**Trabajo de laboratorio N2**

**OBJETIVOS**

1. Identificar las principales amenazas y vulnerabilidades de las comunicaciones de datos que deben considerarse en implementaciones de redes IEEE.802.11x.

2. Incorporar habilidades para configurar dispositivos de acceso e interfaces de hardware (adaptadores) en redes WLAN.

3. Comprender el enfoque recomendado por los estándares de gestión de seguridad de la información para establecer políticas de comunicaciones seguras y hacerlas efectivas mediante los servicios de seguridad adecuados en redes Wireless LAN (WLAN).

**TAREAS PRELIMINARES (EXTRA CLASE)**

1. Elaborar un listado de posibles amenazas a la seguridad de WLAN IEEE 802.11.

**TEORIA**

1. <https://www.wi-fi.org/discover-wi-fi/security>

Wi-Fi Protected Access

WPA3 adds new features to simplify Wi-Fi security, enable more robust authentication, deliver increased cryptographic strength for highly sensitive data markets, and maintain resiliency of mission critical network

WPA3-Personal

WPA3-Personal brings better protections to individual users by providing more robust password-based authentication. This capability is enabled through Simultaneous Authentication of Equals (SAE), which replaces Pre-shared Key (PSK) in WPA2-Personal. The technology is resistant to offline dictionary attacks.

WPA3-Enterprise

WPA3-Enterprise also offers: Authenticated encryption, Key derivation and confirmation, Key establishment and authentication, Robust management frame protection.

Open WIFI

Wi-Fi Enhanced Open™ networks provide unauthenticated data encryption to users, an improvement over traditional open networks with no protections at all. Wi-Fi Enhanced Open benefits users by providing data encryption that maintains the ease of use of open networks, and benefits network providers because there are no public passphrases to maintain, share, or manage.

1. GUIDELINES FOR SECURING WIRELESS LOCAL AREA NETWORKS (WLANS)

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf>

A wireless local area network (WLAN) is a group of wireless networking devices within a limited geographic area, such as an office building, that exchange data through radio communications. WLAN technologies are based on the IEEE 802.11 standard.

The security of each WLAN is heavily dependent on how well each WLAN component—including client devices, APs, and wireless switches—is secured throughout the WLAN lifecycle, from initial WLAN design and deployment through ongoing maintenance and monitoring.

Organizations should implement the following guidelines to improve the security of their WLANs:

* Have standardized security configurations for common WLAN components, such as client devices and Aps: Standardized configurations can also significantly reduce the time and effort needed to secure WLAN components and verify their security.
* When planning WLAN security, consider the security not only of the WLAN itself, but also how it may affect the security of other networks: For WLANs that need wired network access, their client devices should be allowed access only to the necessary hosts on the wired network using only the required protocols. Also, an organization should have separate WLANs if there is more than one security profile for WLAN usage.
* Have policies that clearly state which forms of dual connections are permitted or prohibited for WLAN client devices, and enforce these policies through the appropriate security controls: The term “dual connected” generally refers to a client device that is connected to both a wired network and a WLAN at the same time.
* Ensure that the organization’s WLAN client devices and APs have configurations at all times that are compliant with the organization’s WLAN policies: Ensure that the organization’s WLAN client devices and APs have configurations at all times that are compliant with the organization’s WLAN policies.
* Perform both attack monitoring and vulnerability monitoring to support WLAN security: Identifying patches and applying them, and verifying security configuration settings and adjusting them as needed.
* Conduct regular periodic technical security assessments for the organization’s WLANs.

1. Wireless Network Security Threats, Vulnerabilities and Their Defences

<http://article.sciencepublishinggroup.com/html/10.11648.j.ajomis.20170201.11.html>

* Changing Default SSID: Administration Set Identifier (SSID)
* Utilize VPN: This kind of execution gives high security to the remote system usage without adding noteworthy overhead to the clients.
* Utilize Static IP: By incapacitating DHCP and doling out static IP locations to every remote client, you can minimize the likelihood of the programmer acquiring a legitimate IP address.
* Tool - AirDefense likewise has the ability to find vulnerabilities and dangers in a WLAN, maverick APs and specially appointed systems as examples.
* Tool - Minimize Radio Wave Propagation in Non-user Areas.

**LABORATORIO**

1. Caso de Estudio

1. Cada grupo de alumnos deberá configurar sólo un segmento wireless, para satisfacer las necesidades de comunicaciones WLAN seguras para los integrantes de su Grupo.
2. En cada WLAN solo habrá una PC Administración con acceso web HTTPS seguro.
3. El ambiente de red será integrado por los Grupos de Usuarios 1, 2 y 3, mediante redes WLAN seguras por segmento, dedicadas SOLAMENTE a usuarios de su Grupo. Todos los segmentos WLAN están comunicados en un único segmento LAN. Los usuarios de cada Grupo sólo podrán acceder a la WLAN respectiva. Las direcciones de red de cada Grupo serán 172.16.1.0/24, 172.16.2.0/24 y 172.16.3.0/24, respectivamente. Contraseña de acceso a todas las WLAN: r3dr2d2
4. La Política General de Seguridad de la Información será del tipo RESTRICTIVA: “Todo lo que no está permitido, está prohibido”.

* Las PCs sólo podrán comunicarse dentro de la WLAN respectiva, pero no mediante la WLAN de otro Grupo.
* El Dispositivo M representa un usuario móvil que se comporta como intruso. Las intrusiones pueden realizarse en cualquiera de las WLANs. Se asume conocida la contraseña de acceso a la WLAN.

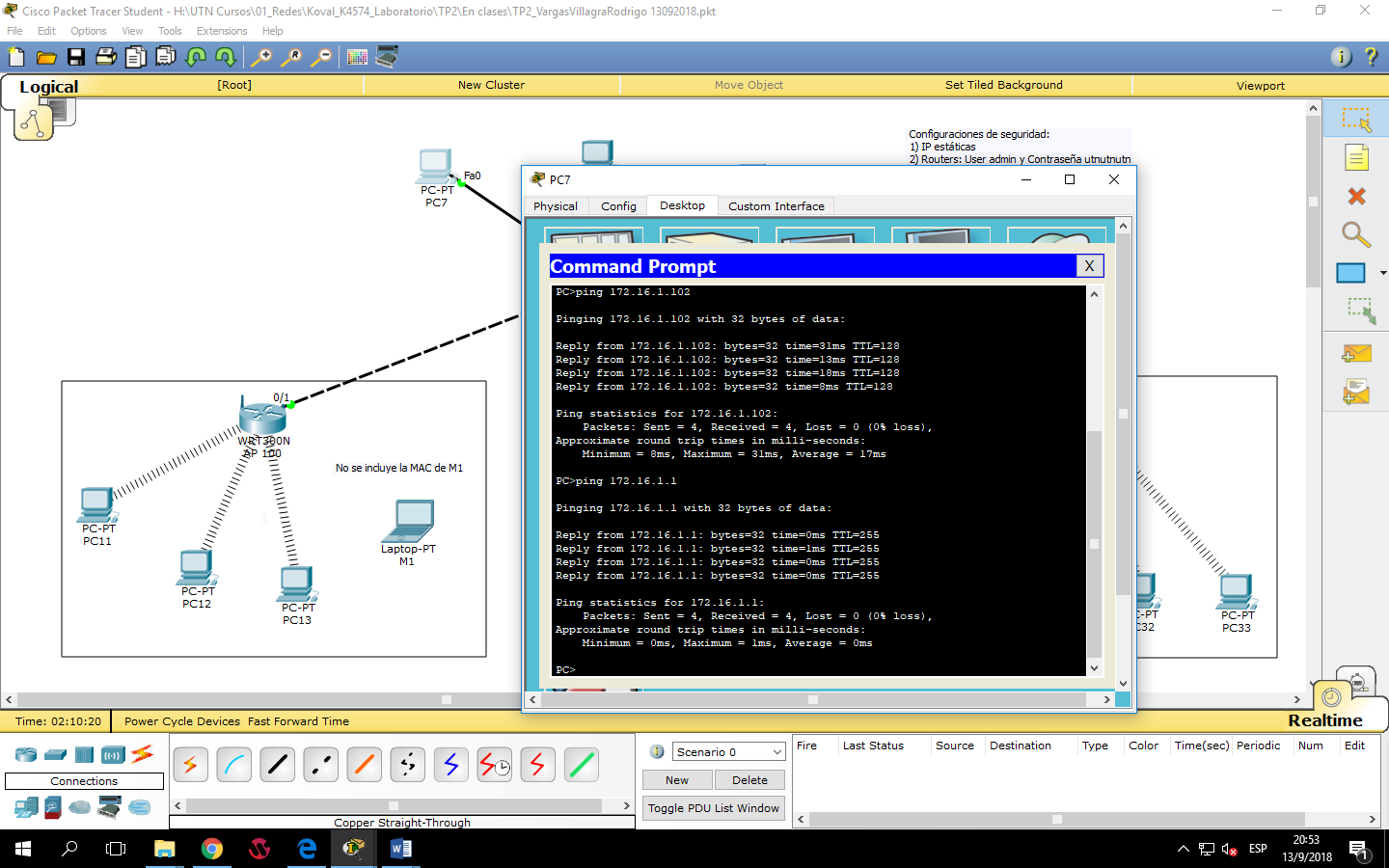
1. Se empleará como guía técnica de configuración del AP el documento Securing your Linksys WRT54G.

