# UNIVERSIDAD AUTÓNOMA METROPOLITANA

# UNIDAD AZCAPOTZALCO

# DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA

**ASESOR:** 

M. EN C. OSCAR ALVARADO NAVA

**ASESOR EXTERNO:** 

ING. RAFAEL GERMÁN PARRA TRUJILLO

ALUMNO:

FELIPE DEL VALLE AGUIÑAGA

**REPORTE DE PROYECTO TERMINAL:** 

# INFRAESTRUCTURA DE ENTRETENIMIENTO Y COMUNICACIÓN CON PRIORIDAD PARA XBOX 360.

**JULIO DE 2011** 

# INDICE

INTRODUCCION	3
SOFTWARE IMPLEMENTADO	4
CAPTURA DE TRAFICO DE XBOX LIVE	6
INSTALACION DE GNS3	34
INTRODUCCION A PORT SECURITY	49
CISCO SWITCH PORT SECURITY	50
INTRODUCCION A VOIP	54
CISCO CALL MANAGER EXPRESS	55
CISCO IP COMMUNICATOR	62
CONFIGURACION DE LOS SERVICIOS DE TELEFONIA DEL F	<b>ROUTER</b> 70
CONFIGURACIÓN DEL WIRELESS ACCESS POINT	74
INTRODUCCION A VPN	83
IMPLEMENTACIÓN DE UNA VPN	86
INTRODUCCION A CALIDAD DE SERVICIO	103
CISCO QOS	107
DESCRIPCION DE LOS VIDEOS DEMOSTRATIVOS	117
SCRIPTS DE SWITCH, ROUTER A, ROUTER B, ROUTER GNS	<b>3 Y WAP</b> 122
FOTO DE LA TOPOLOGIA DE LA RED	155
CONCLUSIONES	156
BIBLIOGRAFIA	157

# **INTRODUCCIÓN**

Este documento explica y detalla todos los requerimientos necesarios para la implementación de la infraestructura de entretenimiento con prioridad para Xbox 360, así como la instalación, configuración e implementación del software y hardware utilizados para su desarrollo, se expone de manera amplia:

- La instalación del software de captura de tráfico de red (Wireshark), de simulación de redes virtuales (GNS3) y de telefonía sobre IP (Cisco IP Communicator), también se explicará como configurar el software para su respectiva función específica dentro del proyecto, que pasos deben seguirse, los parámetros que corresponden a cada campo y como ejecutarlos dentro del ambiente de trabajo; así como las versiones respectivas de cada software.
- Las versiones del IOS de Cisco utilizadas, la configuración de cada equipo, y su función dentro de la red. Se explica a detalla la función de cada equipo, sea de VoIP, de QoS, su correspondiente archivo de configuración, y la manera de enlazarlos en la red de trabajo.
- Los scripts finales de VPN, calidad de servicio (Cisco QoS), configuración de Call Manager Express, y de Switch Port Security. Se describe la construcción del archivo, los comandos utilizados y su función dentro del script, dependiendo el servicio a implementar.
- Las pruebas de conectividad, de enlace y de funcionalidad de cada equipo y software, de manera individual y en conjunto.
- Las conclusiones respectivas de cada módulo, que comportamiento se observo, los casos vistos, la manera en que se logro el objetivo principal, y cuáles fueron los conocimientos adquiridos después del desarrollo del proyecto terminal.

La operación de los equipos de hardware se hará dentro de un laboratorio de redes en un ambiente controlado, para la entrega de la implementación total se realizará un video demostrativo en el cual se muestra con explicación detallada:

- Los pasos de la implementación total
- La construcción del ambiente
- Instalación de Software y configuración de Hardware
- Pruebas de Calidad de servicio y VOIP

Finalmente se entregarán las conclusiones del desarrollo del proyecto, los recursos utilizados, los conocimientos adquiridos y la foto de la topología de la red.

### SOFTWARE IMPLEMENTADO

Captura de tráfico de red:



Simulador grafico de redes:



#### Telefonía Sobre IP:



Software IOS Cisco:

- Call Manager Express versión 4.0.0 : descargable de la página oficial de Cisco
- Cisco IOS versión C3640-JK.BIN
- Cisco QoS para C3640.

Equipo Cisco Utilizado:

- Router Cisco c1700
- Cisco Switch Catalyst 3550
- IP Communicator

Equipo de Cómputo utilizado:

- Laptop HP G42.
- Xbox 360 con disco duro de 250 Gb.

# CAPTURA DE TRAFICO DE XBOX LIVE

## INSTALACIÓN DE WIRESHARK.



Entramos a la página de internet de Wireshark <u>http://www.wireshark.org/</u>:

Descargamos la versión más reciente compatible con nuestro sistema operativo:

<ul> <li>Stable Release (1.4.2)</li> </ul>				
Installer (32-b) 🥪	it)			
Windows Installer (64-bit)				
Windows U3 (32-bit)				
Windows PortableApps (3	2-bit)			
OS X 10.5 (Leopard) Intel	32-bit .dmg			
OS X 10.6 (Snow Leopard	) Intel 64-bit .dmg			
OS X 10.5 (Leopard) PPC	32-bit .dmg			
Source Code				

Old Stable Release (1.2.13)

Especificamos el directorio destino y descargamos



Ejecutamos el programa descargado para iniciar su instalación:



Aceptamos el acuerdo de la licencia:

Wireshark 1.4.2 (32-bit) Setup
License Agreement Please review the license terms before installing Wireshark 1.4.2 (32-bit).
Press Page Down to see the rest of the agreement.
This text consists of three parts: Part I: Some remarks regarding the license given in Part II: The actual license that covers Wireshark. Part III: Other applicable licenses. When in doubt: Part II/III is the legally binding part, Part I is just there to make it easier for people that are not familiar with the GPLv2.
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Wireshark 1.4.2 (32-bit).
Nullsoft Install System v2,44

Elegimos los componentes a Instalar:

Wireshark 1.4.2 (32-bit) Setu	р			
Choose Components Choose which features of Wireshark 1.4.2 (32-bit) you want to install.				
The following components are available for installation.				
Select components to install:	Wireshark         Wireshark         Wireshark         TShark         Image: V Plugins / Extensions         Image: V Tools         W User's Guide			
Space required: 81.6MB	Description Position your mouse over a component t description,	io see its		
Nullsoft Install System v2.44	< Back Next >	Cancel		

Seleccionamos las extensiones de archivos las cuales asociaremos al Wireshark:



Instalamos los archivos en el directorio raíz del software:



Esperamos a que termine la instalación

Wireshark 1.4.2 (32-bit) Setup	
Installing Please wait while Wireshark 1.4.2 (32-bit) is being installed.	
Extract: dictionary.rfc4818	
Extract: dictionary.rfc2868 Extract: dictionary.rfc3162 Extract: dictionary.rfc3576 Extract: dictionary.rfc3580 Extract: dictionary.rfc4072 Extract: dictionary.rfc4372 Extract: dictionary.rfc4675 Extract: dictionary.rfc4679	•
Nullsoft Install System v2.44	Cancel

## Al finalizar, lanzamos la aplicación

Wireshark 1.4.2 (32-bit) Set	up
	Completing the Wireshark 1.4.2 (32-bit) Setup Wizard Wireshark 1.4.2 (32-bit) has been installed on your computer. Click Finish to close this wizard. Run Wireshark 1.4.2 (32-bit) Show News
	< Back Finish Cancel

#### MODO PROMISCUO

Wireshark es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo.

En informática, el modo promiscuo es aquel en el que una computadora conectada a una red compartida, tanto la basada en cable de cobre como la basada en tecnología inalámbrica, captura todo el tráfico que circula por ella. Este modo está muy relacionado con los sniffers que se basan en este modo para realizar su tarea.

El modo promiscuo resulta muy útil para ver que paquetes atraviesan tu red. Su utilidad se basa en que todos los paquetes que pasan por una red tiene la información de a que protocolo perteneces y las opciones de re ensamblado. Incluso si no están cifrados, tienen la información en claro, es decir, que puedo saber que contiene el paquete.

Es especialmente útil en los routers que unen varias redes, ya que con herramientas que analizan los paquetes podemos detectar errores, ataques, pérdida de paquetes, sobrecargas, etc. Al capturar todo el tráfico que atraviesa un Router, se pueden determinar también, usos, servicios que tienen que recibir ancho de banda prioritario, accesos no permitidos a equipos o protocolos, etc.

#### CAPTURA DE PAQUETES DE XBOX LIVE.

En primer lugar necesitamos conectar el Xbox 360 a la laptop, para que el software Wireshark pueda capturar el tráfico de red que fluirá por el puerto Ethernet de la laptop hacia el Xbox 360, tanto de salida como de entrada.

La captura de tráfico determinara el tipo de paquetes, la clase de tráfico, los protocolos utilizados durante la transferencia de información, y los parámetros de red que se establecen cuando se habilita una sesión de juego.

Después de haber conectado el Xbox 360 a la laptop, es necesario hacer unos ajustes a las configuraciones de red al Xbox 360, y crear un puente de red en la laptop para que habilite el paso de tráfico de red del servidor de Xbox Live a la consola, la captura se hará en la interfaz de la laptop conectada al 360, por medio de la opción de capturar interface en el Wireshark, los pasos para conectar el Xbox 360 a Xbox live por medio de la laptop, y sus respectivas configuraciones se describen a continuación.

# CONEXIÓN XBOX 360 A TRAVES DE LAPTOP HP PARA CAPTURA DE TRÁFICO DE RED Y ANALISIS DE PAQUETES DEL SERVICIO DE XBOX LIVE

1.- Verificar que existan 2 interfaces de red en la laptop, una puede ser inalámbrica, si obtenemos un modem router inalámbrico de nuestro ISP.



Fig. 1: Interfaz de red Ethernet e Interfaz de red Inalámbrica

2.- Creamos un puente de red entre la interfaz Ethernet y la interfaz Inalámbrica



Fig. 2: Estableciendo puente de red



Fig. 3: Puente de red creado entre la 2 interfaces.

3.- En el botón de inicio, clic en ejecutar, escribir cmd y enter, después escribir en la ventana de comandos el comando ipconfig /all para ver la configuración de red de la laptop

C:\Windows\system32\cmd.exe
DHCP habilitado : sí Configuración automática habilitada : sí Vínculo: dirección IPv6 local : fe80::69a5:6ed5:4e3:e0df%20(Preferido) Dirección IPv4 de configuración automática: 169.254.224.223(Preferido) Máscara de subred : 255.255.0.0 Puerta de enlace predeterminada : IAID DHCPv6 : 369229900 DUID de cliente DHCPv6 : 00-01-00-01-13-3B-11-EB-C8-0A-A9- 91-09-E7 Servidores DNS : fec0:0:0:ffff::1%1 fec0:0:0:ffff::3%1 NetBIOS sobre TCP/IP : habilitado
Adaptador de LAN inalámbrica Conexión de red inalámbrica:
Sufijo DNS específico para la conexión : gateway.2wire.net Descripción Realtek RTL8191SE 802.11b/g/n WiF i Adapter
Dirección física
Dirección IPv4

Fig. 4: Configuraciones de las interfaces de red

Es necesario asignar una dirección IP que este dentro del mismo segmento que la laptop al Xbox 360, así como su correspondiente mascara de red.

4.- Conectamos la interfaz Ethernet del Xbox 360 a la interfaz Ethernet de la laptop, con un cable Ethernet de entrada RJ-45.



Fig. 5: Xbox 360 conectado de manera alámbrica a la Laptop, esta se conecta inalámbricamente al router del ISP.

5.- Prendemos el Xbox 360 y esperamos a que cargue la pantalla principal.

Xbo	x Guide 2:5	ш () 7 РМ
Но	Xbox Dashboard	
ome	Sign In (2 Profiles)	
	Create Profile	
	Recover Gamertag	
	Close Tray	0
A	elect 📵 Back 🛞 Sign In 🛞 Xbox Dashboard	

Fig. 6: Pantalla principal del Xbox 360

6.- Vamos a la pantalla de System Settings, la cual tiene la configuración de la consola.



Fig. 7: Configuración de la consola.

7.- Se modificaran los parámetros de red, en la opción de Network Settings.

Sys	stem Settings	
	Console Settings	С
		h
	Memory	c c se
	Network Settings	
	Computers	
	Q Xbox LIVE Vision	
	🛴 Initial Setup	

Fig. 8: Parámetros de red.

8.- Modificaremos la red alámbrica, es la que está conectada a la laptop.



Fig. 9: Configurando red alámbrica.



Fig. 10: Propiedades de red y pruebas de conectividad.

9.- Asignamos una IP Estática al Xbox 360, la cual debe estar en el mismo segmento que la dirección IP de la interfaz Ethernet de la laptop, en este caso los parámetros son:

- Dirección IP de clase C privada, usaremos 171.21.1.201
- Mascara de red 255.255.255.0
- Default Gateway 172.21.1.253

El default Gateway es el mismo que el de la laptop, y es la dirección IP de la interfaz interna del router del ISP.

Con	nfigure Network		
	Basic Settings	A	
	IP Settings IP Address Subnet Mask Gateway		
DNS Settings Primary DNS Server Secondary DNS Server			
Edit IP	Fig. 11: Configuración m Settings	anual de red	
s	ubnet Mask	Current Settings	
G	iateway	Enter your IP address. This address must not belong to any other devit on your network and cannot be 0.0.0.0, 255.255.255.255, or 127.0.0	
D	Jone		

Fig.12 Configuramos y guardamos los parámetros de red.

10.- Iniciamos las pruebas de conectividad con el servidor de Xbox Live



Fig. 13: Probando la red, Internet y el servidor de Xbox Live.

11.- Si nos aparecen los 3 campos como conectados, ya establecimos una sesión en línea.



Fig.14: Conexión establecida del Xbox 360.

12.- Iniciamos sesión con un perfil de jugador valido y esperamos la pantalla de inicio de Xbox Live



Fig. 15: Iniciando Sesión

	Xbox	Guide		<b>岡田</b> 〇 3:00 PM			
G	Da	Xbox Dasi	nboard		R		
Imes	IrkR	Friends		9 省	edia		
	aVenMaid	Party		0 🐳			
		enMaide	nM	Messages		0 💌	
			Chat & IM				
	eN	Close Tray		0			
				D. Hourd			

Fig. 16: Sesión iniciada, listo para iniciar juego en línea.

## ANALISIS DE TRÁFICO DE PAQUETES DE RED DE XBOX LIVE.

Se realizo una prueba inicial de captura de tráfico de red, entre la consola Xbox 360, y el servidor de Xbox Live, en esta prueba inicial los aparatos involucrados fueron:

- Consola Xbox 360
- Modem Ruteador de Infinitum modelo 2700 HG
- Laptop HP modelo G42-241LA Procesador Pentium (R) Dual-Core 2.30 GHz 3GB RAM

La captura de los paquetes de Xbox live se realizo con el software Wireshark, la captura tuvo como objetivo principal conocer la estructura de los encabezados de los paquetes que el Xbox 360 envía al servidor de Xbox Live, así como los puertos TCP y UDP que son necesarios para que se establezca la comunicación.

#### ANALISIS PAQUETES DE XBOX LIVE.

#### Captura en Wireshark

El análisis del intercambio de paquetes en la red es muy importante para saber los puertos y los distintos mensajes que se realizan durante el intercambio de mensajes en el Xbox 360, el análisis se expone detalladamente más adelante.

No	Time	Source	Destinution	Protocol	lafe .
	1 0.00000	192, 168, 137, 138	189.180.103.76	UDV	Source port: Abox Destination port: 33776
	2 0.103401	189,180,103,76	192.168.137.136	LIDP	Source port: 33776 Destination port; abox
	3 0.133345	192.168.137.136	189.180.103.76	UDF	Source port: xbox Destination port: 33776
	4 1.951824	192.168.137.136	74.138.34.22	UDP	Source port: xbox Destination port: xbox
	5 2.059696	74.138.34.22	197.168.137.136	UDP	Source port: whom Destination port: whom
	6.4.612698	65.54,186.79	192.168.137.136	107	https > 41814 [RST, ACK] Seg-1 Ack-1 Win-0 Len-0
	7 8,980014	192,168,137,136	85.55.42.180	UDP	Source port: whom Destination port: whom
	8 9,398650	74.138.34.22	192.168.117.136	UDP	Source port: xbox Destination port: xbox
	9 9.425666	192.168.137.136	74.138.34.22	UDP	Source port: xbox Destination port: xbox
	10 9.510715	74.138.34.22	192.168.137.136	UDP	Source port: abox Destination port: abox
	11 9.559133	192.168.137.136	74,138,34,22	UDP	Source port: xbox Destination port: xbox
	12 9.664787	74.138.34.22	192.168.137.136	UDF	Source port: xbox Destination port: xbox
	13 9.692828	192.168.137.136	74.138.34.22	UDP.	Source port: xbox Destination port: xbox
	4 9.798680	74,138,34,22	192.168.137.136	UDP	Source port: xbox Destination port: xbox
	15 9.826289	192,168,137,138	74,138,34,22	UDP	Source port: xbox Destination port: xbox
	16 9.930864	74.138.34.22	192.168.137.136	UDP.	Source port: xbox Destination port: xbox
	17 9.959650	192,168,137,136	74.138.34.22	UDP	Source port: xbox Destination port: xbox
3	18 10.062884	74,138,34,22	192,168,137,136	UDP	Source port: xbox Destination port: xbox
	19 10.093061	192.168.137.136		0x +00 +00 +	
	20 10.126484	192.168.137.136	1000000 192.168.197.1	130 198 199 1	13.10 ULV source port stox. Destination port; 33/76
	21 10.171450	189,180,103.76	In Lyang 1 766 Incra		At hurst contend)
	22 10.199443	74.138.34.22	in the set (or office		
	23 10.226517	192.168.137.136	a Ethernet 11, Src	: Microso	_34:15:64 (00:22:46:84:15:64), DST: /2:11:41:01:31:10 (/2:11:4 _
- 3	24 10.332960	74.138.34.22	E Internet Protoco	1, src: 1	92.168.137.136 (192.168.137.136), Dst: 189.180.103.76 (189.180.)
	25 10.360054	192.168.137.136	a üser Datagram Pr	otocel, S	rc Port: xbox (3074), Dst Port: 33776 (33776)
3	26 10.464894	74,138,34,22	5. 8	123111	CM/Henry dealer and the same field in the second
	27 10.488542	65.55.47.180	A commendant and a second second		
E Fra E Eth E Int E Use E Dat	me 1 (66 bytes on wire, ernet II, Brc: Microsof ernet Protocol, Src: 193 r Datagram Protocol, Src a (24 bytes)	66 bytes captured) 9a:15:6a (00:22:48:9a:15:6 2.168.137.136 (192.168.137. c Port: xbox (3074), Dst Por	0000 2 1 1 1 0 0010 00 34 57 4 0 0020 07 4 0 0 0 0030 07 4 0 0 0 0040 1 2	if fe o0 1 X0 DO 40 1 X3 F0 00 1 72 Se 1a 0	7 44 99 15 61 09 00 15 00 1 94 39 60 38 98 88 94 54 0 50 45 48 79 54 90 76 55 0 50 45 44 79 54 90 76 55 48 5 97 50 14 55 48 5 97 50 50 54 55 58 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5

Fig. 1: Captura de tráfico de red y envió-recepción de paquetes en Wireshark

ARP: Es un protocolo de redes de computadoras, el cual se usa para determinar la dirección de hardware cuando solamente se conoce la dirección IP. Esta función es crítica para el funcionamiento de la conexión del Xbox 360 a Xbox Live, el cual se encuentra dentro de un área local de trabajo, ya que el tráfico de red proveniente del Xbox 360 que pasa por el Router está

basado en direcciones IP, y se necesita determinar el próximo "montículo" por el cual se direccionara ese tráfico, hasta llegar al servidor de Xbox Live.

