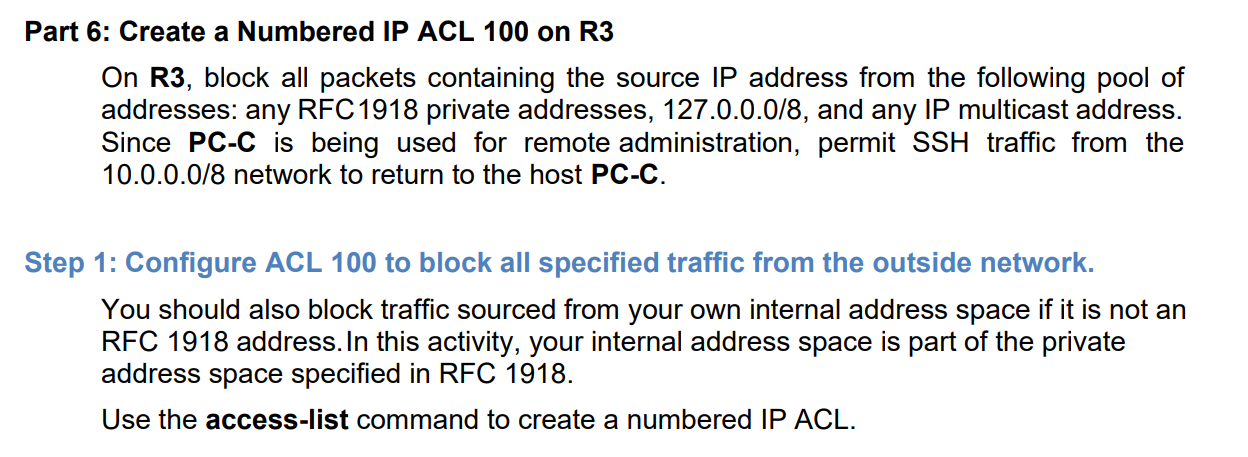
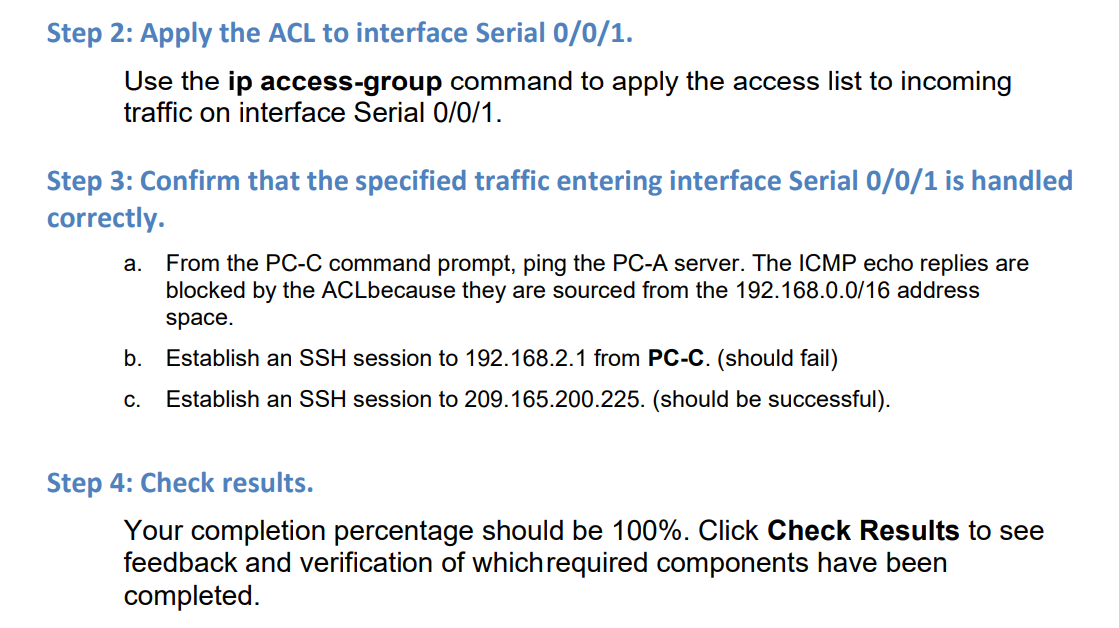