**Requerimientos para el alumno (Objetivos Técnicos)**

Demostrar el funcionamiento de la red, sus dispositivos y equipos en los siguientes puntos de verificación:

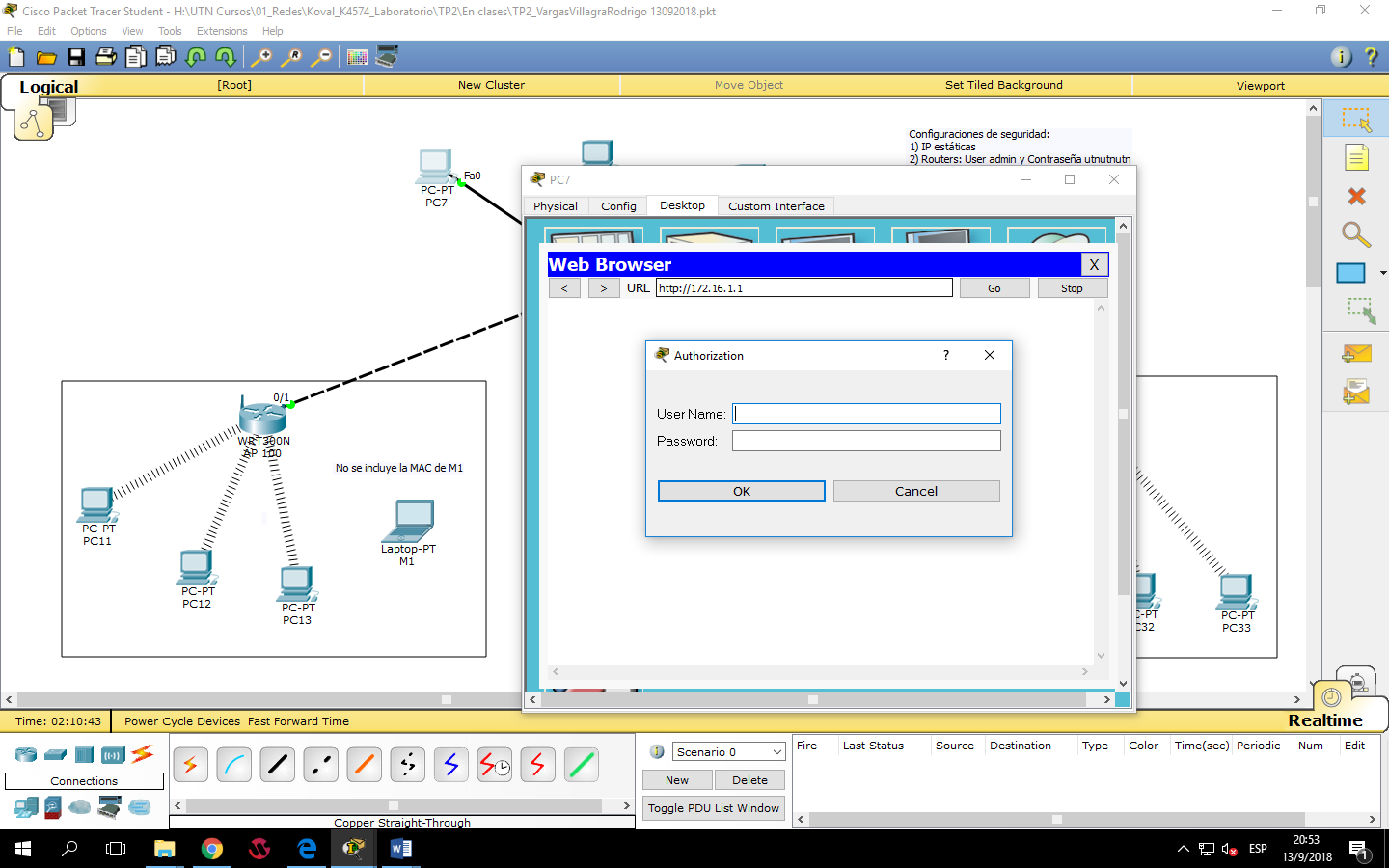
1) Acceso HTTPS desde la PC Administración al AP respectivo. OK