F <u>i</u> lter:		▼ E	pression Clea <u>r</u> App <u>l</u> y			
No.	Time	Source	Destination	Protocol .	Info	
3	31 18.816689	72:f1:a1:61:3f:f6	Microsof_9a:15:6a	ARP	Who has 192.168.137.136? Tell 192.168.137.1	
3	32 18.816768	Microsof_9a:15:6a	72:f1:a1:61:3f:f6	ARP	192.168.137.136 is at 00:22:48:9a:15:6a	
12	66 59.813556	72:f1:a1:61:3f:f6	Microsof_9a:15:6a	ARP	Who has 192.168.137.136? Tell 192.168.137.1	
12	67 59.813867	Microsof_9a:15:6a	72:f1:a1:61:3f:f6	ARP	192.168.137.136 is at 00:22:48:9a:15:6a	
23	82 100.311250	72:f1:a1:61:3f:f6	Microsof_9a:15:6a	ARP	Who has 192.168.137.136? Tell 192.168.137.1	
23	83 100.311558	Microsof_9a:15:6a	72:f1:a1:61:3f:f6	ARP	192.168.137.136 is at 00:22:48:9a:15:6a	
29	53 125.109191	72:f1:a1:61:3f:f6	Brjoadcast	ARP	Who has 192.168.137.168? Tell 192.168.137.1	
29	97 125.817288	72:f1:a1:61:3f:f6	BI 7 331 18 816680 72 ft a1	61-3666 Micro	noof 0a:15:6a ARD Who had 102 168 137 1367 Tall 102 168 137 1	
30	24 126.815661	72:f1:a1:61:3f:f6	Br	origino micit	350_3613.68 ANN WHO HES 122.100.137.130. TCN 132.100.137.1	
34	37 140.824479	72:f1:a1:61:3f:f6	Mi 🕀 Frame 331 (42 b)	/tes on w	ire. 42 bytes captured)	
34	38 140.824786	Microsof_9a:15:6a	71 Ethornot TT Sr	· 72.f1.	a1:61:2f:f6 (72:f1:a1:61:2f:f6) Det: Wicrosof 0a:15:6a (00:22:48:0	
37	94 182.320596	72:f1:a1:61:3f:f6	Mile all a line and		a1.01.51.10 (72.11.a1.01.51.10), DSC. MICLOSOL_98.15.08 (00.22.48.2	
37	95 182.320797	Microsof_9a:15:6a	72 H Address Resolut	ion Proto	col (request)	
41	32 188.311005	72:f1:a1:61:3f:f6	Br			
57	88 222.818258	72:f1:a1:61:3f:f6	M			
57	89 222.818338	Microsof_9a:15:6a	71			
76	31 263.315923	72:f1:a1:61:3f:f6	M1 0000 00 22 48 9a	15 6a 72	f1 a1 61 3f f6 08 06 00 01 ."Hira?	
76	32 263.316105	Microsof_9a:15:6a	72 0010 08 00 06 04	00 01 72	f1 a1 61 3f f6 c0 a8 89 01ra?	
93	96 304.312803	72:f1:a1:61:3f:f6	M1 0020 00 22 48 9a	15 6a cO	a8 89 88 . "Hj	
93	97 304.313098	Microsof_9a:15:6a	72			
112	18 344.810457	72:f1:a1:61:3f:f6	MT			
112	19 344.810761	Microsof_9a:15:6a	71			
132	48 384,824533	72:f1:a1:61:3f:f6	Microsof_9a:15:6a	ARP	Who has 192,168,137,136? Tell 192,168,137,1	

#### Address Resolution Protocol (Petición)

Fig.2: Envió de una petición de un mensaje ARP

En la figura anterior, se envía un mensaje ARP, preguntando quien tiene la dirección MAC de la dirección IP indicada en el campo de "INFO", esta es una petición, y por lo tanto, el siguiente mensaje debe de contener la respuesta a esta petición.

No.	Time	Source	Destination	Protocol .	Info		
331	18.816689	72:f1:a1:61:3f:f6	Microsof_9a:15:6a	ARP	Who has 192.168.137.136	? Tell 192.168.137.1	
332	18.816768	Microsof_9a:15:6a	72:f1:a1:61:3f:f6	ARP	192.168.137.136 is at 0	0:22:48:9a:15:6a	
1266	59.813556	72:f1:a1:61:3f:f6	Microsof_9a:15:6a	ARP	Who has 192.168.137.136	? Tell 192.168.137.1	
1267	59.813867	Microsof_9a:15:6a	72:f1:a1:61:3f:f6	ARP	192.168.137.136 is at 0	0:22:48:9a:15:6a	
2382	100.311250	72:f1:a1:61:3f:f6	Microsof_9a:15:6a	ARP	Who has 192.168.137.136	? Tell 192.168.137.1	
2383	100.311558	Microsof_9a:15:6a					
2963	125.109191	72:f1:a1:61:3f:f6	332 18.816/68 Microsof_9a:15:6a	/2:f1:a1:61:3f	t6 ARP 192,168,137,136 is at 00:22:4	8:9a:15:6a	
2997	125.817288	72:f1:a1:61:3f:f6	Ename 222 (60 hites on	uino 60	huter contured)		
3024	126.815661	72:f1:a1:61:3f:f6	Frame 332 (ou byles on	wire, ou	bytes captured)		
3437	140.824479	72:f1:a1:61:3f:f6 🗄	Ethernet II, Src: Micro	osot_9a:1	5:6a (00:22:48:9a:15:6a)	, Dst: 72:†1:a1:61:3†:†6 (72:†1:a1:0	
3438	140.824786	Microsof_9a:15:6a 🗄	Address Resolution Pro	tocol (re	ply)		
3794	182.320596	72:f1:a1:61:3f:f6					
3795	182.320797	Microsof_9a:15:6a					
4132	188.311005	72:f1:a1:61:3f:f6 <					
5788	222.818258	72:f1:a1:61:3f:f6		0 22 40			
5789	222.818338	Microsof_9a:15:6a		10 ZZ 48	9a 15 0a 08 00 00 01 r	indin Hilling	
7631	263.315923	72:f1:a1:61:3f:f6	10 08 00 00 04 00 02 0	0 22 40	9d 10 0d CU do 69 66	n J	
7632	263.316105	Microsof_9a:15:6a	<b>20</b> 72 11 <b>a</b> 1 01 51 10 0	0 ao og		a:	
9396	304.312803	72:f1:a1:61:3f:f6		0 00 00			
9397	304.313098	Microsof_9a:15:6a					
11218	344.810457	72:f1:a1:61:3f:f6	MICLUSUI_50.15.00	ANE	WHO HAS 152.100.137.130	: TETT 152.100.15/.1	

Fig. 3: Recepción de una respuesta de un mensaje ARP

La figura anterior nos muestra la recepción de la respuesta al mensaje ARP enviado anteriormente el cual pedía la dirección MAC de la IP mostrada en el campo "INFO", en este caso vemos que nos dice que la dirección 192.168.137.136 contiene la dirección MAC 00:22:48:9a:15:6a, la cual corresponde al puerto Ethernet del Xbox 360.

Cabe destacar que el envió del mensaje ARP de la Fig.2 se realiza desde la laptop al Xbox 360, es decir, la dirección fuente MAC 72:f1:a1:61:3f:f6 proviene de la laptop HP G42; esta tiene como objetivo conocer la dirección MAC de la consola Xbox 360; ahora, en el mensaje de respuesta proveniente del Xbox 360 nos dice que la IP 192.168.137.136 contiene la dirección MAC 00:22:48:9a:15:6a.

#### DNS (Domain Name System)

Se encarga de asociar nombres de dominio, con sus correspondientes direcciones IP, el Xbox 360 utiliza el puerto 53, asociado a los DNS, para resolver ciertas direcciones IP del servidor de Xbox Live.

En el siguiente mensaje, s e envía una petición sobre una imagen "Avatar" a Xboxlive.com, el protocolo DNS se encarga de traducir el nombre de xboxlive.com a una dirección IP, para efectos de conexión y transferencia de datos, en este caso, imágenes de jugador

No.	Time	Source	Destination	Protocol .	Info				
16596	456.850517	te80::e5be:e29e:8544:	tt02::1:2	DHCPv6	Solicit				
17374	472.855930	fe80::e5be:e29e:8544:	ff02::1:2	DHCPV6	Solicit				
18798	504.867294	fe80::e5be:e29e:8544:	ff02::1:2	DHCPv6	Solicit				
1060	51.033091	192.168.137.136	192.168.137.1	DNS	Standard query A avatar.	xboxlive.com			
1062	51.089600	192.168.137.1	192.168.137.136	DNS	Standard query response	CNAME avatar.xboxlive.co	om.nsat	c.net CNAME	content.xbox.
1081	51.716925	192.168.137.136	192.168.137.1	DNS	Standard query A avatar.	xboxlive.com			
1083	51.773461	192.168.137,1	102 168 137 136	DNIS	Standard query response	CNAME avatar vhovlive c	n nsat	c.net CNAME	content.xbox.
1280	60.192021	192.168.137 1060 51.	033091 192.168.137.136 192.168.	137.1 DNS Sta	andard query A avatar.xboxlive.com		X		
1284	60.245030	192.168.137						.net CNAME	content.xbox.
1290	60.342322	192.168.137	net TT Src: Microsof (	a-15-6a	(00.22.48.02.15.62) Det.	72.f1.a1.61.3f.f6 (72.f	1.5. *		
1296	60.396878	192.168.137	et II, Sic. Microsol_s	100 107 1	(00.22.40.58.15.08), DSC.	+. 102 100 127 1 (102 10	1.a.	.net CNAME	content.xbox.
1299	60.458452	192.168.137, H Intern	let Protocol, Src: 192.	108.13/.1	L30 (192.108.13/.130), DS	t: 192.108.137.1 (192.10	8.1. E		
1319	60.570812	192.168.137 H User [	Datagram Protocol, Src	Port: de	-server (1256), Dst Port:	domain (53)		.net CNAME	content.xbox.
1409	62.677511	192.168.137. 🗄 Domain	n Name System (query)				$\overline{\nabla}$		
1410	62.730235	192.168.137						.net CNAME	content.xbox.
1482	64.178937	192.168.137					· .		
1484	64.229143	192.168.137, 0000 72	f1 a1 61 3f f6 00 22	48 9a 15	6a 08 00 45 00 ra?	." НјЕ.			
1486	64.230667	192.168.137, 0010 00	41 59 6d 00 00 40 11	8d 64 c0	a8 89 88 c0 a8 .AYm0	ad		.net CNAME	content.xbox.
1493	64.322787	192.168.137, 0020 89	01 04 e8 00 35 00 2d	69 88 59	6c 01 00 00 015.	- i.Yl	Ξ	.net CNAME	content.xbox.
1066	51.149253	192.168.137 0030 00	00 00 00 00 00 06 61	76 61 74	61 72 08 78 62	.a vatar.xb			
1075	51.396404	187.141.2.1 0040 61	78 6C 69 76 65 03 63	6† 6d 00	00 01 00 01 oxlive.	.c om	-		
1089	51.833343	192.168.137							

#### Protocolo DNS

#### Fig. 4: Petición estándar a Xboxlive.com

Después viene la respuesta a la petición enviada anteriormente, se puede observar que la respuesta proviene del mismo puerto (53), por el cual se envió la petición, en este caso contiene CNAME del "Avatar" enviado al Xbox 360.

No.	Time	Source Destin	nation Protocol	• Info	
10000	441.02J105	10000000.0290.0044. 1102		SUTICIU	
16045	442.825623	fe80::e5be:e29e:8544: ff02	:::1:2 DHCPV6	Solicit	
16124	444.838227	fe80::e5be:e29e:8544: ff02	2::1:2 DHCPV6	Solicit	
16275	448.847598	fe80::e5be:e29e:8544: ff02	2::1:2 DHCPV6	Solicit	
16596	456.850517	fe80::e5be:e29e:8544: ff02	2::1:2 DHCPV6	Solicit	
17374	472.855930	fe80::e5be:e29e:8544: ff02	2::1:2 DHCPV6	Solicit	
18798	504.867294	fe80::e5be:e29e:8544: ff02	2::1:2 DHCPV6	Solicit	
1060	51.033091	192.168.137.136 192.1	168.137.1 DNS	Standard query A avatar.xboxlive.com	
1062	51.089600	192.168.137.1 192.1	168.137.136 DNS	Standard query response CNAME avatar.xboxlive.co	m.nsatc.net CNAME content.xbox.
1081	51.716925	192.168.137.136 192.1	168.137.1 DNS	Standard query A avatar.xboxlive.com	
1083	51.773461	192.1			satc.net CNAME content.xbox.
1280	60.192021	192.1	137.1 192.108.137.136 DNS Standard	query response CNAME avatar.xboxiive.com.nsatc.net CN	
1284	60.245030	192.10 In Frame 1062 (222 b	hutos on wino 222 hutos	conturod	satc.net CNAME content.xbox.
1290	60.342322	192.10 H FT alle 1002 (223 D	bytes on wrie, 225 bytes	Captul eu)	
1296	60.396878	192.1( Ethernet II, Src:	: /2:f1:a1:61:3f:f6 (/2:f	1:al:61:3f:f6), Dst: Microsof_9a:15:6a (00:22:48:9	a: satc.net CNAME content.xbox.
1299	60.458452	192.1( 🗄 Internet Protocol	l, src: 192.168.137.1 (19	02.168.137.1), Dst: 192.168.137.136 (192.168.137.13)	5)
1319	60.570812	192.10 🕀 User Datagram Pro	otocol. Src Port: domain	(53). Dst Port: de-server (1256)	satc.net CNAME content.xbox.
1409	62.677511	192.10 Domain Name Syste	em (response)		
1410	62.730235	192.10 Domain Name Syste	em (response)		satc.net CNAME content.xbox.
1482	64.178937	192.10		III	
1484	64.229143	192.10 0000 00 00 00 00 11	5 C- 70 Ft 1 C1 05 FC		
1486	64.230667	192.10 0000 00 22 48 9a 1	.5 64 /2 TI 41 61 3T TO	08 00 45 00 . Hjra?E.	satc.net CNAME content.xbox.
1493	64.322787	192.10 0020 80 88 00 25 0	10 00 00 11 94 d3 C0 d8	91 90 00 01 5 VI	satc.net CNAME content.xbox.
1066	51.149253	192.1 0030 00 05 00 00 0	0 00 06 61 76 61 74 61	72 08 78 62 a vatar vh	
1075	51.396404	187.14 0040 of 78 oc 69 7	6 65 03 63 6f 6d 00 00	01 00 01 c0  oxlive c om	
1089	51.833343	192.1 0050 00 05 00 0	1 00 00 05 52 00 1f 06	61 76 61 74 D avat	•
1100	51 076393	107 1			

Fig. 5: Recepción de la respuesta al DNS query.