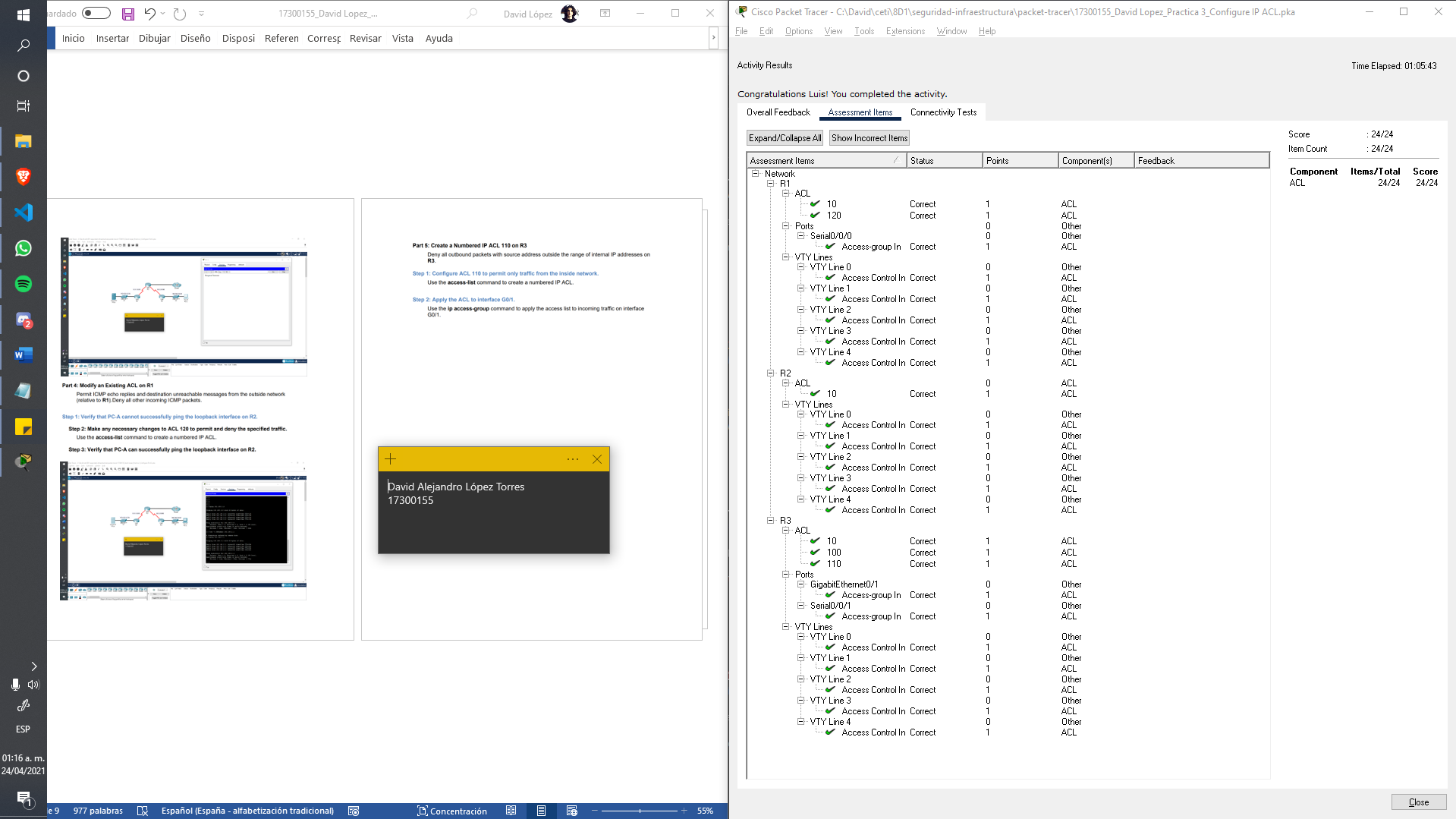












**7. Observaciones**

Es recomendable contar con un directorio de puertos conectados y su relación con los dispositivos finales, de maneta que la administración por listas de control sea más intuitiva, dinámica y más eficiente; en particular, cuando se tiene una gran cantidad de dispositivos involucrados en la lista de acceso.

**8. Conclusiones**

La implementación de listas de accesos requiere de una particular atención en los pequeños detalles, pues un pequeño error de gestión puede representar un gran obstáculo para el desarrollo de las actividades propias de la empresa donde se implementa. Además, tener un orden estricto en la designación de permisos facilita la gestión y mantenimiento de la red y en particular del apartado correspondiente a las listas de acceso. A pesar de estar consideraciones, las ACLs constituyen en gran medida una herramienta base para garantizar la eficiencia de la red y el control del tráfico de la red. Pudimos ver como la implementación es realmente simple si se siguen los consejos que se nos han dado acerca de la gestión de las listas de accesos.

**9. Referencias**

Configuración de Listas de Acceso IP. Recuperado el 22/04/2021 de:

<https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.pdf>