*Conexión entre Admin 1 y Router 100*

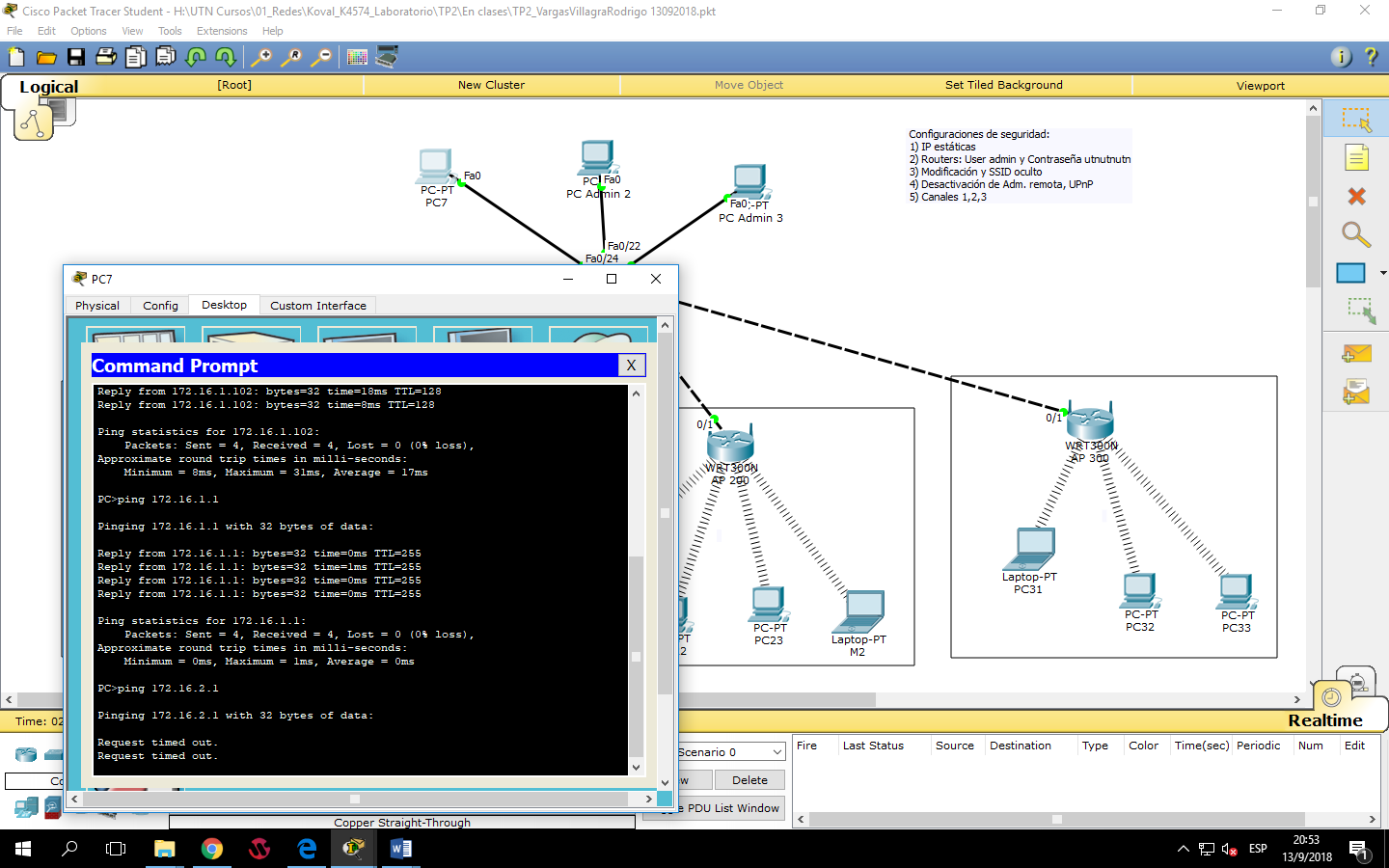


2) Restricción de acceso web para toda otra PC. OK

*Acceso de Admin 1 al router por web*

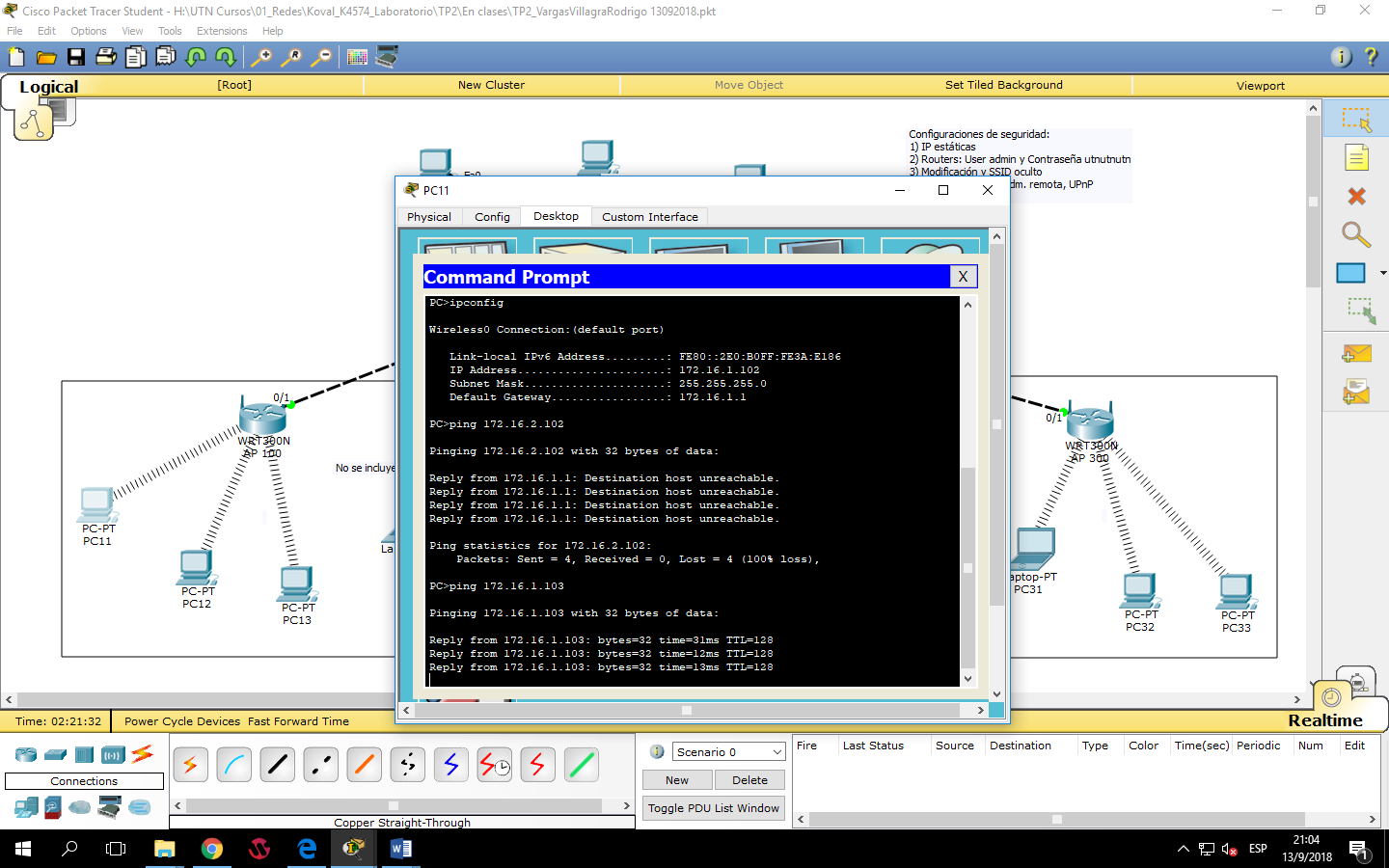


*Intento de acceso desde Admin 1 a la Red 2*

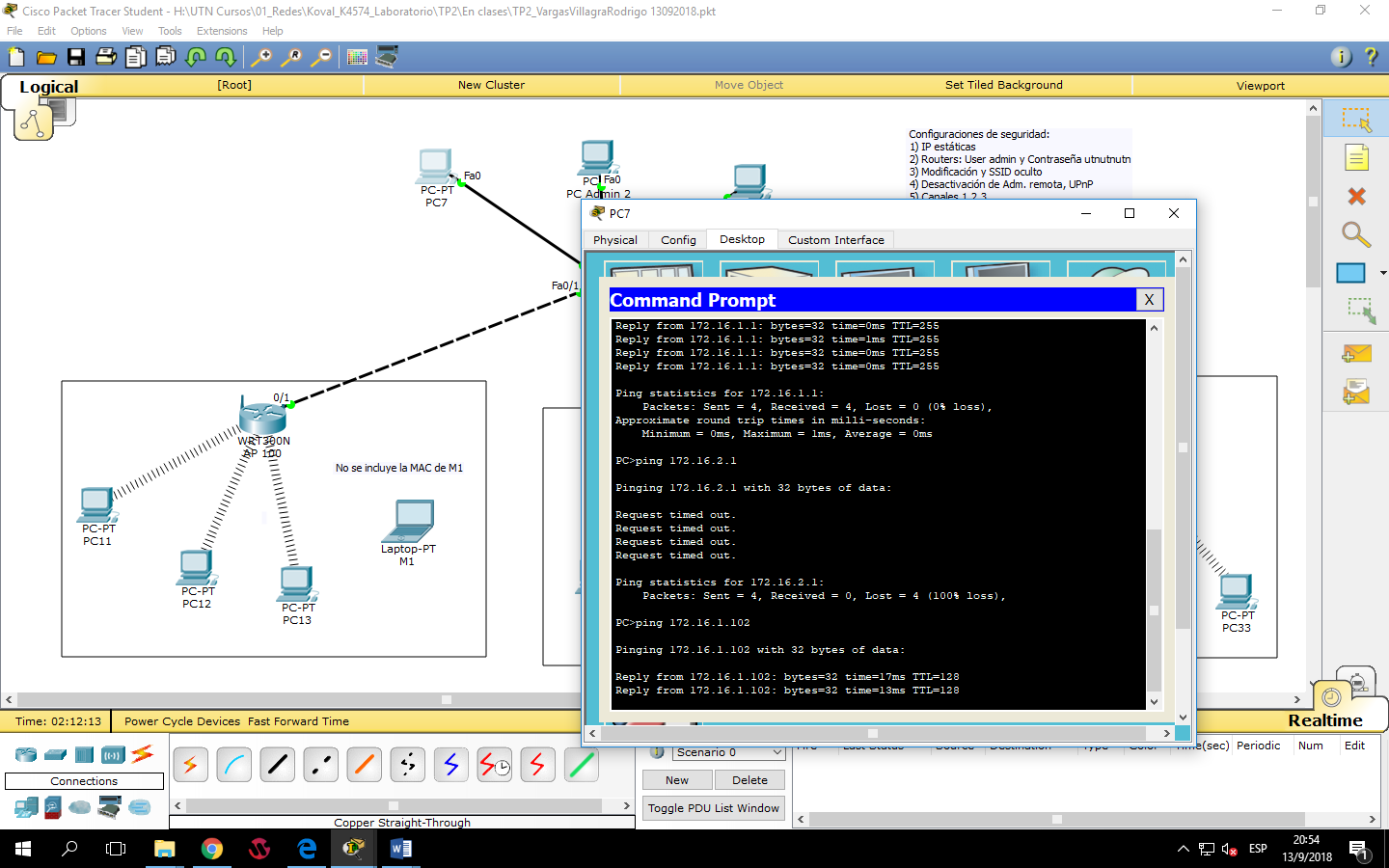


3) Acceso correcto (PING) dentro de la WLAN respectiva. OK

*Pc de la red 1 – Conexión entre 101 y 102*