#### HTTP

La consola Xbox 360 tiene acceso a Internet por medio del protocolo HTTP; la conexión a internet se habilito para el juego en línea, descarga de actualizaciones, descarga del bazar de Xbox Live, el puerto destino al enviarse el paquete es el 80



#### Protocolo HTTP (80)

Fig. 6: Solicitud por el puerto 80

La respuesta es un mensaje de un tipo (PNG), el cual contiene la imagen del jugador en la lista de amigos, si esta llega sin ninguna complicación, vendrá acompañada de la palabra OK

	No.	Time	Source	Destination	Protocol .	Info	
j	1482	64.178937	192.168.137.136	192.168.137.1	DNS	Standard query A avatar.xboxlive.com	
	1484	64.229143	192.168.137.136	192.168.137.1	DNS	Standard query A avatar.xboxlive.com	
	1486	64.230667	192.168.137.1	192.168.137.136	DNS	Standard query response CNAME avatar.xboxlive.c	om.nsatc.net CNAME content.xbox.
1	1493	64.322787	192.168.137.1	192.168.137.136	DNS	Standard query response CNAME avatar.xboxlive.c	om.nsatc.net CNAME content.xbox.
1	1066	51.149253	192.168.137.136	187.141.2.104	HTTP	GET /avatar/Ddestr0y88/avatarpic-l.png HTTP/1.1	
j	1075	51.396404	187.141.2.104	192.168.137.136	HTTP	HTTP/1.1 200 OK (PNG)	
j	1089	51.833343	192.168.137.136	187.141.2.80	HTTP	GET /avatar/crash13955/avatarpic-l.png HTTP/1.1	
1	1102	51.976282	187.14				
j	1288	60.324957	192.16 1075 51.396404 18	7.141.2.104 192.168.137.136 HTTP	HTTP/1.1 20	0 OK (PNG) 🗖 🗉 🕳 🗠	
j	1308	60.492446	192.16	(COL 1	/ L		P/1.1
1	1315	60.522129	187.14 ± Frame 10/5	(694 bytes on wire, 69	4 bytes c	(aptured)	
1	1324	60.608573	192.16 Ethernet II	, Src: 72:f1:a1:61:3f:	f6 (72:f1	.:a1:61:3f:f6), Dst: Microsof_9a:15:6a (00:22:4 🛓	
1	1345	60.754671	187.14 🗄 Internet Pr	otocol, Src: 187.141.2	.104 (187	7.141.2.104), Dst: 192.168.137.136 (192.168.137	1
j	1348	60.778914	187.14 🕀 Transmissio	n Control Protocol. Sr	c Port: h	nttp (80), Dst Port: nbt-wol (6133), Seq: 6621.	
1	1418	62.794366	192.16	Lass - Concoll		0.00(4.00)) #4.000(4.00)) #4.004(4.00)) #4.000(4.00)	1
1	1432	62.936996	187.14	II		•	
j	1495	64.329322	192.16				
j	1510	64.429312	192.16 0000 00 22 4	3 9a 15 6a 72 f1 a1 6	1 3† †6 0	8 00 45 70 ."Hjra?Ep	P/1.1
1	1514	64.462153	187.14 0010 02 a8 /	1 86 40 00 3C 06 DT 3	3 00 80 0	2 68 CO a8t.@.<3n	
1	1537	64.670972	187.14 0020 89 88 0	<u>, 20 1/ 12 ac ec 80 e</u>	u 8e 8C 5	▼ 1 EL 50 18P	
1	6043	229.323556	fe80:: Erame (604 hider)	Reassembled TCD (7260 bytes)			
j	11974	359.972493	fe80::	neussembleu rer (7200 bytes)			
	44077	200.0204.04	6.00				

Fig. 7: Responde con la imagen y con estatus OK

El mensaje es de Tipo Internet Protocol, la dirección IP la cual envía la respuesta, corresponde al Router externo de Telmex (187.141.2.104), la respuesta llega a la dirección IP de la consola Xbox, por medio de la Laptop, los puertos utilizados son:

- Puerto Fuente http(80)
- Puerto Destino (63895)

#### Solicitud DHCPv6

El Protocolo de Configuración Dinámica de Host es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. De una manera más generalizada es un protocolo de tipo cliente-servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién utiliza una IP en particular, el tiempo que fue asignado, y a quien se le asigno después.

DHCPV6 se utiliza para IPv6, funciona de manera similar que para IPv4, se utiliza si el administrador de la red desea tener un control más personalizado de la asignación de direcciones IP.

En la captura de trafico de red, se utiliza observa que la LAPTOP solicita una asignación de dirección IPv6 al servidor DHCP, el cual se encuentra dentro del modem-ruteador 2WIRE de Infinitum.

La petición de asignación de dirección IPv6 se captura dentro del trafico de red del Xbox 360, ya que la consola Xbox se encuentra conectada de manera física a la Laptop, y ya que el Xbox también recibe una dirección IPv4 y IPv6 del modem-ruteador, entonces esta pasa por la Laptop, para finalmente llegar al Xbox, cabe destacar que ambas direcciones, tanto de la laptop como del

Xbox 360, se asignan dinámicamente, y es muy probable que si el modem-ruteador se reinicia, o se apaga y después de un periodo determinado de tiempo se vuelve a encender, estas direcciones serán diferentes a las anteriormente asignadas.

Filter			Egression Clear Apply	
No.	Time	Source	Destination Protocol . Info	
175	114301341	fe8011e35#1e29e1854	4 ff02 i 2 DHCPu5 Solicit	-
101	15.042837	fe80::e3be:e29e:854	4: ff02::1:2 DHCPV6 solicit	
232	17.054843	fe80::e3be:e29e:854	4:ff02::1/2 DHCPv6 Solicit	
434	21.063515	fe80::e3be:e29e:854	4:ff02::112 DHCPV6 Solicit	
640	29.066502	fe80::e5be:e29e:854	4:ff02::1:2 DHCPVé solicit	
962	45.072274	fe80::e3be:e29e:854	4:ff02::1:2 DHCPV6 solicit	
1756	77.083228	fe80::e5be:e29e:854	4: ff02::1:2 DHCPv6 Solicit	
16006	441.825103	fe80::e5be:e29e:854	4: ff02::1:2 DKPv6 solicit	
16045	5.442.825623	fe80::e5be:e29e:854	4: ff02::1:2 DKPv6 solicit	
16124	444, 838227	fe80::e5be:e29e:854	4: ff02::1:2 DKPv6 Solicit	
16275	448.847598	fe80::e5be:e29e:854	4: ff02::1:2 DKPv6 Solicit	
16596	456.850517	fe80::e5be:e29e:854	4: ff02::112 DKPvf Solicit	
17374	472.855930	fe8011e5be1e29e1854		
18796	504.867294	fe80::e5be:e29e1834		
1060	51.033091	192,168,137,118	In prase 15, 155 bottes on vice - 155 bottes contract()	
1062	1,089600	192.168.137.1	content of the state of the sta	xbox.
1081	51.716925	192,168,137,136	<pre>= strenet 11, SrC: /2:11:81:01:37:76 (/2:11:81:01:37:76), DSt: 1=V68C835_00:01:00:02 (33)</pre>	
1083	3 51,773461	192.168.137.1	a Internet Protocol Version 6	xbox.
1280	60.192021	192.168.137.136	user Datagram Protocol, Src Port: dhcpv6-client (546), Ost Port: dhcpv6-server (547)	
1284	60.245030	192, 168, 137, 1	content	.xbox.
1290	60.342322	192,168,137,136		
1290	60.396878	192.168.137.1	content.	.xbox.
1299	60.458452	192.168.137.136		
1319	60.570612	192.168.137.1	0020 b2 36 53 44 50 56 fr 02 50 50 50 50 50 50 50 50 50 50 50 50 50	xbox.
1409	62.677511	192.168.137.136	0030 00 00 00 01 07 01 02 03 13 00 00 10 14 10 10 1	
1410	62.730235	192,168,137,1	0040 "e f7 00 08 00 02 00 00 00 01 00 0e 00 01 00 02	. xbox.
1483	64 178017	101 168 117 116	insta in the second s	

#### Mensaje DHCPv6

Fig. 8: Petición de asignación de dirección DHCPv6.

Se observa que es un mensaje de tipo Internet Protocol Versión 6, y los puertos involucrados en este caso son:

- Puerto Fuente: dhcpv6-cliente (546)
- Puerto Destino: dhcpv6-servidor (547)

#### ICMPv6

El protocolo Mensajes de Control de Internet (Internet Control Message Protocol) es el protocolo de control y de notificación de errores que puedan existir en el Protocolo de Internet (IP). Su uso principal es enviar mensajes de error, por ejemplo, que un servicio, no está disponible, que la petición no recibió respuesta, o que un host o Router no puede ser localizado.

ICMPv6 es la implementación de ICMP para el Protocolo de Internet versión 6. Es una parte integral de IPv6, y se encarga del reporte de errores, de diagnostico de funciones (ejemplo tracert, ping), descubrir equipos vecinos en la red, y como un ambiente de trabajo para extensiones para implementaciones futuras del Protocolo de Internet.

Los mensajes de ICMPv6 son clasificados en 2 categorías, mensajes de error y mensajes de información, los primeros identifican cualquier problema en la red, ya sea de algún servicio deshabilitado, o de un equipo (Router) no encendido, mientras que el segundo reporta si un Router envió una petición a otro Router, o si se envió un broadcast dentro de la red.

Dentro del tráfico de red, encontramos paquetes de protocolo ICMPv6, el primer paquete contiene información de tipo "Router Advertisement", en el cual se reporta en un mensaje de información de un anuncio hacia el Router en la red, por parte de la Laptop.

No.	Time	Source	Destination	Protocol .	, Ma	
123/	64.0/09/2	18/,141,2,80	192,108,137,130	ntir	HEIP/1.1 200 OK (PMb)	
6043	229.32336	Te60::e3bere29e:8344:	ff02:::1	LUNPLE	kouter advertisement	
11974	359,972491	fe80::e5be:e29e:8544:	ff02::16	10/Pv6	Multicast Listener Report Message v2	
11977	360.020191	fe80::e5be:e29e:8544:	ff02::16	ICMPV6	Multicast Listener Report Message V2	
11980	360.034253	fe80::e5be:e29e:8544:	ff02::16	104PV6	Hulticast Listener Report Hessage v2	
11982	360,034853	fei0::e5be:e29ez				
11998	360.317187	fe60::e5be:e29e	3 229.323556 fe80:e5bee/2le/854	44:0066 #02:	02:1 ICMPv6 Router advertisement	
12000	360. 363941	fe80::e3be:e29e				
12004	360, 392431	fe80::e5be:e29e	ane 5013 (86 bytes on )	nice, Sb	86 bytes captured)	
12030	360.815420	fe80::e5be:e29e = Et	hernet 11, Src: 72:f1::	al:61:3f	3f:f6 (72:f1:a1:61:3f:f6). 0st: 1Pv6mcast_00:00:00:01 (33:33:0	
12069	361.814588	fe80::e5be:e29e	Destination: Thumerast	00:00:00	100:01 (33:32:00:00:01)	
12092	362.366087	fe80::e5be:e29e	Faundate The Start of the be	Ac 177.4	harmon (providence)	
12096	362, 387944	fe80::e5be:e29e	source: /2:11:42:01:31	16 (113	£171.81.01.37.FQ)	
12098	362.393385	fe80::eSbe:e29e	Type: IPv6 (0x86dd)			
12101	362,432603	fe80::e3be:e29e = 10	ternet Protocol version	n 6		
12101	362,441578	fe80::e3be:e29e	ternet Control Message	Protocol	col vi	
12105	367.442197	fe60::e5be:e29e	200-142-142-142-142-142-142-142-142-142-142			
12125	362.813328	fe80::e5be:e29e				
12126	362.817366	fe80::eSbe:eZ9e 0000	15 13 00 00 00 01 72	11 41.6	RADIAL STRATE STRATE STRATE	
12130	362.865208	fe80::e5be:e29e 0010	00 00 00 20 3a ff fe	80 00 0	00 00 00 00 00 e5 be	
12151	363.312504	fe80::e5be:e29e 0020	e2 9e 05 48 a0 06 ff.	02 00 0	00 00 00 00 00 00 00D.f.,	
17251	365.823752	fe80::e5be:e29e 0030	00 00 00 00 00 01 85	00 26 2	28 00 10 07 08 00 00 6(	
12485	369.817348	fe80::e5be:e29e 0040	00 00 00 00 00 00 01	01 72 1	an all all and a first control of the first firs	
13288	385.823018	fe80::e5be:e29e	THE CONTRACTOR OF THE			
14132	401.813042	fe80::e5be:e29e:85c41	1102:01	100910	Router ad entisement	

#### ICMPv6 Advertisement

Fig. 9 Anuncio al Router en la red

Otro paquete de tipo ICMPv6 dentro de la red capturado es uno con información de tipo "Router Solicitation", el mensaje describe la solicitud al Router enviado por la Laptop.

- 1						
	No.	Time	Source	Destination Protocol .	I., Info	
	12126	362.817366	fe80::e5be:e29e:8544:	ff02::16 ICMPv6	5 Multicast Listener Report Message v2	
	12130	362.865208	fe80::e5be:e29e:8544:	ff02::16 ICMPv6	5 Multicast Listener Report Message v2	
	12151	363.312504	fe80::e5be:e29e:8544:	ff02::16 ICMPv6	5 Multicast Listener Report Message v2	
	12251	365.823752	fe80::e5be:e29e:8544:	ff02::2 ICMPv6	5 Router solicitation	
	12485	369.817348	fe80::e5be:e29e:8544:	ff02::2 ICMPv6	5 Router solicitation	
	13288	385.823018	fe80::e5be:e29e:8544:	ff02::1 ICMPv6	5 Router advertisement	
	14132	401.813042	fe80::e5be:e29e:8544:	10051 005 000750 ( 00 5L 00 054		
	14856	417.818718	fe80::e5be:e29e:8544:	12251 305.823752 fe80::e5be:e29e:8544	44:aUbb ffU2::// ICMPVb Kouter solicitation	
	11975	359.972828	192.168.137.1	Ename 12251 (70 bytes on w	wine 70 bytes captured)	
	11978	360.020717	192.168.137.1	Prame 12251 (70 bytes off w	4 (4 (5 (5 (7) (4 (4 (5 (5 (5)) (5 (5 ))))))))))	
	11981	360.034406	192.168.137.1	Ethernet II, Src: /2:TI:al	a1:61:3T:T6 (/2:T1:a1:61:3T:T6), DST: 1PV6mCaSt_00:00:02 (33::	
	11983	360.035331	192.168.137.1	Destination: IPv6mcast_0	_00:00:00:02 (33:33:00:00:00:02)	
	11997	360.317023	192.168.137.1		.f6 (72:f1:a1:61:3f:f6)	
	12001	360.364161	192.168.137.1	Type: IPv6 (0x86dd)		
	12005	360.392933	192.168.137.1	Thternet Protocol Version	16	
	12029	360.816294	192.168.137.1	Thernet Protocol version		
	12093	362.366492	192.168.137.1	■ Internet Control Message P	Protocol Vo	
	12097	362.388470	192.168.137.1	•		
	12099	362.393613	192.168.137.1	0000 23 33 00 00 00 02 72 f	f1 a1 61 2f f6 86 dd 60 00 22 r a2 `	
	12102	362.433131	192.168.137.1	0010 00 00 00 10 3a ff fe 8	80 00 00 00 00 00 00 e5 be	
	12104	362.441825	192.168.137.1	0020 e2 9e 85 44 a0 66 ff 0	02 00 00 00 00 00 00 00 00p.f.	
	12106	362.442679	192.168.137.1	0030 00 00 00 00 00 02 85 0	00 39 dc 00 00 00 01 01 9	
	12124	362.813095	192.168.137.1	0040 72 f1 a1 61 3f f6	ra?.	
	12127	362.818334	192.168.137.1			

#### ICMPv6 Solicitation

Fig. 10 Solicitud al Router en la red

En ambos mensajes la dirección MAC fuente corresponde a la Laptop, esto indica que es dispositivo de origen dentro de la red de los mensajes de información ICMPv6.

#### IGMP

El Protocolo de Administración de Grupos de Internet (Internet Group Management Protocol) es un protocolo de comunicaciones usado por hosts y routers adyacentes en redes IP para establecer membrecías de grupos multicast.

Es parte esencial de las especificaciones de IP multicast, el cual consiste en un método de enviar datagramas IP a un grupo de clientes interesados en recibir una sola transmisión.

Es análogo al protocolo ICMP para conexiones unicast.

El protocolo IGMP tiene su uso en el servicio de Xbox Live, ya que es usado también para video y juego en línea, ya que permite un uso más eficiente de recursos ya que le da apoyo a estos tipos de aplicaciones.

En Xbox Live se pueden ver videos de juegos o películas, por Internet, pero principalmente su uso apoya el juego en línea del modo multijugador.

No.	Time	Source	Destination	Protocol 🗸	. Info
14856	417.818718	fe80::e5be:e29e:8544:	ff02::1	ICMPV6	Router advertisement
11975	359.972828	192.168.137.1	224.0.0.22	IGMP	V3 Membership Report / Leave group 224.0.0.252
11978	360.020717	192.168.137.1	224.0.0.22	IGMP	V3 Membership Report / Join group 224.0.0.252 for any sources
11981	360.034406	192.168.137.1	224.0.0.22	IGMP	V3 Membership Report / Leave group 224.0.0.252
11983	360.035331	192.168.137.1	224.0.0.22	IGMP	V3 Membership Report / Join group 224.0.0.252 for any sources
11997	360.317023	192.168.137.1	224.0.0.22	TGMP	V3 Membership Report / Join group 224.0.0.252 for any sources
12001	360.364161	192.168.137.1	11975 359.972828 192.168	137.1 224.0.0	.0.0.22 IGMP V3 Membership Report / Leave group 224.0.0.252
12005	360.392933	192.168.137.1			
12029	360.816294	192.168.137.1	∎ Frame 11975 (54 by	tes on w	wire, 54 bytes captured)
12093	362.366492	192.168.137.1	Ethernet II Src	72 · f1 · a1	a1:61:3f:f6 (72:f1:a1:61:3f:f6) Dst: TPV4mcast 00:00:16 (01:00:5e)
12097	362.388470	192.168.137.1	Destination: TD	Amenet Of	00:00:16 (01:00:50:00:00:16)
12099	362.393613	192.168.137.1	B Deschiacton. IPV	411CaSt_0	
12102	362.433131	192.168.137.1		:61:31:10	:f6 (/2:f1:a1:61:3f:f6)
12104	362.441825	192.168.137.1	Туре: IP (ОхО8ОС	)	
12106	362.442679	192.168.137.1	Internet Protocol.	Src: 192	192.168.137.1 (192.168.137.1), Dst: 224.0.0.22 (224.0.0.22)
12124	362.813095	192.168.137.1	Thternet Group Mar	agement (	t Protocol
12127	362.818334	192.168.137.1	in incernee droup mar	agemente	
12131	362.865731	192.168.137.1	1		
12150	363.312302	192.168.137.1	0000 01 00 5e 00 00	16 72 f1	f1 a1 61 3f f6 08 00 46 00 A r a2 E
11988	360.145699	fe80::e5be:e29e:8544:	0010 00 28 12 3f 00	00 01 02	02 = 68 = 60 = 60 = 60 = 60 = 60 = 60 = 60
11989	360.145975	192.168.137.1	0020 00 16 94 04 00	00 22 00	00 fa 01 00 00 01 03 00".
12010	360.504324	fe80::e5be:e29e:8544:	0030 00 00 e0 00 00	fc	
12011	360.504880	192.168.137.1			
12111	362.547925	fe80::e5be:e29e:8544:			
10110	262 540242	100 160 107 1			

#### IGMP

Fig. 11 Reporte de "membrecía" de un grupo multicast.

La dirección IP fuente pertenece a la Laptop, la dirección IP destino es la de algún servidor remoto, el cual envía un mensaje a un grupo interesado, el mensaje es de tipo multicast, y la Laptop es un cliente de ese grupo interesado en recibir el mensaje.

También podemos observar que para efectos de rendimiento a la hora de recibir mensajes, la Laptop, el cliente, abandona el grupo, cuando no está interesado en recibir el mensaje que envía el servidor, después de un cierto periodo de tiempo, cuando el cliente este interesado en volver a recibir el mensaje del servidor, envía un mensaje, y se vuelve a unir al grupo, para recibir el o los mensajes que envié el servidor a ese grupo de cliente.

No.	Time	Source	Destination	Protocol .	Info
14830	41/.818/18	Te80::e5De:e29e:8544:	TTU2::1	TCWAAP	KOUTER AGVERTISEMENT
11975	359.972828	192.168.137.1	224.0.0.22	IGMP	V3 Membership Report / Leave group 224.0.0.252
11978	360.020717	192.168.137.1	224.0.0.22	IGMP	V3 Membership Report / Join group 224.0.0.252 for any sources
11981	360.034406	192.168.137.1	224.0.0.22	IGMP	V3 Membership Report / Leave group 224.0.0.252
11983	360.035331	192.168.137.1	224.0.0.22	IGMP	V3 Membership Report / Join group 224.0.0.252 for any sources
11997	360.317023	192.168.137.1	11070 260 020717 102 160 12	71224002	122 IGND V2 Mambarship Papart / Jain aroun 224 0.0 252 for any courses
12001	360.364161	192.168.137.1	M 113/0 200/020/11/ 135/100/12	/.1 224.0.0.2.	122 IOMP VS Membership Report / Join group 224.0.0.232 for any sources
12005	360.392933	192.168.137.1	Ename 11978 (54 hyp)	on wir	ine 54 bytes cantured)
12029	360.816294	192.168.137.1	E Fthennet II Sto (St by C		1.25.55 (72.51.11.51.25.56) Det. Thulmost 00.00.16 (01.00.50.0)
12093	362.366492	192.168.137.1	Ethernet II, Src: 7	(11:d1:0	(01:31:10 (/2:11:a1:01:31:10), USL: 1PV4mcaSt_00:00:10 (01:00:50:00
12097	362.388470	192.168.137.1	🗄 Destination: IPv4r	ncast_00:	0:00:16 (01:00:5e:00:00:16)
12099	362.393613	192.168.137.1	⊞ Source: 72:f1:a1:0	51:3f:f6	5 (72:f1:a1:61:3f:f6)
12102	362.433131	192.168.137.1	Type: IP (0x0800)		
12104	362.441825	192.168.137.1	Thternet Protocol (	tro: 102	2 168 137 1 (102 168 137 1) Det · 224 0 0 22 (224 0 0 22)
12106	362.442679	192.168.137.1	Thernet Frococor, .	SIC. 192.	2.100.157.1 (152.100.157.1), DSC. 224.0.0.22 (224.0.0.22)
12124	362.813095	192.168.137.1	HI INTERNET GROUD Manad	iement Pr	
12127	362.818334	192.168.137.1	1		
12131	362.865731	192.168.137.1	0000 01 00 5e 00 00 1	6 72 f1	a1 61 3f f6 08 00 46 00^ra?F.
12150	363.312302	192.168.137.1	0010 00 28 12 40 00 0	0 01 02	e8 cf c0 a8 89 01 e0 00 .(.@
11988	360.145699	fe80::e5be:e29e:8544	0020 00 16 94 04 00 0		f9 01 00 00 00 01 04 00"
11989	360.145975	192.168.137.1	0030 00 00 e0 00 00 f	c	
12010	360.504324	fe80::e5be:e29e:8544			
12011	360.504880	192.168.137.1			
12111	362.547925	fe80::e5be:e29e:8544:	tt02::1:3	LLMNR	Standard query ANY RAVEN-P
12112	362 548243	102 168 127 1	224 0 0 252	LEMND	Standard query ANY PAVEN_P

Fig. 12 Unión del cliente al grupo multicast.

#### LLMNR

El protocolo de Resolución de Nombres de Enlace Local Multicast (Link Local Multicast Name Resolution) está basado en DNS, permite resolución de nombres para hosts en el mismo enlace local.

#### Mensaje local LLMNR

No.	Time	Source	Destination	Protocol 🗸	Info			
12150	363.312302	192.168.137.1	224.0.0.22	IGMP	V3 Membership Report / :	Join group 224.0.0.252 for	any sources	
11988	360.145699	fe80::e5be:e29e:8544:	ff02::1:3	LLMNR	Standard guery ANY RAVE	N-P		
11989	360.145975	192.168.137.1	224.0.0.252	LLMNR	Standard query ANY RAVE	N-P		
12010	360.504324	fe80::e5be:e29e:8544:	0					1
12011	360.504880	192.168.137.1	11988 360.145699 fe80::e5	be:e29e:8544:	a066 ff02::1:3 LLMNR Standard quer	y ANY RAVEN-P		
12111	362.547925	fe80::e5be:e29e:8544:			(			
12112	362.548243	192.168.137.1	± Frame 11988 (8/ D)	/tes on wi	ire, 87 bytes captured)			
12135	362.969290	fe80::e5be:e29e:8544:	Ethernet II, Src:	72:f1:a1:	:61:3f:f6 (72:f1:a1:61:3f	:f6), Dst: IPv6mcast_00:0	L:00:03 (33:33	
12136	362.969686	192.168.137.1	🗄 Destination: IP	/6mcast_00	):01:00:03 (33:33:00:01:0	0:03)		
782	37.278991	65.55.71.169	■ Source: 72:f1:a	1:61:3f:f@	5 (72:f1:a1:61:3f:f6)			OCreator%3d%22w
811	38.204219	192.168.137.136		(dd)	(12111111111111111111)			
814	38.317095	65.55.71.169	Type. 19V0 (0x8	Juu)				
965	45.223345	65.55.71.169	Internet Protocol	Version 6	)			3\246%20%20\320'
994	47.762005	65.55.71.169	🗄 🗉 User Datagram Prot	tocol, Sro	: Port: 62888 (62888), Ds	st Port: llmnr (5355)		OCreator%3d%22w
1048	50.549451	192.168.137.136	Source port: 62	388 (62888	3)			
1049	50.629701	65.55.71.169	Destination port	· llmnr (	(5355)			
2560	110.778288	65.55.71.169	Lengths 22		(3333)			
2636	114.734321	65.55.71.169	Lengun: 55					
2638	114.953107	65.55.71.169	E Checksum: 0x0f1	5 [validat	tion disabled]			
2657	116.602939	65.55.71.169	🗄 🗄 Link-local Multica	ast Name P	Resolution (query)			3969
2659	116.606401	65.55.71.169						
2673	117.013972	192.168.137.136	·					mail.com
2677	117.101057	65.55.71.169	0000 33 33 00 01 00	03 72 f1	a1 61 3f f6 86 dd 60 0	0 33ra?`.		mail.com
2703	118.298085	65.55.71.169	0010 00 00 00 21 11	01 fe 80	00 00 00 00 00 00 00 e5 b	e!		
2705	118.319626	65.55.71.169	0020 e2 9e 85 44 a0	66 ff 02	0 00 00 00 00 00 00 00 0	0D.f	E	
2707	118.325019	65.55.71.169	0030 00 00 00 01 00	03 f5 a8	14 eb 00 21 Of 16 3f 2	9		msnobj%20Creator
2720	118.548495	192.168.137.136	0040 00 00 00 01 00	00 00 00	00 00 07 52 41 56 45 4	e	-	
2724	118.650223	65.55.71.169	[ <u>0050 07 50 00 00 ++</u>			D		
2062	126 006460	65 55 71 160	107 169 127 126	MCARAC	FIN rafaalant@hotmail c	nm		

Fig. 13 Consulta de Host Raven-P

#### MSNMS

Es un tipo de mensaje del Servicio de Messenger de la Red de Microsoft (Microsoft Network Messenger Service), se utiliza para conectarse un cliente al servidor MSN.

La consola Xbox 360 recibió una actualización la cual les permite a los usuarios de Xbox Live conectarse al servidor de MSN por medio de la consola.

No.	Time	Source	Destination	Protocol .	Info		
10106	362.363236	100.100.107.1	224 0 0 252	LEPHIN	Standard query Ant Neven 1		
12130	302.909080	192.108.13/.1	224.0.0.252	LLMNK	Standard query ANY RAVEN-F		- 0/2 -0/2 2
/82	37.278991	00.00./1.109	192.108.137.130	MSNMS	NLN NLN we lovech coche@hot	mail.com Sileno 2685403392 %3Cmsnobj%20Creato	^%30%22W(
811	38.204219	192.108.13/.130	05.55./1.109	MSNMS	SBP 27 6C25DUED-2Ca3-4a8D-	90/4-4C60/0CD1/48 MEN STIENO	
814	38.31/095	65.55./1.169	782 37 278001 65 55 71 160	102 168 137	136 MSNMS NUN NUN welovechicoche	Rhotmail.com Silano 2685403302 %3cmsnohi 🗖 🗖 🔀	a(20) 220)
965	45.223345	65.55./1.169	102 51:210551 05:55:11:105	152.100.157.	1250 MISHING HER HER WEIGVEENEGENE	ginoanan.com sileno 2005405552 /asensilobji	%20\320
994	4/./62005	65.55./1.169	Frame 782 (340 byt	es on wir	e. 340 bytes captured)		%30%22W(
1048	50.549451	192.168.13/.136	Cthornot II Sec	72.f1.a1.	61 · 2f · f6 (72 · f1 · 51 · 61 · 2f · f	6) Det: Microsof 02:15:62 (00:22:48:02:15:62	
1049	50.629/01	65.55./1.169	Ethernet II, Sic.	/2.11.d1.		0), DSC. MICLOSOL_94.13.04 (00.22.40.94.13.04	
2560	110.//8288	65.55./1.169	Destination: Mic	rosor_9a:	15:6a (00:22:48:9a:15:6a)		
2636	114./34321	65.55./1.169	🗄 Source: 72:f1:a1	:61:3f:f6	5 (72:f1:a1:61:3f:f6)		
2638	114.95310/	65.55./1.169	Type: IP (0x0800	)			
265/	116.602939	65.55./1.169	Thternet Protocol	Sect 65	55 71 160 (65 55 71 160)	Det: 102 168 127 126 (102 168 127 126)	
2659	116.606401	65.55.71.169	Incernet Protocory     Transmission Contra	-1		Det Det (422) (102) Crev 1 Adv 1 Ave	
2673	117.013972	192.168.137.136	Iransmission Contr	OI Protoc	:01, SFC POFT: MSNp (1863),	DST PORT: 1403 (1032), Seq: 1, ACK: 1, Len:	
2677	117.101057	65.55.71.169	🗄 MSN Messenger Serv	ice			
2703	118.298085	65.55.71.169					
2705	118.319626	65.55.71.169					
2707	118.325019	65.55.71.169					OCreator
2720	118.548495	192.168.137.136					
2724	118.650223	65.55.71.169					
3063	128.008480	65.55.71.169	4				
3481	149.557418	65.55.71.169					.com Kee
3495	151.547288	192.168.137.136	0000 00 22 48 9a 15	6a 72 f1	a1 61 3f f6 08 00 45 70	."Hira?Ep	
3496	151.605484	65.55.71.169	0010 01 46 27 ff 40	00 76 06	08 32 41 37 47 a9 c0 a8	.F'.@.v2A7G	%3cmsnoł
8806	290.802147	192.168.137.1	0020 89 88 07 47 04	08 09 c8	17 77 Of 9f 1a ce 50 18	GP.	
8920	293.799166	192.168.137.1	0030 ff ff aa 62 00	00 4e 4c	4e 20 4e 4c 4e 20 77 65	bNL N NLN we	
9056	296.811115	192.168.137.1	0040 6c 6f 76 65 63	68 69 63	6f 63 68 65 40 68 6f 74	lovechic oche@hot	
9212	299.849412	192.168.137.1	0050 6d 61 60 6c 20	62 6t 6d	20 52 60 6c 65 6o 6f 20	mail com Filopo	

#### Respuesta MSNMS

Fig. 14: Recepción de mensaje MSNMS del servidor MSN

En la captura anterior, se muestra la dirección IP (65.55.71.169) del servidor de MSN, la dirección IP contenida en el paquete de recepción puede variar si la conexión se realiza a un servidor diferente de Microsoft, de su servicio de Messenger, la dirección IP destino, es la de la consola Xbox 360, la cual recibe el mensaje del servidor de MSN.

También aparece la dirección MAC, pero esta pertenece a la Laptop, lo cual se explica de la siguiente forma: la consola Xbox 360 está conectada de manera alambrica al puerto Ethernet de la Laptop, la Laptop recibe el mensaje del servidor de MSN y después llega al Xbox 360, por lo tanto en el paquete capturado, se despliega como dirección MAC fuente.

Los puertos utilizados en esta transferencia de paquetes son:

- Puerto Fuente: msnp (1863), es el puerto del Protocolo de Notificación de Protocolo, es un protocolo de Mensajería Instantánea y es usado por Windows Live Messenger.
- Puerto Destino: iad3 (1032), este puerto sirve para utilizar el protocolo TCP/UP, el cual tiene varias utilidades, como la transferencia de mensajes por TCP (transacciones de software) y UDP (juego en tiempo real).

Ambos puertos deben estar habilitados tanto en el Xbox 360, como en la Laptop.

#### Envió MSNMS

No.	Time	Source	Destination	Protocol .	Info	
1150	2 200.142212	192.100.13/.1	224.0.0.232	LEPINK	Scalluar u quel y ANT KAVENTE	
1201	0 360.504324	fe80::e5be:e29e:8544:	ff02::1:3	LLMNR	Standard query ANY RAVEN-P	
1201	1 360.504880	192.168.137.1	224.0.0.252	LLMNR	Standard query ANY RAVEN-P	
1211	1 362.547925	fe80::e5be:e29e:8544:	ff02::1:3	LLMNR	Standard query ANY RAVEN-P	
1211	2 362.548243	192.168.137.1	224.0.0.252	LLMNR	Standard query ANY RAVEN-P	
1213	5 362.969290	fe80::e5be:e29e:8544:	ff02::1:3	LLMNR	Standard query ANY RAVEN-P	
1213	6 362.969686	192.168.137.1	224.0.0.252	LLMNR	Standard query ANY RAVEN-P	
78	2 37.278991	65.55.71.169	192.168.137.136	MSNMS	NLN NLN welovechicoche@hotmail.com Sileno 2685403392 %3cmsnobj%20Creator%3	d%22w(
81	1 38.204219	192.168.137.136	65.55.71.169	MSNMS	SBP 27 6c25b0eb-2ca3-4a8b-9074-4c607dcb1748 MFN Sileno	
81	4 38.317095	65.55.71.169	192.168.137.136	MSNMS	SBP 27 6c25b0eb-2ca3-4a8b-9074-4c607dcb1748 MFN Sileno	
96	5 45.223345	65.55.71.169				X ),
99	4 47.762005	65.55.71.169	811 38.204219 192.108.13	/.130 00.00./.	1.109 MSNMS SBP 2/ 0C2SDUED-2Ca3-4a8D-9U/4-4C0U/0CD1/48 MFN Sileno	
104	8 50.549451	192.168.137.136	E Enamo 811 (110 by	tos on wi	no. 110 bytes contured)	
104	9 50.629701	65.55.71.169	E FLAME OIL (ILU Dy	Les on wi	re, 110 bytes captured)	
256	0 110.778288	65.55.71.169	🗄 Ethernet II, Src:	Microsof	_9a:15:6a (00:22:48:9a:15:6a), Dst: 72:†1:a1:61:3†:†6 (72:†1:a1:61:3†:†6)	E
263	6 114.734321	65.55.71.169	🗄 Internet Protocol	, Src: 19	2.168.137.136 (192.168.137.136), Dst: 65.55.71.169 (65.55.71.169)	
263	8 114.953107	65.55.71.169	Transmission Cont	rol Proto	col. Src Port: jad3 (1032). Dst Port: msnp (1863). Seq: 1. Ack: 287. Len: 5	6
265	7 116.602939	65.55.71.169	Fource port: is	d2 (1022)		
265	9 116.606401	65.55.71.169	Source porc. ra	us (1032)		
267	3 117.013972	192.168.137.136	Destination por	t: msnp (	1863)	Ψ.
267	7 117.101057	65.55.71.169	(		III III III III III III III III III II	
270	3 118.298085	65.55.71.169		. (c. oo. o:		_
270	5 118.319626	65.55.71.169	0000 72 TI al 61 31	T6 00 24	2 48 9a 15 6a 08 00 45 00 ra? HjE.	~
270	7 118.325019	65.55.71.169			0 40 90 CU að 89 88 41 37 . X@, NA/	= )1
272	0 118.548495	192.168.137.136		47 01 91	1 14 LE U9 LO 10 90 DU 10 UUP.	
272	4 118.650223	65.55.71.169	0040 35 62 30 65 63	) 2d 22 6	2 30 20 32 37 20 30 03 32 7.030 P 27 0C2 2 61 32 34 61 38 63 34 500eb-3c a3-438b-	
306	3 128,008480	65.55.71.169		20 32 0	5 20 27 64 62 62 21 27 24 0074 Ac6 07dch174	Ψ.
348	1 149.557418	65.55.71.169	132.100.137.130	GUNICO	אבוע ועבוע וועמסטא דווויבעמדדעכטע נוופטער ט רפטוזמוומוונדומנעמווכנעמן טעווענדוכר דר כפווטנוומדד. כ	UIII KEI
349	5 151.547288	192.168.137.136	65.55.71.169	MSNMS	000/TU0	

Fig. 15: Envió de mensaje MSNMS al servidor MSN

El envió se realiza de la consola Xbox 360 (192.168.137.136) hacia el servidor de MSN (65.55.71.169), ahora cabe destacar que en este caso los puertos fuente y destino se invierten:

- Puerto Destino: msnp (1863)
- Puerto Fuente: iad3 (1032

De acuerdo a la captura realizada, también se destaca que las direcciones MAC fuente y destino cambiaron, la dirección MAC fuente corresponde a la consola Xbox 360, que es donde estamos conectados al servicio de Windows Live Messenger, la dirección MAC destino corresponde a la Laptop, que es donde el paquete llegara, para después salir hacia el Router, y seguir el camino hasta llegar al servidor de MSN.