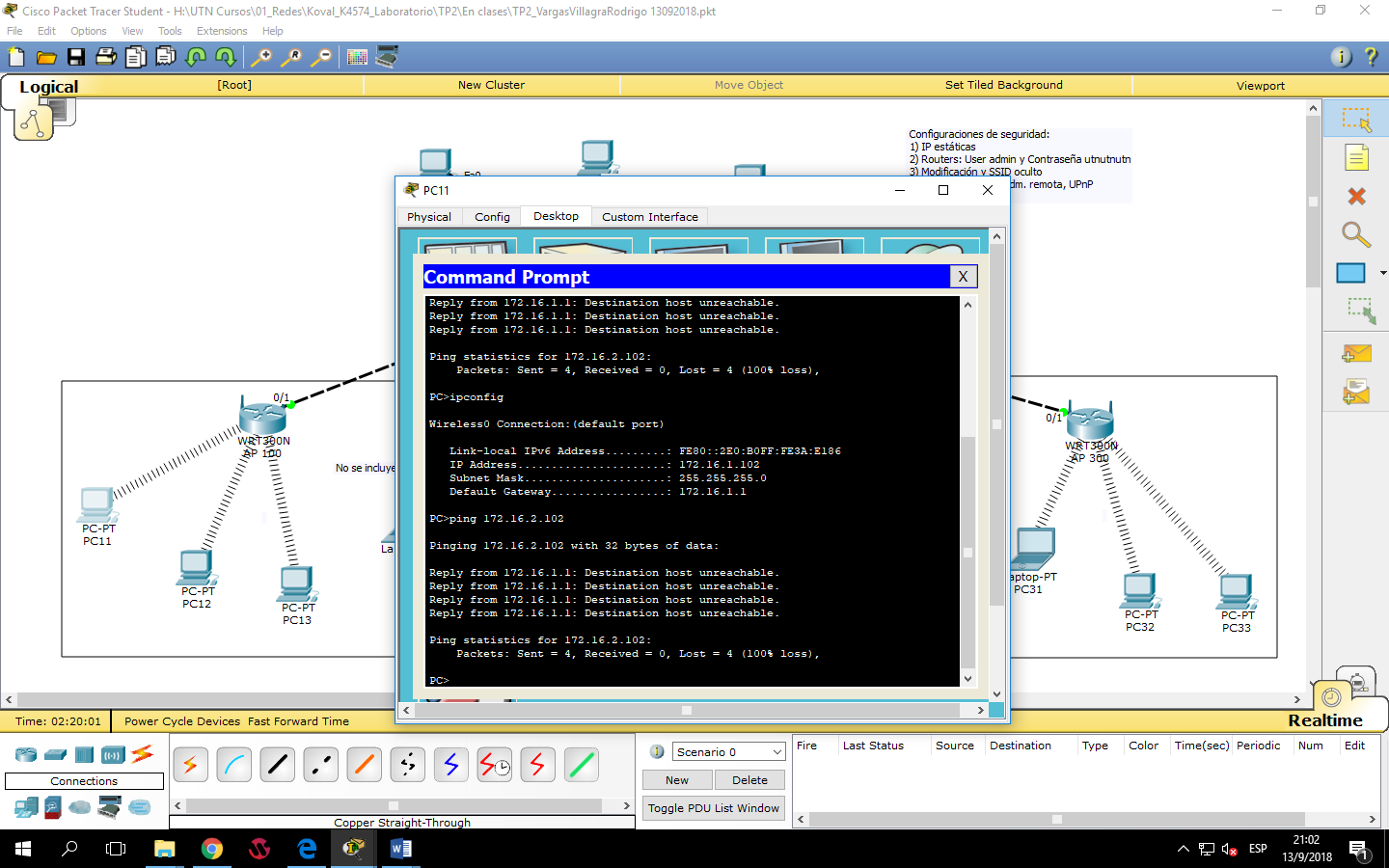


4) Comunicación (PING) entre AL MENOS DOS PC de la WLAN respectiva. OK



5) Restricción de comunicación, aún clave conocida, (acceso wireless fallido) entre DOS PC de distintas WLANs. OK

*Prueba entres Pc de Red 1 y 2*



6) Servicios de seguridad implementados según la guía, a requerimiento del docentelas vulnerabilidades a las que está expuesta la red del estudio de caso. OK