#### SSDP

El Protocolo Simple de Descubrimiento de Servicios (Simple Service Discovery Protocol) es un protocolo utilizado para anuncios y descubrimiento de servicios de red y para información de la red.

Logra lo anterior sin asistencia de mecanismos de configuración basados en servidores como el protocolo DHCP o el DNS.

La consola Xbox 360 lo utiliza para percibir información de la red en que se encuentra conectada, ya que el protocolo SSDP es la base del de descubrimiento del Protocolo Universal de Plug and Play.

#### Paquete SSDP

-							
No.	Time	Source	Destination	Protocol .	Info		
349	5 151.547288	192.168.137.136	65.55.71.169	MSNMS	000/TU0		
349	5 151.605484	65.55.71.169	192.168.137.136	MSNMS	NLN BSY fanr4@hotmail.com	:-Osid:-O%20PunK%20para%20PoP's!!! 2789	003580 %3cmsnol
880	5 290.802147	192.168.137.1	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1		
892	) 293.799166	192.168.137.1	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1		
905	5 296.811115	192.168.137.1	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1		
921	2 299.849412	192.168.137.1	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1		
933	7 302.847248	192.168.137.1	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1		
945	4 305.857848	192.168.137.1	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1		
1148	2 349.892052	192.168.137.1	811 28 204210 102 168 127 1	26 65 55 71 1	60 MSNIMS SRD 27 6c25b0ab-2ca2-4a9	h-9074-4c607dch1749 MEN Silano	
1163	2 352.891860	192.168.137.1	11 30:204213 132:100:137:1	.10 00.00.11.1	105 MISINIMIS SDF 27 0C2500E0-2C85-480	5-3074-40070001740 WITN SITENO	
1179	355.902650	192.168.137.1	⊕ Erame 811 (110 bvte	s on wire	e. 110 bytes captured)		
1192	9 358.943707	192.168.137.1	S Fthermot IT Ency M	icrosof (	0.15.62 (00.22.48.02.15.62	) pett 72,f1,s1,61,2f,f6 (72,f1,s1,61,	25.55
1207	5 361.955432	192.168.137.1	Ethernet II, Sic. M	1010301_5	9a.15.0a (00.22.40.9a.15.0a	(), DSC. 72.11.a1.01.51.10 (72.11.a1.01.	51.10)
1221	3 364.966209	192.168.137.1	∃ Internet Protocol,	Src: 192.	.168.13/.136 (192.168.13/.1	.36), Dst: 65.55./1.169 (65.55./1.169)	
1236	L 368.006872	192.168.137.1	🗉 Transmission Contro	1 Protoco	ol, Src Port: iad3 (1032),	Dst Port: msnp (1863), Seq: 1, Ack: 287	', Len: 56 💷 📄
1253	L 371.014981	192.168.137.1	Source port: iad3	(1032)			
1266	4 374.014163	192.168.137.1	Destination port	msnn (18	863)		
1330	3 386.144256	192.168.137.1	[Stroom index: 1]	manla (11			
1350	2 389.146495	192.168.137.1	[Stream muex, 1]				
1370	4 392.157141	192.168.137.1	Sequence number:	1 (re	lative sequence number)		·
1383	7 395.197489	192.168.137.1	•		III		
1395	5 398.194640	192.168.137.1	0000 72 f1 a1 61 3f f	6 00 22	48 92 15 62 08 00 45 00	га? "ніс	
1410	) 401.205722	192.168.137.1	0010 00 60 58 f1 00 0	0 40 06	4e 96 c0 a8 89 88 41 37	`χ. @. ΝΔ7	<u></u>
1782	7 484.603520	192.168.137.1	0020 47 a9 04 08 07 4	47 Of 9f	1a ce 09 c8 18 95 50 18	GP.	E
1782	3 484.604551	fe80::e5be:e29e:8544:	0030 Be cc 62 d8 00 0	00 53 42	50 20 32 37 20 36 63 32	>.b5B P 27 6c2	
1782	9 484.605442	192.168.137.1	0040 35 62 30 65 62 2	2d 32 63	61 33 2d 34 61 38 62 2d	5b0eb-2c a3-4a8b-	
1783	) 484.606153	fe80::e5be:e29e:8544:	0050 20 20 27 24 24 3	24 62 26	20 27 64 62 62 21 27 24	0074 4c6 07dcb174	
1783	L 484.606949	192.168.137.1	239.200.200.200	SSUP	NUILFY ^ HIIP/1.1		
1783	2 484, 607506	fe80::e5be:e29e:8544:	ff02::c	SSDP	NOTTEY * HTTP/1.1		

Fig. 16 Petición de tipo M-SEARCH

En la figura anterior se muestra el envió de una petición SSDP M-SEARCH, esta petición es usada para la búsqueda de aparatos o de tipos de aparatos que concuerden con los parámetros especificados en la función de consulta de descubrimiento. El proveedor SSDP obtiene los documentos de descripción de aparatos que respondan a la petición SSDP M-SEARCH.

Después de procesar los documentos de descripción, el SSDP regresa las instancias correspondientes a los aparatos principales, y aunque los documentos de descripción describen tanto como servicios y aparatos, los servicios son ignorados y solo los aparatos son enumerados.

#### тср

El protocolo de control de transmisiones se encarga del servicio de intercambiar datos de manera directa entre 2 hosts de red, de manera particular, TCP provee una entrega confiable y ordenada de un flujo de bytes de un programa (aplicación o juego de video) de un equipo de red a otro equipo, es el protocolo en el cual la mayoría de las aplicaciones de Internet se apoyan.

Durante la captura de tráfico de red en el Xbox 360, se observaron 2 cosas:

1.- La transmisión de datos durante el inicio de sesión en el bazar de compras de Xbox live, se realizo por medio de https; cualquier transacción involucrando datos personales del usuario de Xbox live se realiza de manera segura, todo paquete que se envié, debe recibir su respuesta correspondiente de manera sincronizada y en un rango de tiempo determinado, en otras palabras se usa https para transacciones sensibles de seguridad en Xbox Live.

2.- El intercambio de paquetes de red entre la consola Xbox 360 y el servidor de Xbox live, contiene, entre varios artículos en línea, imágenes descargables, escenas de videojuegos, primeros

vistazos al desarrollo de un juego, videos de títulos que saldrán próximamente, y envió de mensajes de voz, de video o de texto a otros jugadores de la comunidad.

Estos mensajes deben de enviarse y recibir su respuesta de manera correcta y ordenada, sin que se pierda ningún paquete en el proceso, si llegase a ocurrir esto, se deben enviar el número de paquete donde se quedo la transferencia, y después reenviarse los paquetes perdidos en el camino, se usa TCP porque todo paquete necesita llegar a su correspondiente destino.

No. Ten	te:	Source	Destination	Protocol .	lefe -			
20110 970	U_U+107+		11Means	5507	MALLET TRAFTLACK			
18117 490	0.642180	192/168-137/1	239.255.255.250	550P	NOTIFY * HTTP/1.1			
19118 490	0.642581	fe80::e5be:e29e:8544:	ff02::c	SSOP	NOTIFY * HTTP/1.1			
0.43	612698	69659110717	NUMBER BOARD	10.0	Https > 41414 (451.	ACCURATE ACCURATE	rin-0 Len-0	
783 37.	. 279266	192.168.137.136	65.55.71.169	TCP	tad3 > msrp [ACK] 5	en+1 Ack+287 win+16	5076 Lenv0	
815 38.	. 317391	192.168.137.136	65.55.71.169	TCP	fad3 > msrp [ACK] 5	ep+57 Ack+343 Win+1	6020 Len=0	
966 45.	. 222649	192.168.137.136	65.55.71.168	TC#	iad3 > msrp [ACK] 5	40-57 Ack-664 Min-1	5699 140-0	
995 47.	.762305	192,168,137,136	65.55.71.16			And a second second second second		
1050 50.	. 630002	192,168,137,136	65.55.71.16	0 4.01,295 03 34 155.7	132.168.152.138.1CP https://	41514 (RSI, ACK) Seq=1 Ac	ck=1 Winco Lmc0	THE PARTY OF
1063 51.	.099708	192,168,137,136	167, 141, 2, 1		And Person and Person in the Person of the P	Contraction of the second second		
1064 51.	136498	187,141,2,104	192, 168, 137	174-2 B (34 B)D	e or enter se pares	Capital sal		a a construction and a second second
1065 51.	136802	192, 168, 137, 136	187,141.2.1	Ethernet II, Sro	c: 72:11:a1:61:31:16	(72:11:41:61:31:16	<li>b), Dst: Microsof_9a:15</li>	5:6a (00:22:48:9
1067 51.	.187650	187.141.2.104	192,168,137 0	Internet Protoco	1, SFC: 65.54.186.7	9 (65.54.188.79), 6	BI: 192.168.137.136 (1	97.168.137.136)
1068 51.	339528	187.141.2.104	192,168,133 =	Transmission Col	tro] Frotocol, Src	Fort: https (443).	Dot Fort: 41814 (41814	), 540: 1, Ack:
1069 51.	351296	187.141.2.104	192,168,133	Chiera nort - 1	PPAR (412)	Carl of the second s		Contraction of the second s
1070 51.	351595	102.168.137.136	187,141 2.3	source porc. 1	1443			
1071 51.	363161	187, 141, 7, 104	192, 168, 133	pestimation po	WI: 41814 (41814)			
1072 51.	376917	187, 141, 2, 104	192, 168, 133	[Stream index:	: 0)			1.0
1073 51.	177215	192,168,117,136	187,141,7,1	Sequence number	er: 1 (relative s	equence number)		
1074 51.	390690	187,141,7,104	197, 168, 137	Arknow]estrienes	st number: 1 (rel	ative ark mather)		
1076 51	396702	192.165.137.135	167 141 2 1	Desider Jacobi	20 h.e.s	all the sea tensor ?		
1077 51	466229	192, 168, 137, 136	187,141,2,1	enalities installed	The first are			
1078 51.	490919	187.141.2.104	197, 168, 137	CONTRACTOR OF A	And the second second second		273 aug - 114	
1079 51.	.491225	192,168,137,135	187,141 2 2 000	00 10 22 45 94	15 ca 72 fl al fit :	s fe os co 45 po	The Private Contract	
1064 51.	783705	192, 168, 137, 136	187, 141, 2 8 000	10 00 28 24 1a	40 00 ff 06 11 ff 4	41 36 bit 4F c0 all	. (5.0	
1065 51	820351	187, 141, 2, 80	197,168,133 00.	20 89 88 01 50	ai 16 00 02 11 lif 1	15 68 43 60 50 14	·····V································	
1086 51.	820650	102.168.137.136	187,141,2,8 00	30 00 00 el 21	00.00		and a second	
1097 51.	.879176	187,141,2,80	197,168,133					
1093 51.	911056	187,141,2,80	192, 168, 132					
1070 SL 1071 SL 1072 SL 1072 SL 1073 SL 1074 SL 1076 SL 1076 SL 1077 SL 1078 SL 1078 SL 1085 SL 1085 SL 1092 SL 1093 SL	.351395 .351361 .375912 .375912 .375912 .396502 .465229 .460919 .490215 .491225 .783705 .420931 .820630 .879378 .911056	152, 168, 137, 136 187, 141, 2, 104 187, 141, 2, 104 192, 168, 137, 136 192, 168, 137, 136 192, 168, 137, 136 192, 168, 137, 136 192, 188, 137, 136 187, 141, 2, 80 187, 141, 2, 80 187, 141, 2, 80	187, 141, 2, 1 190, 168, 137 190, 268, 137 190, 268, 137 190, 268, 137 190, 268, 137 190, 268, 137 197, 268, 137 197, 168, 137 197, 198, 197 197, 198 197,	Source port: - Destination pr Stream index Sequence made Acknowledgemen Header lacoth Header lacoth 00 00 22 45 40 00 00 27 25 10 00 00 27 21	ntyp (v=2) rt: 41814 (41814) : 0] rr: 1 (relative s rt number: 1 (rel : 01 horse 11 et c? (d c1 c1 14 et c? 00 c0 00 c0 00 00 c0 00 c0	equence number) attive ack number) 	10 (F. 1461 A) 13 (F. 1461 A) 14 (F. 1461 A) 15 (F. 1461 A) 15 (F. 1461 A)	- •

#### TCP (HTTPS)

Fig. 17 Paquete TCP HTTPS (Modo Seguro)

En la captura el paquete utiliza protocolo https para recibir la respuesta del servidor de Microsoft, el cliente que recibe la respuesta es la consola Xbox 360, los puertos involucrados son:

- Puerto Fuente (443): Puerto de Hypertext Transfer Protocol Secure (HTTPS), es una combinación del protocolo HTTP combinado con el protocolo de seguridad y encriptación SSL/TLS; https se encarga de encriptar datos y de crear un canal seguro sobre una red no segura.
- Puerto Destino (41814): Puerto destino del servidor de Xbox Live, debido a la naturaleza de https no hay demasiada información sobre este puerto, mas que es un puerto de uso libre dependiendo la aplicación que lo utilice.

La dirección MAC destino corresponde a la consola Xbox 360, la dirección MAC fuente corresponde a la Laptop, utiliza internet Protocol versión 4, su TTL es de 255, el TTL (Time to Live) es el límite en el periodo de tiempo o numero de iteraciones en transmisiones de redes que una unidad de datos puede experimentar antes de ser descartada.

Para este mensaje se utilizan identificadores de tipo Acknowledgement, el cual se utiliza para verificar que la comunicación sea constante y no se pierdan paquetes

#### TCP (HTTP)

No.	Time	Source	Destination	Protocol .	Info
995	4/./02305	192.108.13/.130	03.33./1.109	ICP	Jad3 > webb [ack] ed=>\ vck=apt wiu=tpatp reu=n
1050	50.630002	192.168.137.136	65.55.71.169	TCP	iad3 > msnp [ACK] Seq=63 Ack=959 Win=16917 Len=0
1063	51.099708	192.168.137.136	187.141.2.104	ТСР	nbt-wol > http [SYN] Seq=0 Win=17212 Len=0 MSS=1324 WS=0
1064	51.136498	187.141.2.104	192.168.137.136	ТСР	http > nbt-wol [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 WS=5
1065	51.136802	192.168.137.136			
1067	51.187650	187.141.2.104	1003 21:033/08 135:108:131	.136 187.141.	2.104 ICP nbt-wol > http [SYN] Seq=0 Win=1/212 Len=0 MSS=1324 WS=0
1068	51.339528	187.141.2.104	T Frame 1062 (66 buts	c on win	a 66 hytos capturad)
1069	51.351296	187.141.2.104	E Frame 1005 (00 Dyte	SOLIWIN	e, oo bytes captured)
1070	51.351595	192.168.137.136	🖃 Ethernet II, Src: M	icrosof_9	9a:15:6a (00:22:48:9a:15:6a), Dst: 72:t1:a1:61:3t:t6 (72:t1:a1:61:3t:t6)
1071	51.363161	187.141.2.104	Destination: 72:f	1:a1:61:	3f:f6 (72:f1:a1:61:3f:f6)
1072	51.376912	187.141.2.104	Source: Microsof	9a:15:6a	(00:22:48:9a:15:6a)
1073	51.377215	192.168.137.136	TVDA: TP (0x0800)		
1074	51.390690	187.141.2.104	Triternet Destacel	Cnc. 103	168 117 136 (103 168 117 136) Det. 187 141 3 104 (187 141 3 104)
1076	51.396702	192.168.137.136	Incernet Prococol,	SPC: 192.	.108.13/.130 (192.108.13/.130), DSL: 18/.141.2.104 (18/.141.2.104)
1077	51.466229	192.168.137.136	Transmission Control	l Protoco	ol, Src Port: nbt-wol (6133), Dst Port: http (80), Seq: 0, Len: 0
1078	51.490919	187.141.2.104	Source port: nbt-	wol (6133	3)
1079	51.491225	192.168.137.136	Destination port:	http (80	0)
1084	51.783705	192.168.137.136	[Stream index: 2]		-7
1085	51.820351	187.141.2.80	[Scream muex. 5]		
1086	51.820650	192.168.137.136	sequence number:	0 (re	Tative sequence number)
1092	51.879176	187.141.2.80	Header length: 32	bytes	•
1093	51.911056	187.141.2.80	4		III +
1094	51.923043	187.141.2.80			
1095	51.923354	192.168.137.136	0000 72 fl al 61 3f	F6 00 22	48 9a 15 6a 08 00 45 00 ra?" HjE.
1096	51.934729	187.141.2.80	0010 00 34 59 6T 00 1	00 40 06	19 2T CO 88 89 88 DD 80 .4YO
1097	51.949163	187.141.2.80	0020 02 08 1/ 15 00		05 2c 01 02 02 00 01 01 cz
1098	51.949467	192.168.137.136		JU UZ U4	
1099	51.962412	187.141.2.80	0040 04 02		
1100	51.974055	187.141.2.80			

Fig. 18: Paquete TCP

Los puertos utilizados en este caso son:

- Puerto Fuente: nbt-wol (6133): usado por el servidor de Xbox live.
- Puerto destino (80): como se describió anteriormente es el puerto del servicio HTTP.