*Configuraciones de seguridad:*

*1) IP estáticas*

*2) Routers: User admin y Contraseña utnutnutn*

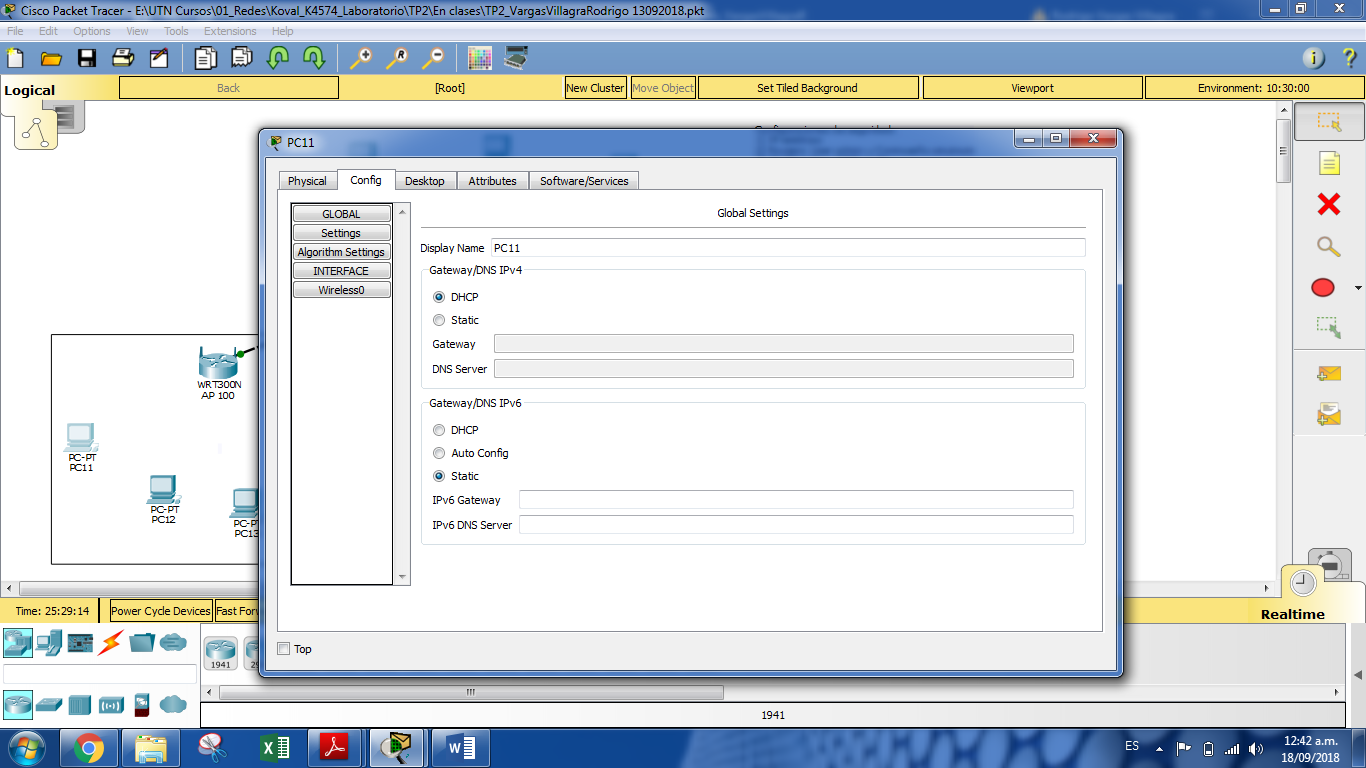
*3) Modificación y SSID oculto*

*4) Desactivación de Adm. remota, UPnP*

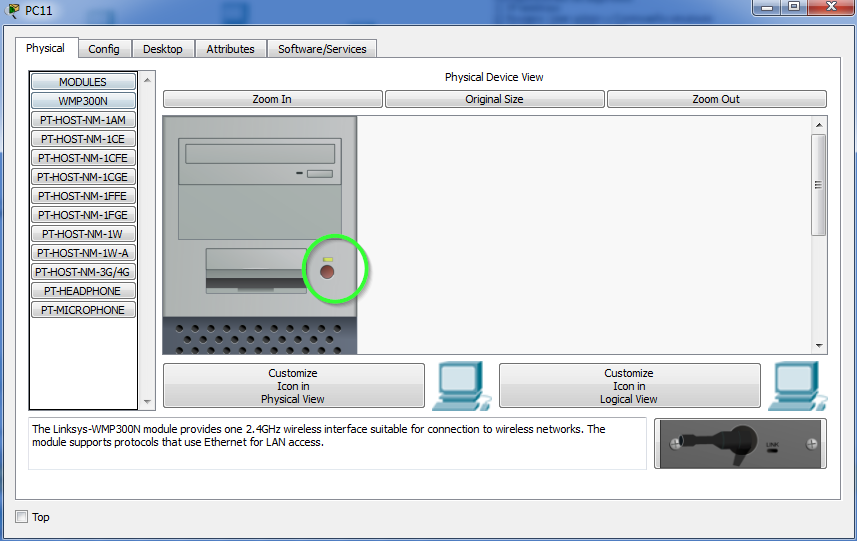
*5) Canales 1,2,3*

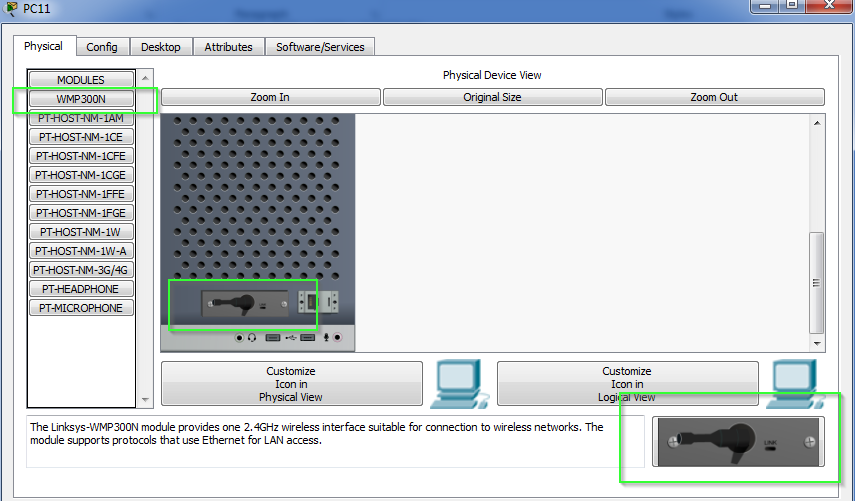
**Configuraciones realizadas**

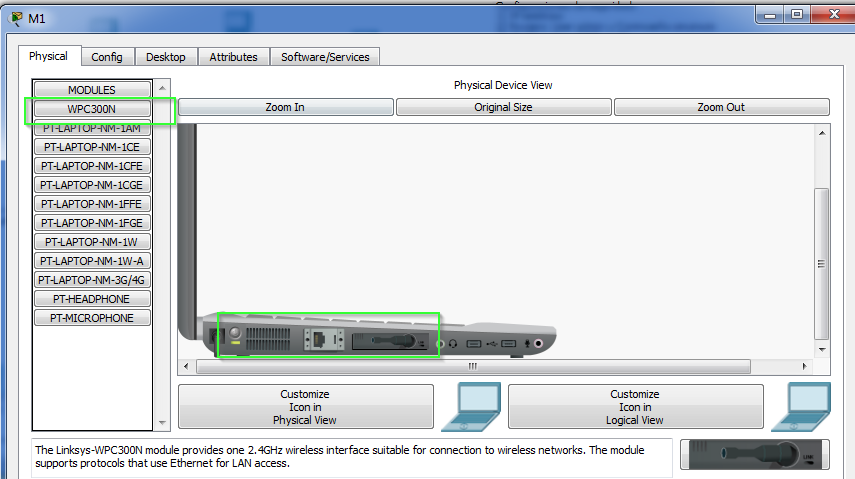
1. Efectuar la configuración sobre 1 sola WLAN, luego se replica la misma para las otras.
2. Nombrar los dispositivos de red según el TP.