En este caso el paquete tiene como dirección MAC destino la correspondiente a la Laptop, y como fuente la dirección MAC de la consola Xbox 360.

Este paquete describe una descarga de un ítem de Xbox live, el ítem es gratuito por lo tanto no necesita modo https, sin embargo no debe haber errores en la transferencia del ítem, es decir todo lo que se envía debe llegar.

El análisis de los paquetes de red y los protocolos utilizados, así como los puertos usados en las transferencias de datos y establecimiento de sesiones multijugador, ayuda al ingeniero en redes a hacer el análisis para determinar el modelo de calidad de servicio mas adecuado para implementarse en la red.

En el modelo a implementar de QoS, se tendrá en cuenta este análisis para saber qué porcentaje de ancho de banda es necesario para que cualquier transacción que se realice entre el usuario y el servidor sea completada sin retrasos, sin deficiencia de banda y sin pérdida de paquetes, lo último es muy importante a considerar en el modelo de QoS, ya que existen transferencias las cuales todos sus paquetes deben de llegar y enviar, se debe asegurar el ancho de banda para esas transferencias, así como permitir que la sesión de juego tenga calidad optima, que todos los paquetes lleguen en el tiempo que deben llegar, y que otras aplicaciones no le quiten ancho de banda a la sesión principal de juego.

El análisis de tráfico de Xbox se realizo durante una sesión activa de juego en línea.

#### **INSTALACION DE GNS3**

Primero descargamos la versión del software más actualizada, esta la encontramos en el sitio WEB: http://www.gns3.net/

Google" Custor Graphical Network Simulator	Search
Home News RSS Docs Team Screenshots Forum	n Blog Download
Ads by Google Cisco IOS Router Lab Cisco Router Cisco CCIE Lab	
What is GNS3 ?	
GNS3 is a graphical network simulator that allows simulation of complex networks.	DOWNLOAD
To allow complete simulations, GNS3 is strongly linked with :	
Dynamips, the core program that allows Cisco IOS emulation.	
<ul> <li>Dynagen, a text-based front-end for Dynamips.</li> <li>Qemu, a generic and open source machine emulator and virtualizer.</li> </ul>	Sponsored Link
GNS3 is an excellent complementary tool to real labs for network engineers, administrators and people wanting to pass certifications such as CCNA, CCNP, CCIP, CCIE, JNCIA, JNCIS, JNCIE.	Free CCIE Voice Training
It can also be used to experiment features of Cisco IOS, Juniper JunOS or to check configurations that need to be deployed later on real routers.	Attend Free CCIE Voice vLectures We've Certified 1700+ CCIEs
This project is an open source, free program that may be used on multiple operating systems, including Windows, Linux, and MacOS X.	Contact IPexpert.com/CCIE Ads by Google

#### Damos click en la ventana de Download:



## Download

Below you can download GNS3, a network simulator for making topologies of routers (IOS, JunOS), firewalls (ASA, PIX). It is particularly useful for training to Cisco certifications (CCNA, CCNP, CCIP, CCSP, CCVP or CCIE) or Juniper certifications (JNCIA, JNCIS or JNCIE).

Cisco OEM GLC-SX-MM New, Factory Sealed, In Stock Special \$294.00 (866)913-5252 www.CiscoGLC.com Free CCIE Voice Training Attend Free CCIE Voice vLectures We've Certified 1700+ CCIEs Contact IPexpert.com/CC Cursos LINUX LPI - GREEN Modo texto/terminal, Debian, RedHat Sistemas, Redes, Samba, FireWall www.green.com.i Ads by Google

#### Windows

- · GNS3 v0.7.2 all-in-one (includes Dynamips, Qemu/Pemu, Putty and WinPCAP 4.1.1)
- GNS3 v0.7.2 binary

#### MacOS X

GNS3 v0.7.2 DMG package (experimental and Intel x86-64 only, includes dynamips).

#### Sources

- . GNS3 v0.7.2 zip
- · GNS3 v0.7.2 tgz
- GNS3 v0.7.2 bz2

source forge	a de -13-072 win32-alt in sincese de -onto-vo-2 at s	
Find Software Develop Create Project	Adventencie de seguridad de Descarge de archivos	
Your GNS3 download will start Problems with the download? Check your box	Se edd nig 0.22 Aver 0.22 Aver 0.22 Aver 0.22 Aver 0.22 Aver 0.22 Aver 1.22 Aver	
Cisco*	Arreue les archives procedentes de Hamer pueden ier bles, ess teo de archives puedentes de Hamer pueden ier bles, ess ingen, no escubé ri guade este arthrese. <u>Coutes at issue</u> Template-driven. Eavy to use Your code. Yout way, Faster	
There are only 20,000 in the world	Join Them!	

Seleccionamos la opción de Windows all-in-one:

Después de elegir el directorio donde se guardara el archivo, y descargarlo, lo ejecutamos para instalar el software:



Aceptamos el acuerdo de licencia:

() GNS3 0.7.2 Setup	23
License Agreement Please review the license terms before installing GNS3 0.7.2.	3
Press Page Down to see the rest of the agreement.	
GNU GENERAL PUBLIC LICENSE Version 2, June 1991	
Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.	
Preamble	
The licenses for most software are designed to take away your	-
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install GNS3 0.7.2.	
Nullsoft Install System v2.44	
< Back I Agree Cancel	

Elegimos el directorio de instalación:

() GNS3 0.7.2 Setup	
Choose Start Menu Folder Choose a Start Menu folder for the GNS3 0.7.2 shortcuts.	
Select the Start Menu folder in which you would like to create the program's sh can also enter a name to create a new folder.	ortcuts. You
Accessories Administrative Tools Bloodshed Dev-C++ CCleaner Colasoft Capsa 7 Free CyberLink DVD Suite CyberLink MediaShow CyberLink PowerDVD 8 CyberLink YouCam Dia Games HP	T
Nullsoft Install System v2.44	Cancel
Seleccionamos los componentes a Instalar del software:

() GNS3 0.7.2 Setup		
Choose Components Choose which features of GNS	3 0.7.2 you want to install.	
Check the components you wa install. Click Next to continue.	nt to install and uncheck the com	ponents you don't want to
Select components to install:	<ul> <li>✓ WinPCAP 4.1.1</li> <li>✓ Dynamips 0.2.8 RC2</li> <li>✓ Qemu 0.11.0 patched</li> <li>✓ GNS3</li> </ul>	Description Position your mouse over a component to see its description,
Space required: 56.6MB		
Nullsoft Install System v2.44	< Back	Next > Cancel

# Directorio de Instalación:

(i) GNS3 0.7.2 Setup	
Choose Install Location	
Choose the folder in which to install GNS3 0.7.2.	50
Setup will install GNS3 0.7.2 in the following folder. To install in a diffe and select another folder. Click Install to start the installation.	erent folder, click Browse
Destination Folder C:\Program Files\GNS3	Browse
Space required: 56.6MB Space available: 232.2GB Nullsoft Install System v2.44 ABack	nstall Cancel

Esperamos mientras procede la instalación:

() GNS3 0.7.2 Setup	
Installing Please wait while GNS3 0.7.2 is being installed.	5
Extract: qemuwrapper.exe	
Extract: dynamips-start.cmd Extract: gns3.exe Extract: gns3.ico Extract: libgcc_s_dw2-1.dll Extract: mingwm10.dll Extract: msvcr90.dll Extract: putty.exe Extract: python26.dll Extract: pywintypes26.dll Extract: qemuwrapper.exe	▲ ■
Nullsoft Install System v2.44	Cancel

Lanzamos el GNS3 al finalizar la instalación:

() GNS3 0.7.2 Setup	
	Completing the GNS3 0.7.2 Setup Wizard
	GNS3 0.7.2 has been installed on your computer.
	Click Finish to close this wizard.
	< Back Finish Cancel

🔸 GNS3		
File Edit View Help		
📑 🗷 🖀 🏝 🛸 🔀	] 😣 🛯 🧳 🖬 🕨 👖 🔳 🗁 🖼	
Nodes Types 🗗 🗙	^	Topology Summary 🗗 🗙
Router c1700     Router c2600     Router c2691     Router c3700     Router c3700     Router c7200     PDX firewall     ASA firewall     Juniper router     Ethernet switch     ATM switch     Frame Relay switch     Ins		
Qemu host	۲	
Cloud	Console 8 ×	1
	Dynagen management console for Dynamips (adapted for GNS3) Copyright (c) 2008 GNS3 Project =>	

Ejecutamos el software y nos despliega la pantalla principal:

Cargamos el IOS a utilizar en nuestra simulación:

OS Images	External hypervisors		
Images			
IOS image	Model/Chassis		
Settings			Hypervisors
Image file :			Use the hypervisor manager
	-2700		
Distance	1. 2. (11)		
Platform:	(5)00		
Platform: Model:	3725		
Platform: Model: IDLE PC:	3725		
Platform: Model: IDLE PC:	3725	r minimum PAM requireme	
Platform: Model: IDLE PC: Default RAM:	3725 0 MB 🔶 <u>Check fo</u>	r minimum RAM requireme	• ent
Platform: Model: IDLE PC: Default RAM: Ø Default ima	3725 0 MB 🔶 Check for age for this platform	r minimum RAM requireme	• ent
Platform: Model: IDLE PC: Default RAM: Ø Default ima	3725 0 MB 🔹 <u>Check fo</u> age for this platform	r minimum RAM requireme	• ent

S Images Exter	G C CNA >	•	67 Buscar CCNA	P
IOS images	Organizar 👻 Nueva car	peta	8	••••••
100 millige	Documentos ^	Nombre	Fecha de modifica	Tipo
	🔛 Imágenes	3 CBT Nuggets	02/08/2010 04:31	Carpeta de archivos
	Música	🕌 Colasoft Administrar Red	30/09/2010 06:01	Carpeta de archivos
	Videos	🕌 Packet Tracer 5.1	02/08/2010 04:31	Carpeta de archivos
	1 Equipo	C3640-JK.BIN	11/10/2006 09:13	Archivo BIN
	A Disco local (C:)	capturaLIVE	05/08/2010 09:57	Wireshark capture
Settions	RECOVERY (D:)	GNS3-0.4.1_documentation_spanish	30/08/2010 07:13	Adobe Acrobat D
Je vangs	HP TOOLS (E)	GNS3-0.5-tutorial	02/10/2010 02:28	Adobe Acrobat D
Image file :	- DARKRAVENM (C =	D P Communicator	17/08/2010 04:56	Adobe Acrobat D
Platform:	DARKRAVENMA		19/08/2010 10:33 a	Adobe Acrobat D
Model		Sybex.CCNA.Cisco.Certified.Network.Ass	26/09/2007 12:11	Adobe Acrobat D
	🗣 Red			
IDLE PC:		< [		
Default RAM:	Nomb	C2540-IV RIN	- All Glass (5.2)	
Default image fe	Nomo	C3040-36.5814	* [Pair tiles ( ; ; )	
			Abrir	Cancelar

Seleccionamos el directorio donde se encuentra la versión del IOS a cargar en el simulador:

Configuramos el Dynamips para el correcto funcionamiento del simulador:

General	Dynamips	
Dynamips		
Capture	Dynamips Hypervisor Manager	
Qemu	Settings	
	Executable path:	
	dynamips-wxp.exe	
	Working directory:	
	C:\Users\Raven\AppData\Local\Temp	
	Automatically clean the working directory	
	Base port: Base UDP: Base console:	
	7200	*
	Enable ghost IOS support	
	Tenable mmap support	
	✓ Enable JIT sharing support (Dynamips > 0.2.8 RC2)	
	Enable sparse memory support	
	Test Dynamips successfully started	

Con el IOS, iniciamos la simulación del Router.



Por medio de la línea de comandos configuramos las interfaces del Router, así como su manejo básico de administración de red:

	KA KA	
ſ	B Dynamips(1): R9, Console port	۲.
	Press RETURN to get started!	^
	*Mar 1 00:00:04.479: %LINK-4-NOMAC: A random default MAC address of 0000.0c04.7 ael has been chosen. Ensure that this address is unique, or specify MAC addresses for commands (such as 'novell routing') that allow the use of this address as a default.sslinit fn	7
	<pre>*Mar 1 00:00:11.927: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-NullO , changed state to up *Mar 1 00:00:11.927: %LINEPROTO-5-UPDOWN: Line protocol on Interface IPv6-mpls, changed state to up *Mar 1 00:00:14.979: %SYS-5-RESTART: System restarted Cisco IOS Software. 3600 Software (C3640-JK9035-M), Version 12.4(10a), RELEASE S</pre>	5
con S3 P	OFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2006 by Cisco Systems, Inc. Compiled Wed 11-Oct-06 20:52 by prod_rel_team *Mar 1 00:00:14.991: %SNMP-5-COLDSTART: SNMP agent on host Router is undergoing a cold start Router>	4 III

## GNS3 EN MODO DE ALTO RENDIMIENTO.

Paso 1:

Windows: Abrir el administrador de tareas y ordenar por porcentaje de CPU. Linux: Abrir una ventana de consola y teclear el comando *top*.

Paso 2:

En GNS3, iniciar una nueva topología con solo 1 ruteador Iniciar el ruteador Abrir la consola. Cuando el ruteador esté totalmente arriba, configurar lo siguiente:

Código: Router>enable Router#conf t Router(config)#line con 0 Router(config-line)#exec-timeout 0

Paso 3:

De vuelta en el administrador de tareas, tomar nota del consumo del CPU usado por Dynamips.

Paso 4:

En GNS3, dar click derecho en el ruteador y elegir idle-pc

Cuando encontremos un valor marcado con un asterisco, anotarlo, si aparecen múltiples valores, anotar todos ellos y elegir uno de los que aparezcan.

Paso 5:

Tomar nota de la utilización del CPU para Dynamips en el Administrador de Tareas. Estimar aproximadamente el valor del consumo del CPU de 15 a 20 segundos. Anotarlo al lado de la tabla de los valores de idle-pc del GNS3

Paso 6:

Seleccionar el valor de *idle-pc* de la lista de los posibles valores el cual se aproxime mas al consumo registrado del CPU el cual se obtuvo del paso anterior, y darle click en seleccionar valor, el cual será el valor más aproximado al porcentaje de CPU usado por ese ruteador, de una lista de 1 o más valores óptimos posibles en el GNS3.

Paso 7:

Verificar que GNS3 guardo el mejor valor posible para las imágenes de los ruteadores que estamos usando, esto es en:

Edit->IOS Images and Hypervisors

Seleccionamos la imagen que estamos usando y verificamos el valor de *idle-pc,* el cual debe ser el que seleccionamos anteriormente.

Ahora GNS3 automáticamente usara ese valor en cualquier nueva topología que creemos.

Paso 8:

Si se tiene alguna topología ya salvada anteriormente que use esta imagen de IOS, abrir el archivo .net y reemplazar el valor *idle-pc* encontrado por nuestro nuevo valor optimo de *idle-pc*.

CONEXIÓN DE ROUTER EN GNS3 A INTERNET

Primero revisamos que Dynamips este correctamente instalado y configurado:		
F	572	P

General	Dynamips
Dynamips	
Capture	Dynamips Hypervisor Manager
Oemu	Settings
<b>~</b>	Executable path:
	dynamips-wxp.exe
	Working directory:
	C:\Users\Raven\AppData\Local\Temp
	Automatically clean the working directory
	Base port: Base UDP: Base console:
	7200 😧 10000 😧 2000 🗣
	Enable ghost IOS support
	Enable mmap support
	Enable sparse memory support
	Test Dynamips successfully started

Debemos cargar la imagen de la versión de IOS del Router que virtualizaremos dentro de GNS3:

Images       Model/Chassis         I27.0.0.1:C:\Users\Raven\Desktop\CCNA\C3640-JK.BIN       3640         127.0.0.1:G:\FelipeDelValle\c2800nm-adventerprisek9-mz.124-25d.bin 3725       3725         Settings	OS Images Ex	ternal hypervisors	
IOS image       Model/Chassis         127.0.0.1:C\Users\Raven\Desktop\CCNA\C3640-JK.8IN       3640         127.0.0.1:G\FelipeDelValle\c2800nm-adventerprisek9-mz.124-25d.bin       3725         Settings       Hypervisors         Image file :       C:\Users\Raven\Desktop\CCNA\C3640-3K.8IN         Platform:       c3600         Model:       3640         IDLE PC:	Images		
127.0.0.1:C:\Users\Raven\Desktop\CCNA\C3640-JK.BIN       3640         127.0.0.1:G:\FelipeDelValle\c2800nm-adventerprisek9-mz.124-25d.bin       3725         Settings	IOS image	*	Model/Chassis
127.0.0.1:G:\FelipeDelValle\c2800nm-adventerprisek9-mz.124-25d.bin 3725         Settings         Image file :       C:\Users\Raven\Desktop\CCN4\C3640-X.8DN         Platform:       c.3600         IDLE PC:         Default RAM:       128 M8         Image for this platform	127.0.0.1:C:\Us	ers\Raven\Desktop\CCNA\C3640-JK.BIN	3640
Settings Image file : C:\Users\Raven\Desktop\CCNA\C3640-XK.BIN Platform: c3600 Model: 3640 IDLE PC:  Default RAM: 128 MB C Check for minimum RAM requirement @ Default image for this platform	127.0.0.1:G:\Fe	ipeDelValle\c2800nm-adventerprisek9-mz.124-25d.b	in 3725
Model: 3640   IDLE PC: Default RAM: 128 MB  Check for minimum RAM requirement Default image for this platform	Settings	C:\Lisers\Raven\Desktop\CCNA\C3640-X.8IN	Hypervisors Use the hypervisor manager
IDLE PC: Default RAM: 128 MB C <u>check for minimum RAM requirement</u> Default image for this platform	Platform:	c3600	-
Default RAM: 128 MB Check for minimum RAM requirement C Default image for this platform	Platform: Model:	c3600 3640	•
Default image for this platform	Platform: Model: IDLE PC:	c3600 3640	•
	Platform: Model: IDLE PC: Default RAM:	c3600 3640 128 MB Check for minimum RAM require	• ements

3.- Seleccionamos un modelo de Router compatible con el IOS que cargamos, y también seleccionamos una nube, la cual representara la interfaz de red física a la cual se conectara nuestro Router virtual:



4.- Configuramos la nube para que esté conectada a la interfaz de red Ethernet de nuestra computadora: seleccionamos en la pestaña de "Generic Ethernet" la interfaz de red física a la cual nos conectaremos, esta debe estar conectada al Modem ADSL con conexión a Internet, le damos click en "Add" para agregar el controlador, después en "Apply" y finalmente en "Ok":

• Node configurator	5 <mark>x</mark>
Clouds Cl	C1 node         NIO Ethernet       NIO UDP       NIO TAP       NIO UNIX       NIO VDE       NIO NULL         Generic Ethernet NIO (require Administrator access)       [rpcap:///Device/WPF_(2E035124-5BAA-4E4A-9717-492B42D94F06) : Network adapter 'Realtz •         c PCIe FE Family Controller' on local host: Conexión de área local       Add       Delete         nio_gen_eth:\device\npf_(2e035124-5baa-4e4a-9717-492b42d94f06)
Reset	OK Cancel Apply

5.- Por medio de una interfaz Fast Ethernet de nuestro router, conectamos un cable virtual Ethernet de nuestro router a la nube conectada a la tarjeta de red:



6.- Iniciamos el Router virtual y empezamos a configurarlo por medio de la línea de comandos del IOS:



7.- Configuramos una interface FastEthernet de manera que este habilitada para la conexión con la nube que representa la interfaz de la red real, ambas deben tener la dirección IP dentro de la misma subred:

C/Windows/system32/cmd.exe	Depaidog Summary     Topology Summary
Adaptador de Ethernet Conexión de área local:	
Sufijo RMS específico para la conexión : gateway.Zwire.net Descripción Realtek PCIe FE Pamily G	Controller
Dirección física	eforido) C1
Dirección IPv4: 192.160.1.64(Preferido) Máscara de subred: 255.255.255.255.45 Concesión obtenida: niércoles.05 de enero d 22258 a.a.	Dynamips(0): R1, Console port
La concesión expira	*Nar 1 00:00:26.463: %LINEPROTO-S-UPDOWN: Line protocol on Interface Fa Router>stEthernet1/0, changed state to down *Mar 1 00:00:26.467: %LINEPROTO-S-UPDOWN: Line protocol on Interface FastEthern
DUID de cliente DHCPv6	et2/0, changed state to down *Mar 1 00:00:26.467: %LINEFROTO-5-UPDOWN: Line protocol on Interface FastEthern et3/0, changed state to down Router>
Adaptador de túnel 6104 Adapter:	Router>
	Routerbenable Souterboof r
	Enter configuration commands, one per line. End with CNTL/Z.
	Router(config)#interface fast
	Router(config)#interface fastEthernet 0/0
	Router(config-if) #ip address 192.168.1.10 255.255.255.0
	Router(config-if) #no shutdown
4	Router (config-if) fend
Conscie	o up
Duranan management special for Duranities (advated for CNC2)	*Mar 1 00:05:03.259: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
Copyright (c) 2008 GNS3 Project	et0/0, changed state toend
->	Routers
	Router#

8.- Configuramos la ruta de los paquetes de red de nuestro Router virtual, será ruteo estático, dentro de esta también especificaremos la dirección IP de nuestra puerta de salida predeterminada:

🚱 Dynamips(0): R1, Console port	
Router(config-if)#ip address 192.168.1.10 255.255.255.0	
Router(config-if)#no shutdown	
Router(config-if)#end	
*Mar 1 00:05:02.259: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t	
oup	
*Mar 1 00:05:03.259: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern	
et0/0, changed state toend	
Router#	
Router#	
Router#	
*Mar 1 00:05:10.363: %SYS-5-CONFIG_I: Configured from console by console	
Router#	
Router#ip rou	
Router#ip rout	
Router#conf t	
Router#conf terminal	
Enter configuration commands, one per line. End with CNTL/Z.	
Router(config)#ip rout	
Router(config)#ip route	≡
§ Incomplete command.	
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.254	
Router (config) #	
Router (config) #	-

9.- Hacemos un ping a un servidor externo (sea 4.2.2.2) y verificamos que recibamos respuesta en nuestro Router:



10.- Hacemos un Ping a nuestra dirección IP asignada por nuestro ISP y a algún otro sitio de Internet, por ejemplo la IP de Google.com, y debemos recibir su correspondiente respuesta:

```
- 0 -X
B Dynamips(0): R1, Console port
Router#pi
*Mar 1 00:09:49.655: %SYS-5-CONFIG_I: Configured from console by consoleng
Protocol [ip]:
Target IP address:
Bad IP address
Router#
Router#ping 4.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/100/176 ms
Router#
Router#
Router#ping 66.102.7.104
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 66.102.7.104, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/129/204 ms
Router#
                                                                                  Ξ
Router#
Router#
Router#
```

Tener habilitado el router dentro de GNS3 es necesario para la creación de la VPN entre 2 equipos con 2 routers virtuales, la conexión a Internet es necesaria, ya que se creara un túnel seguro IPsec para el envió y la recepción de documentos, archivos y datos de manera segura entre 2 usuarios conectados por Internet.

# INTRODUCCIÓN A PORT SECURITY.

### ANTECEDENTES

Una característica sumamente importante en la seguridad de nuestras redes LAN es tener el control de que usuarios pueden y quienes no acceder a la red interna de la empresa.

Un escenario frecuente a resolver, es la posibilidad de conectarse a la red utilizando cualquier puerto libre en un Switch instalado en el edifico. La pregunta sería ¿Puede alguien que visite la empresa e ingrese al edificio, conectar una laptop a un puerto disponible y acceder a la red empresarial? Una medida importante podría ser deshabilitar aquellos puertos que no tienen en el momento una terminal de trabajo conectada. Pero también puede ocurrir que alguien desconecte una computadora conectada al Switch y conecte a ese puerto su propia laptop o un hub.

Este escenario es frecuente. Siempre hay un visitante a la empresa que requiera una conexión que es proporcionada sin respetar las políticas de seguridad de la empresa; o un trabajador de la misma que trae su propia laptop y decide conectarla a la red. La forma más fácil en que se logra esto es desconectando una terminal conectada a la red y utilizar ese puerto para ganar acceso a Internet.

Una medida para contrarrestar esto es implementar *port-security* en los switches de acceso.

Port-Security es una característica de los switches Cisco que les permite retener as direcciones MAC conectadas a cada puerto del dispositivo y permitir solamente a esas direcciones MAC comunicarse a través de ese puerto del Switch. Si un dispositivo con otra dirección MAC intenta comunicarse a través de ese puerto, port-security deshabilitara el puerto. Incluso se puede implementar SNMP para recibir en el momento en el sistema de monitoreo la notificación correspondiente al bloqueo del puerto.

## CISCO SWITCH PORT SECURITY.

Podemos usar la característica de Port Security para restringir la entrada a una Interfaz del Switch, limitando e identificando las direcciones MAC de las estaciones de trabajo que están permitidas para accesar al puerto. Cuando asignas un grupo de direcciones MAC seguras a un puerto seguro, el puerto no enviara paquetes con direcciones fuente fuera del grupo de las direcciones definidas como seguras. Si limitamos el número de direcciones MAC seguras a solo una y asignamos solo una dirección MAC segura, la estación de trabajo que esté conectada a ese puerto tiene asegurado el ancho de banda completo de ese puerto.

Si un puerto es configurado como un puerto seguro y el número máximo de direcciones MAC seguras es alcanzado, cuando la dirección MAC de alguna estación de trabajo tratando de accesar al puerto es diferente de alguna de las direcciones MAC identificada como seguras, una violación de seguridad ocurre. Si alguna estación de trabajo con una dirección MAC segura que fue aprendida en un puerto, intenta accesar a otro puerto seguro, una bandera de violación es activada.

Después de que se configuro el número máximo de direcciones MAC seguras en un puerto, las direcciones seguras son incluidas en una tabla de direcciones en una de estas maneras:

- Se pueden configurar todas las direcciones MAC seguras usando el comando de configuración de interfaces **switchport port-security mac-address** *mac\_address*
- Se puede permitir el puerto para dinámicamente configurar direcciones MAC seguras con las direcciones de los aparatos conectados.
- Se pueden configurar un número de direcciones y permitir al resto ser configuradas dinámicamente.

Nota: Si el puerto es desactivado o apagado, todas las direcciones aprendidas dinámicamente son removidas.

Después de que el número máximo de direcciones MAC es configurado, ellas son guardadas en una tabla de direcciones. Para asegurarse que un aparato conectado tiene todo el ancho de banda del puerto, se debe poner como número máximo de direcciones a solo una y configurar la dirección MAC contenida en el aparato conectado.

Una violación de seguridad ocurre si el número máximo de direcciones MAC seguras han sido agregadas a la tabla de direcciones y una estación de trabajo cuya dirección Mac no está en la tabla de direcciones intenta accesar a la interface.

Se puede configurar la interface en uno de 3 modos de violación: protegido, restringido o apagado.

Configuración por default de Port Security

Port Security: Desactivado en un puerto Número Máximo de direcciones MAC seguras: 1 Violation Mode: Apagado. El puerto se apaga cuando el número máximo de direcciones MAC seguras es excedido, y una notificación es enviada.

Recomendaciones para configurar Port Security:

- Un puerto seguro no puede ser un puerto trunco
- Un puerto seguro no puede ser un puerto de destino para Switch Port Analyzer (SPAN)
- Un puerto seguro no puede pertenecer a una interface EtherChannel.
- Debemos tener sumo cuidado cuando habilitemos port security en puertos conectados a switches adyacentes cuando hay enlaces redundantes entre los switches, porque port security puede deshabilitarlos debido a violaciones en la configuración de port security.

Configurando Port Security en una Interface:

Para restringir trafico a través de un puerto limitando e identificando la dirección MAC de las estaciones de trabajo habilitadas para usar el puerto, realizar esta tarea:

	Comando	Propósito
Paso 1	Router(config)# <b>interface</b> <i>interface_id</i>	Entra al modo de configuración y entra a la interfaz física a configurar, por ejemplo <b>gigabitethernet 3/1</b> .
Paso 2	Router(config-if)# switchport mode access	Habilita el modo de interface como acceso: una interfaz en el modo default no puede ser configurada como un puerto seguro
Paso 3	Router(config-if)# switchport port-security	Habilita el port security en la interfaz.
Paso 4	Router(config-if)# switchport port-security maximum valor	(Opcional) Habilita el numero maximo de direcciones MAC en la interfaz. El rango es de 1 a 128, el default es 128.
Paso 5	Router(config-if)# switchport port-security violation {protect   restrict   shutdown}	(Optional) Activa el modo violacion y la accion a ser tomada cuando una violacion sea detectada
Paso 6	Router(config-if)# switchport port-security mac-address direccion_MAC	(Opcional) Ingresa una direccion MAC segura a la interfaz.
Paso 7	Router(config-if)# end	Regresa al modo privilegiado EXEC
Paso 8	Router# show port-security interface interface_id	Verifica nuestras entradas.
	Router# show port-security address	

Cuando estemos configurando port security, notemos la siguiente información sobre la sintaxis acerca de los modos de violación de port security:

- protect: Descarta los paquetes con una dirección fuente desconocida hasta que removamos un número suficiente de direcciones MAC seguras para que sean menores que las del valor máximo
- restrict: Descarta los paquetes con una dirección fuente desconocida hasta que removamos un número suficiente de direcciones MAC seguras para que sean menores que las del valor máximo y causa que el contador de Seguridad/Violación se incremente.
- shutdown: Pone la interfaz en el estado de deshabilitarse al detectar error inmediatamente y envía una notificación.

Para regresar la interfaz a su condición por default (puerto no seguro) ingresar el comando no switchport port-security.

Para regresar la interfaz a su número por default de direcciones MAC seguras, ingresar el comando no switchport port-security máximum valor.

Para borrar una dirección MAC de la tabla de direcciones, ingresar el comando **no switchport port**security mac-address dirección mac.

Para regresar el modo violación a su condición por default (shutdown mode) ingresar el comando no switchport port-security violation {protocol | restrict}

Este ejemplo muestra como habilitar port security en la interfaz Fast Ethernet 12, y poner el número máximo de direcciones seguras a 5. El modo de violación es el default, y no hay direcciones MAC seguras configuradas.

### Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# interface fastethernet 3/12

Router(config-if)# switchport mode Access

Router(config-if)# switchport port-security

Router(config-if)# switchport port-security maximum 5

Router(config-if)# end

### Router# show port-security interface fastethernet 3/12

Security Enabled: Yes, Port Status: SecureUp

Violation Mode:Shutdown

Max. Addrs:5, Current Addrs:0, Configure Addrs:0

Este ejemplo muestra como configurar la dirección MAC segura en un puerto Fast Ethernet 12 y verificar la configuración.

#### Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# interface fastethernet 5/12

Router(config-if)# switchport mode access

Router(config-if)# switchport port-security

Router(config-if)# switchport port-security mac-address 1000.2000.3000

Router(config-if)# end

Router# show port-security Address

Secure Mac Address Table

-----

Vlan Mac Address Type Ports

--- -----1 1000.2000.3000 SecureConfigured Fa5/12

# INTRODUCCIÓN A VOIP.

Voz sobre Protocolo de Internet, también llamado Voz IP o VoIP (por sus siglas en inglés), es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet).

Esto significa que se envía la señal de voz en forma digital, en paquetes, en lugar de enviarla en forma digital o analógica, a través de circuitos utilizables sólo para telefonía como una compañía telefónica convencional o PSTN (sigla de Public Switched Telephone Network, Red Telefónica Pública Conmutada).

### Telefonía sobre IP

Para la implementación de Telefonía sobre IP, se pueden utilizar teléfonos especiales que puedan comunicarse a través de la red y a la vez poder proporcionar codificación y descodificación de audio en señales digitales. También existe software especializado, *Softphones*, que se encargan de simular los teléfonos IP.

Los Teléfonos IP son solo una parte de la integración total de voz sobre IP, para ello se necesita tener un modo de controlar las llamadas y direccionarlas de acuerdo a las características de las mismas, para ello se hace uso de equipos de centralización, en el caso de Cisco se utiliza el *Cisco Unified Communications Call Manager*, proveyendo la capacidad de transferir llamadas, reenviar llamadas, y realizar conferencias con múltiples usuarios.

Las características principales de esta tecnología en términos de tecnologías Cisco son:

- VOIP se refiere a una manera de llevar llamadas de teléfono sobre una red IP, ya sea en Internet o en nuestra propia red. Una atracción principal de VOIP es la habilidad de reducir gastos porque las llamadas de teléfono viajan a través de la red de datos en lugar de la línea de teléfono.
- Telefonía IP incluye los servicios de interconexión de teléfonos para comunicaciones, tales como conferencia, transferencia de llamadas, envió y en espera.
- Comunicaciones IP incluyen aplicaciones de negocios que mejoran las comunicaciones para habilitar presentaciones como mensajes unificados, centros de contactos integrados, y conferencia rica en recursos como voz, video y datos.
- Comunicaciones unificadas toman las comunicaciones IP un paso más allá usando tecnologías como SIP (Session Initiation Protocol) y presencia junto con soluciones móviles para unificar y simplificar todas las formas de comunicaciones, independientemente de la locación, tiempo o aparato.

VoIP y todos los recursos que tiene disponible pueden transformar la manera en que una empresa hace negocios con sus clientes.

# CISCO CALL MANAGER EXPRESS.

Instalación de Cisco Call Manager Express.