1. Las PC vienen sin el módulo de Red Wi FI, por lo que se debe agregar el mismo. Los pasos son: Apagar la PC, retirar el módulo de ethernet, agregar el módulo de Wifi, volver a encender la PC. Como las configuraciones por defecto coinciden con las del Router Wi Fi, la pc se conectará automáticamente.





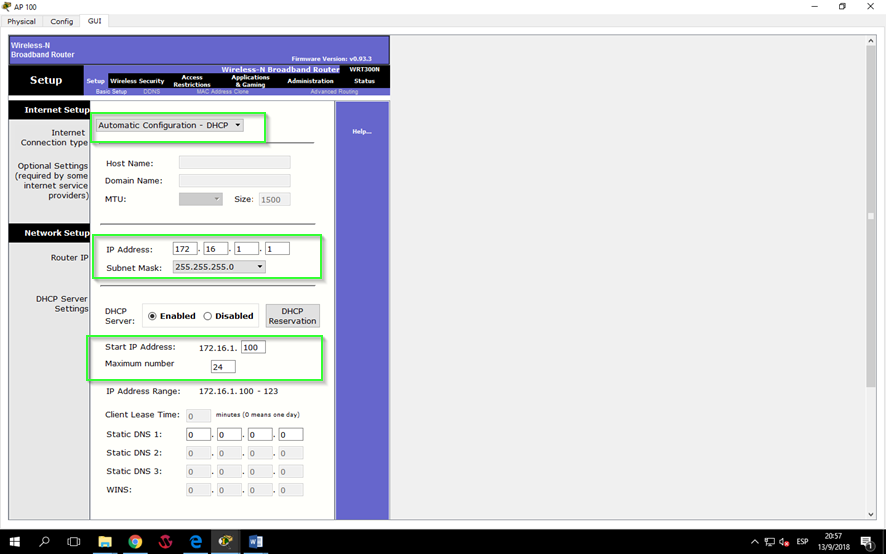


1. Configurar el Router (ejemplo para la RED 1)

Configuro la red LAN

Le asigno una IP Fija. Esto determinará la red en la que estará el dispositivo. Ejemplo: 172.16.1.1 el número en color determina la red.

Le asigno un rango de IPs que asignará a las PCs que se le conecte (23 para el caso)

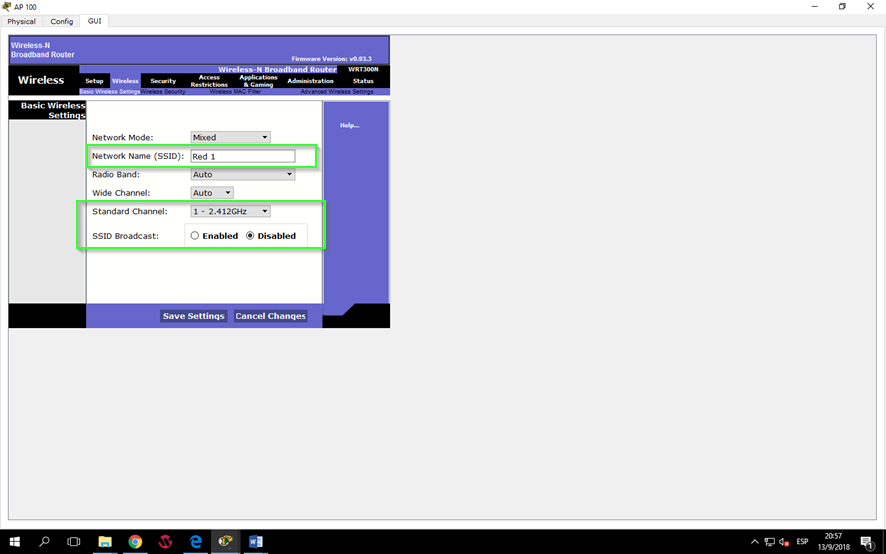


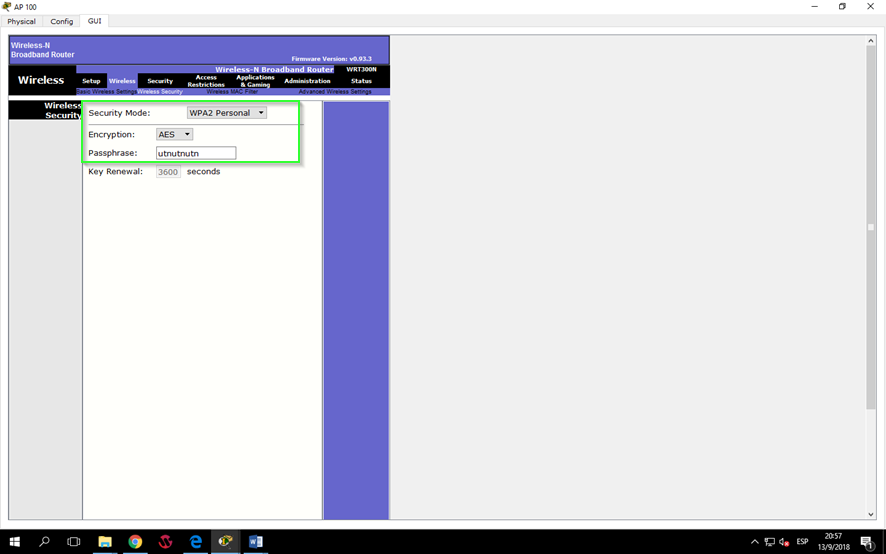
Configuro la red WIFI

Le asigno un nombre a la red wifi.

Recomendación de seguridad

* Le asigno un canal, elegir uno distinto para cada red
* Oculto el SSID
* Habilito la protección WPA2 – Personal y asigno una clave (será la clave del Wifi)
* Restrinjo la conexión por direcciones MAC (para la prueba, dejo una pc afuera).
* Cambiar el usuario y contraseña de administración del router (utnutnutn)
* Desactivar la administración remota



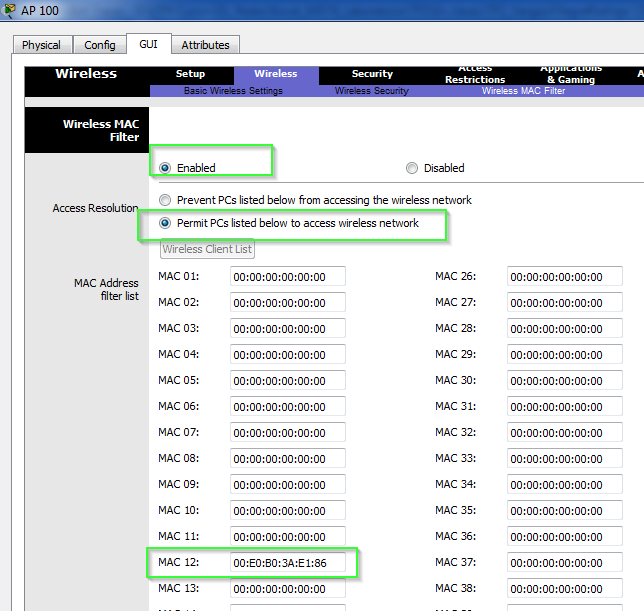


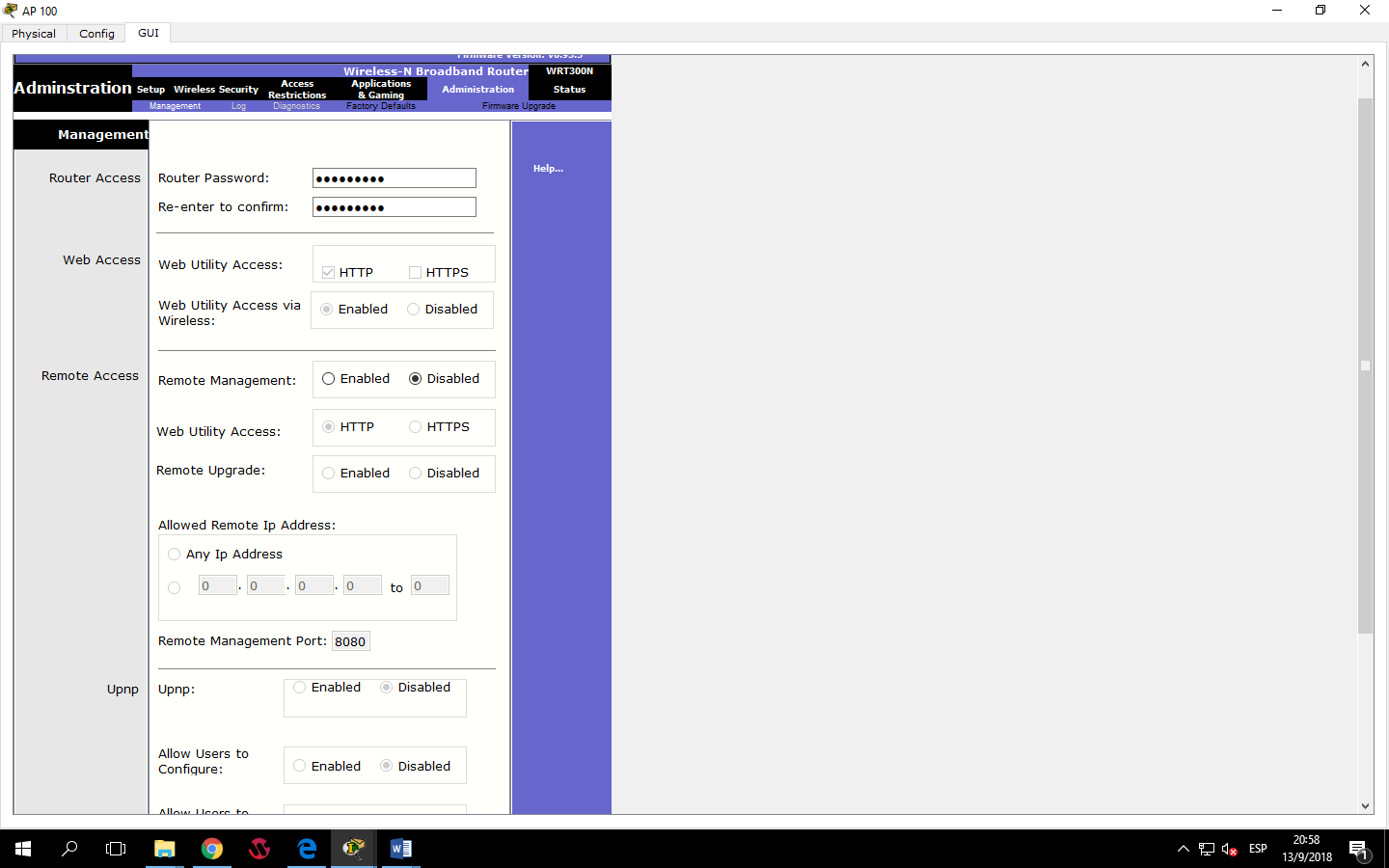
Mac configuradas

00:E0:B0:3A:E1:86

00:40:0B:7C:B7:11

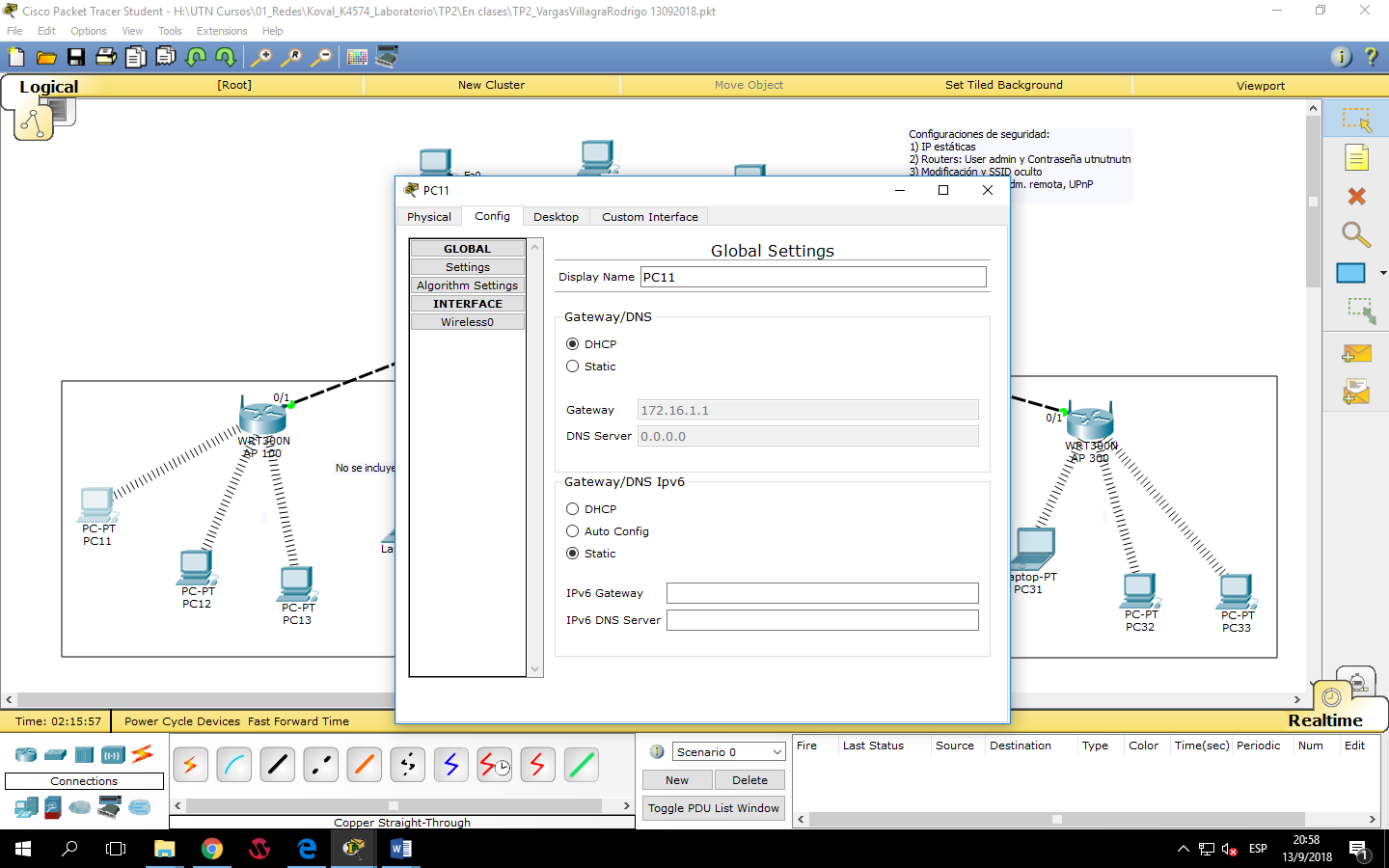
00:40:0B:3E:C9:55

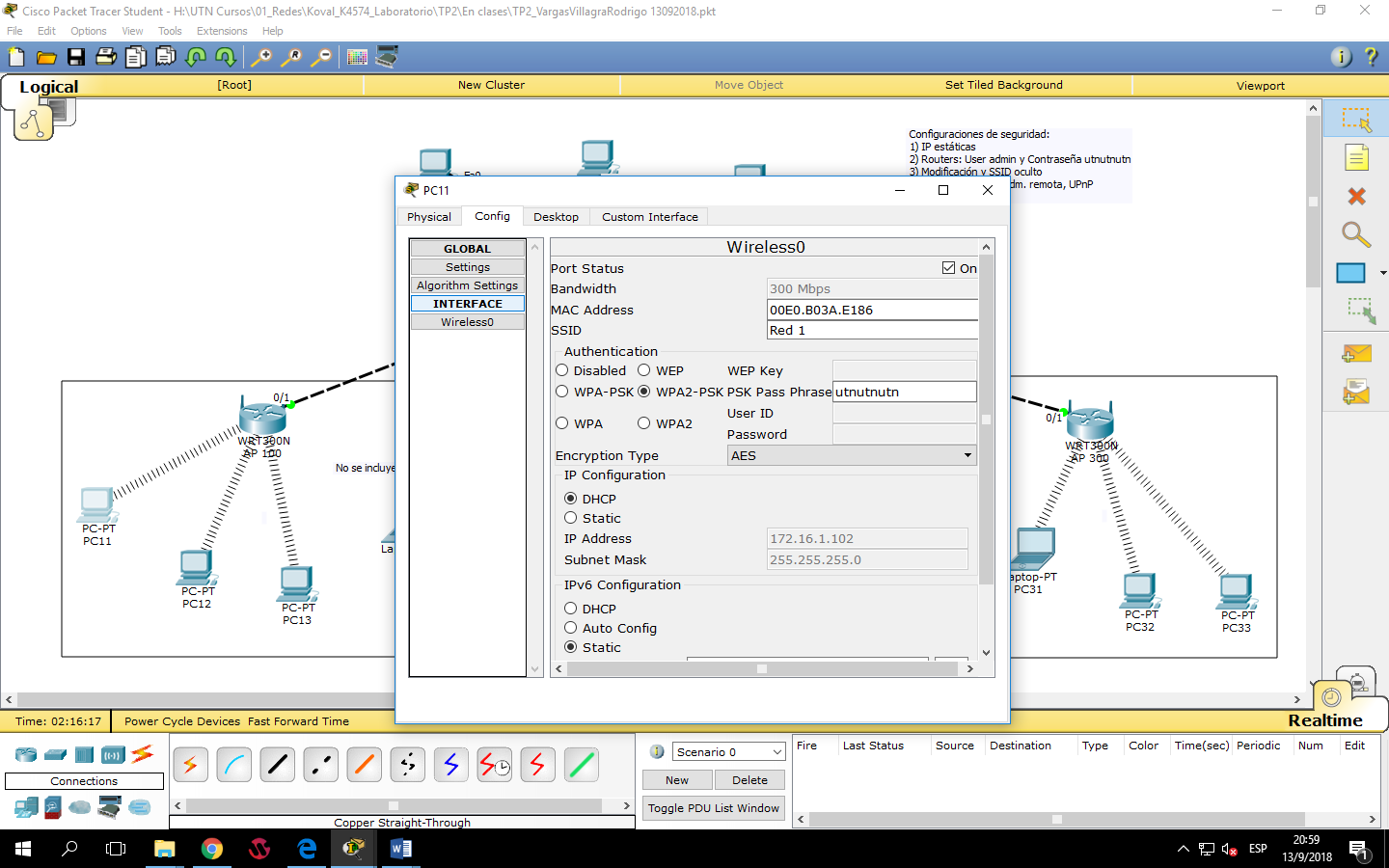


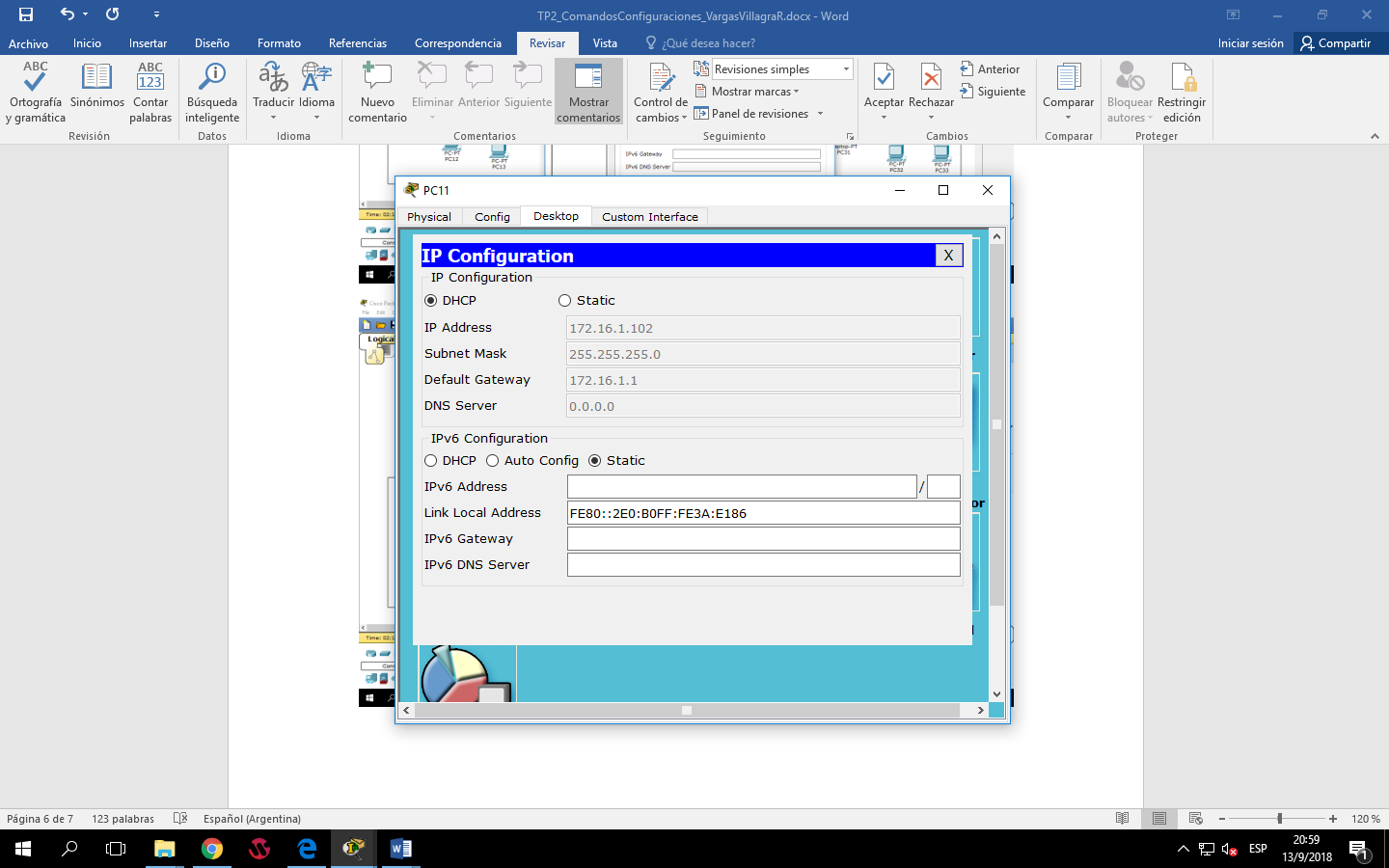


Configuro la PC para que se conecten a la red 1

Red 1 – PC 1







Red 1 – Admin => Debe ser la única que pueda acceder a la administración remota del router