1.- Descargamos el archivo cme-x.x.x.zip del Cisco.com, siendo x.x.x.x la versión del software a descargar

Conclored Software	- Cisco Sustans - Windows Internet Evolut	-	- G -X
Comical Software	· Cisco systems · Windows internet Explor		0
	c//www.cisco.com/cisco/software/release.	timi:mahas2//642/622 • 😸 😁 🗙 🔟 Bing	P
Archivo Edición y	Eer Eavoritos Herramientas Ayuda		Data and the second
Pavontos 38 (	TouTube - Metallica Whi	=16Ltbs=1 -2-J1+Agregado a la cola 🖉 Sitios	sugendos • 🖉 Galeria de Web Slice •
88 🔹 🏉 Lillian 🛔	🚟 YouT 🔀 Lab 2 🗰 Do 🗙 🛞	All 7 S 😭 * 🔯 * 🔤 * Eágina	🔹 Seguridad 👻 Herramienţas 👻 🐏 🕶
		Worldeide change Log In	Account   Register My Cisco   *
Products & Service	es Support How to Duy	Training & Events Partners	्
	Cisco Unified Communications Manag	er Express	The Developed Court (2 James) (2) Hole
INOLOGY	Download Ooltware		TOWNERS THE (A REAR) (A LED
oftware	Release 8.6		Ξ.
General	+ Products > Voice and Unified Commu	nications > P Telephony > Call Control > Cisco Unified Co	mmunications Manager Express >
	Unified Communications Manager Exp	ress Complete Support File Set-0.6	
Autoes	10 V		
pgrade	Find Release Find	Related Information	
	Encoded (Change)	Sort By: File Name	-
d Operate	Copero es l Cose es		
0E		Download Now cme-151-411v1.zip	
	-0 85	Add to cart CME tar bundle for version 8.6	e
	- 0 80	5ize: 212504.72 KB (217696992	( bytes)
	🖹 😁 Al Releases		
	B-01 8X		
	8 🛄 8.5		
	8-00 8-2		
<			•
Listo		Internet   Modo protegido: activado	€ <sub>0</sub> ▼ 8,100% ▼

Descomprimir los archivos en una carpeta nueva:

<ul> <li>✓ Favoritos</li> <li>Biblico</li> <li>CME 8.5</li> <li>Mis archivos recibid</li> <li>Stios recientes</li> <li>Biblicotecas</li> <li>Documentos</li> <li>Imágenes</li> <li>Música</li> <li>Videos</li> </ul>	860 GUI mm-9971.9-1-15R1.tar mm-9951.9-1-15R1.tar -00-9-00.tar mm-9961.9-1-15R1.tar mm-9797-sip.9-1-15R1.tar mm-7975-sicp.9-1.15R1.tar	Image: Conterns - 7935-sccp.3-2-9.tar         Image: Conterns - 7935-sccp.9-1-15R1.tar         Image: Conterns - 7916-1-0-4.tar         Image: Conterns - 7915-1-0-4.tar         Image: Conterns - 7912-0-sccp.8-0-4.tar         Image: Conterns - 7912-0-sccp.8-0-4.tar	Organizar por: Carpeta = Come-tsp-2-2.0.5.zip 7970-71-75-Background-rea 7970-71-75-backgroundsv1.1 cucme-mipp.tar cucme-mipp.tar munic-on-bold au
Mis archivos recibid Stos recientes Bibliotecas Documentos Indigenes Misica Videos	8.6.0 GU rm-9971.9-1-15R1.tar rm-9951.9-1-15R1.tar -08-9-00.tar rm-9901.9-1-15R1.tar rm-7975-sip.9-1-15R1.tar rm-7975-scp.9-1.15R1.tar	mic ornterm-7935-sccp.3-2-9.tar       mic ornterm-7931-sccp.9-1-1581.tar       mic ornterm-79161-0-4.tar       mic ornterm-79151-0-4.tar       mic ornterm-79154-sccp.5-0-4.tar       mic ornterm-7912G-sccp.8-0-4.tar	cme-tsp-2.2.0.5.zip     7970-71-75-Background-rea     7970-71-75-backgroundsv1.     cucme-mlpp.tar     ingtones.tar     mouto-on-hold au
Equipo Equipo Equipo C:	trm-7970_7971-sip.9-1-15R1.tar trm-7945_7965-sip.9-1-15R1.tar trm-7945_7965-sip.9-1-15R1.tar trm-7945_7962-sip.9-1-15R1.tar trm-7942_7962-sip.9-1-15R1.tar trm-7942_7962-sip.9-1-15R1.tar trm-7941_7961-sip.9-1-15R1.tar trm-7941_7961-sip.9-1-15R1.tar	image: conterm=7911_3906-scc.ps-0-11581.tar           image: conterm=7910-scc.ps-0-7.tar           image: conterm=79005-scc.ps-0-2.tar           image: conterm=79005-scc.ps-0-2.tar           image: conterm=6921_41_61-scc.ps-0-1-1-0.tar           image: conterm=6921_41_61-scc.ps-0-1-1-0.tar           image: conterm=6921_6911-scc.ps-0-2-0.tar           image: conterm=6921_6911-scc.ps-0-2-0.tar           image: conterm=6921_6911-scc.ps-0-2-0.tar           image: conterm=6921_6911-scc.ps-0-2-0.tar           image: conterm=6921_6912_0_2_a.zip           image: conterm=692_69202_0_a.zip	

Instalar un servidor TFTP, tftpd32 es el recomendado, después de descargarlos lo instalamos y lo ejecutamos:

🏘 Tftpd32 by Ph. Jou	nin			x		
Current Directory C:\Users\Raven\Desktop\CCNA\TFT   Browse Server interface 192.168.1.68   Show Dir						
Tftp Server Tftp Clier	nt DHCP server	Syslog server	Log viewer			
peer	file	start time	progress			
	III					
About	<u>S</u> ettin	gs	<u>H</u> elp			

Un servidor TFTP nos servirá para transferir los archivos necesarios del Cisco Call manager Express a nuestro router, el cual los instalará en la memoria flash del router que tendrá el CME para la administración de la Voz sobre IP

La pestaña con la etiqueta "Current Directory", contiene la ruta del directorio donde se encuentran los archivos que se pueden transferir del servidor tftp a un cliente, ya sea otra computadora, o un equipo como el router cisco que tendrá instalado el CME.

La pestaña con el nombre de server interface, es la que nos informa de la dirección IP sobre la cual tiene su interface el servidor tftp, es decir, si un equipo desea conectarse al tftp, debe conectarse a esta dirección IP, para ellos deberá estar dentro del mismo segmento de red, o tener acceso autorizado para establecer una conexión activa con el servidor, nuestro router donde se instalará el CME debe ser capaz de alcanzar y establecer una dirección con esta IP.

También aparece en la ventana de trasferencias el receptor del archivo que se está transfiriendo, el nombre del archivo transmitiéndose o transmitido, el tiempo de inicio, y el progreso de la transmisión del archivo. Estos datos nos pueden ayudar a dar un estimado de cuánto tiempo y cuanto volumen del archivo falta que finalice una transferencia del archivo, así como los clientes conectados al servidor que están realizando operaciones.

Este servidor nos servirá para transferir todos los archivos al router desde nuestra computadora, también se pueden hacer copias de la configuración inicial de los routers, para que a la hora de

cargar su configuración, lo puedan hacer copiando los archivos del servidor tftp especificado, para que carguen con una configuración especifica.

Iniciamos GNS3 con un router cargado, y creamos una nube, la cual esta conectada a la interfaz de red física de nuestra computadora:



Iniciamos la configuración del router en el GNS3:

B Dynamips(0): R1, Console port
*Mar 1 00:03:30.891: %LINK-5-CHANGED: Interface Serial3/1, changed state to adm ^
inistratively down
*Mar 1 00:03:30.895: %LINK-5-CHANGED: Interface Serial3/2, changed state to adm
inistratively down
*Mar 1 00:03:30.895: %LINK-5-CHANGED: Interface Serial3/3, changed state to adm
inistratively down
*Mar 1 00:03:31.883: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to down
*Mar 1 00:03:31.887: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/0, changed state to down
*Mar 1 00:03:31.891: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et2/0, changed state to down
Router>
Router>
Router>enable
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#

Configuramos la interfaz FastEthernet del router virtual para que este en el mismo segmento de red que la dirección IP de la interfaz física de la computadora:

C:\Windows\system32\cmd.exe
Adaptador de LAN inalámbrica Conexión de red inalámbrica:
Sufijo DNS específico para la conexión : gateway.2wire.net Descripción Realtek RTL8191SE 802.11b/g/n WiF
Dirección física
Vínculo: dirección IPv6 local : fe80::d89:ef33:5de1:6d23x15(Preferido) Dirección IPv4 : 192.168.1.68(Preferido)
Pascara de subred
La concesion expira
Servidor DHCP
91-09-E7 Servidores DNS
Adaptador de Ethernet Conexión de red Bluetooth:

```
Dynamips(0): R1, Console port
o up
*Mar 1 00:13:19.551: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
Router(config-if)#
Router(config-if)#speed auto
Router(config-if)#
Router(config-if)#
Router(config-if)#end
Router#
Router#pi
*Mar 1 00:13:25.243: %SYS-5-CONFIG I: Configured from console by consoleng 192.
168.1.68
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.68, timeout is 2 seconds:
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/27/40 ms
Router#ping 192.168.1.68
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.68, timeout is 2 seconds:
                                                                                 11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/32/44 ms
Router#
```

En estas pantallas observamos que al enviar un ping de la interfaz de nuestro router a la dirección IP de la tarjeta física de la red, este llega y recibe su respuesta, por lo tanto el router virtual y la computadora con el servidor tftp están en la misma red, y puede establecerse una conexión activa entre los 2.

Procedemos a colocar los archivos del Call Manager Express en el directorio raíz de nuestro servidor tftp:

🗿 🕢 🗢 🕌 🕨 CCNA 🕨	TFTPD32 •		- + Buscar TFTPL	032	
Organizar 👻 Incluir en	biblioteca 👻 Compartir con 👻 Grab	ar Nueva carpeta		800 -	<b>1</b>
🔆 Favoritos	Nombre	Fecha de modifica	Tipo	Tamaño	
🐞 Descargas	🎉 cme-151-4Mv1	09/06/2011 08:12	Carpeta de archivos		
🎉 Mis archivos recibid	🊎 7970-71-75-backgroundsv1.tar	20/01/2009 04:01	PowerArchiver TA	626 KB	
Sitios recientes	🧱 cme-151-4Mv1.zip	25/05/2011 05:41	PowerArchiver ZIP	212,595 KB	
	🧱 cucme-mlpp.tar	09/01/2009 01:42 a	PowerArchiver TA	580 KB	
词 Bibliotecas	🖼 GUI.tar	09/06/2011 08:13	PowerArchiver TA	810 KB	
Documentos	053-08-9-00.tar	16/12/2010 02:17 a	PowerArchiver TA	998 KB	
Imágenes Música Videos Equipo Lisco local (C:) RECOVERY (D:) HP_TOOLS (E:) Red	Tftpd32-4.00-setup.exe	08/06/2011 04:50	Aplicación	547 KB	
7 elementos					

#### Iniciamos la transferencia de los archivos del servidor TFTP al router en GNS3:

archive tar /xtract tftp://x.x.x.x/cme-full-4.3.0.0.tar flash:"(X = TFTP direction IP del servidor o nombre del DNS)



Después de copiar los archivos de nuestro servidor tftp al router virtual, tecleamos los siguientes comandos para la instalación de CME y de sus componentes:

```
ip http server
ip http authentication local
no ip http secure-server
ip http path flash:/gui
!
username cisco privilege 15 secret cisco
!
telephony-service
web admin system name cisco secret cisco
dn-webedit
time-webedit
!
```

Con estos comandos preparamos el CME para empezar a levantar el administrador de las llamadas por medio de IP Communicator o cualquier otro teléfono IP, abrimos la ventada de administración:



Entramos a la página de configuración por medio de HTTP para el CME, al mismo tiempo verificamos que si accedamos a esta página, es que esta levantado CME en nuestro router, y podemos accesar a él desde nuestra PC:



Tener configurado Call Manager Express, así como su correcta instalación es necesario para el funcionamiento adecuado de nuestro servicio de VOIP, ya que administrara las llamadas de los IP Communicator, así como la asignación de los números de teléfono dentro de la LAN, sus identificadores y sus respectivos archivos de configuración.

# CISCO IP COMMUNICATOR.

### INSTALACIÓN DE CISCO IP COMMUNICATOR.

Darle click al icono de IP Communicator y esperar a que cargue los componentes

InstallShield Wizard	
	Preparing to Install
-	Cisco IP Communicator Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.
	Extracting: Cisco IP Communicator.msi
	Cancel

En la pantalla principal dar click en siguiente



Aceptar los términos de la licencia de usuario

B Cisco IP Communicator - InstallShield Wizard	×
License Agreement Please read the following license agreement carefully.	cisco
End User License Agreement	<b>^</b>
IMPORTANT: PLEASE READ THIS END USER LICENS AGREEMENT CAREFULLY. DOWNLOADING, INSTAL OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.	SE LLING
CISCO IS WILLING TO LICENSE THE SOFTWARE TO YO ONLY UPON THE CONDITION THAT YOU ACCEPT ALL	OU , OF –
<ul> <li>I accept the terms in the license agreement</li> <li>I do not accept the terms in the license agreement</li> </ul>	
InstallShield	Cancel

Seleccionamos la carpeta donde se instalara IP Communicator

😸 Cisco IP	Communicator - InstallShield Wizard	×
Destina Click Next	tion Folder to install to this folder, or click Change to install to a different folder.	cisco
	Install Cisco IP Communicator to: C:\Program Files\Cisco Systems\Cisco IP Communicator\	Change
InstallShield		
	< <u>B</u> ack <u>N</u> ext >	Cancel

Empezamos la instalación

B Cisco IP Communicator - InstallShield Wizard	×
Ready to Install the Program	ahaha
The wizard is ready to begin installation.	CISCO
Click Install to begin the installation.	
If you want to review or change any of your installation settings, exit the wizard.	dick Back. Click Cancel to
InstallShield	
< <u>B</u> ack Ir	nstall Cancel

Esperamos mientras se instalan los componentes

📸 Cisco IP (	P Communicator - InstallShield Wizard	
Installing The prog	gram features you selected are being installed.	
1 <del>1</del>	Please wait while the InstallShield Wizard installs Cisco IP Communicator. This may take several minutes.	
	Status: Copying new files	
InstallShield -	< <u>B</u> ack <u>N</u> ext >	Cancel

Al final debemos reiniciar el equipo, le damos en la opción de Si

😸 Cisco I	IP Communicator Installer Information	x
£	You must restart your system for the configuration changes made to Cisco IP Communicator to take effect. Click Yes to restart now or No if you plan to restart later.	
	<u>Y</u> es <u>N</u> o	

Después de reiniciar seleccionamos lo archivos de sonido

🕸 Audio Tuning Wizard	
	Select and Tune Audio Devices
<b>U</b> S	Before you begin:
	Close all other programs that play or record sound, such as Microsoft Sound Recorder.
	Make sure the audio devices (headset, speakers, microphone and handset) you wish to use are plugged in and turned on.
	If you are using a headset, position its microphone as close to your mouth as the headset manufacturer recommends.
	To continue, select Next.
	Back Next Cancel

Ahora debemos seleccionar la forma en que hablaremos y escucharemos la voz, es decir el aparato por el cual enviaremos y recibiremos la voz para cada modo de audio: tenemos las siguientes opciones:

- Headset
- SpeakerPhone
- Handset
- Ringer

Audio Tuning Wizard -	Select Audio Devices
For each audio mode, y audio devices and mod	ou must select the device you want Communicator to use. If you need help understanding es, see the user guide.
Headset:	Default Windows Audio Device 👻
Speakerphone:	Default Windows Audio Device 🔹
Handset:	Default Windows Audio Device 🔹
Ringer:	Altavoces (Realtek High Definit
	Back Next Cancel

Si el firewall nos manda mensaje, permitimos el acceso del IP Communicator

🔗 Alerta de segur	idad de Windo	ws	x
Firewa progra	ll de Windo ma	ows bloqueó algunas características de este	
Firewall de Windows públicas y privadas.	s bloqueó alguna	as características de AudioTuningWizard en todas las redes	
- AD	Nombre:	AudioTuningWizard	
108	Editor:	Cisco Systems, Inc.	
	<u>R</u> uta de acceso:	C:\program files\cisco systems\cisco ip communicator \audiotuningwizard.exe	
Permitir que AudioT	uningWizard se	comunique en estas redes:	
Redes privadas, como las domésticas o del trabajo			
Redes públic estas redes p	as, como las de públicas suelen t	aerop <u>u</u> ertos y cafeterías (no se recomienda porque ener poca seguridad o carecer de ella)	
¿Cuál es el riesgo de permitir que un programa pase a través de un firewall?			
		Permitir acceso Cance	elar

Después ajustamos el volumen y le damos clic en siguiente:

Audio Tuning Wizard - Adjust the Li	stening Volume for 'Altavoces (Realtek High Definit'
Adjust the Listening Volume	
Make sure you are listening to the pla to their maximum values before tunin sounds are being played at a comfor slider at 75% and then adjusting the	ayback device below. If your device has external volume controls, increase them ng. Press the <b>Play</b> button and then adjust the Volume sliders until the sample table level. If you see both a Master and a Wave slider, try setting the Wave Master slider to a comfortable level.
Playback device:	Altavoces (Realtek High Definit
Wave volume:	
Master volume:	
	Play
	Back Next Cancel

Ajustamos el volumen del micrófono y le damos click en siguiente

Audio Tuning Wizard - Adjust t	ne Microphone Volume for 'Micrófono (Realtek High Definit'
Adjust the Microphone Volu	me
Make sure you are speaking into the typical volume at which you v peaks at the highest yellow segn then adjust the Fine slider to a c when the volume sliders are set	the recording device listed below. Press the <b>Test</b> button and read this message at /ould speak while on a phone call. Adjust the volume sliders until the level meter nent. If you see both a Master and a Fine slider, set the Master slider at 75% and omfortable level. If the level meter does not peak above the green segments even to their highest levels, enable <b>Microphone Boost</b> if available.
, Recording device:	Micrófono (Realtek High Definit
Fine volume:	
Master volume:	
Playout	Test
	Back Next Cancel

Finalizamos el asistente de configuración de IP Communicator.

Audio Tur	ning Wizard
	You have now completed the Audio Tuning Wizard         Run this Wizard again if.         • You connect a new device         • Experience audio quality issues with your audio devices         • Change your audio settings in another program such as the Sounds and Multimedia Control Panel         This Wizard may reappear automatically when you launch Cisco IP Communicator if you have changed any of your audio settings outside the Wizard. You should choose Revert unless you wish to make changes to your audio settings.         To close this wizard, click Finish.
	Back Finish Cancel

Si nos aparece:

Cisco IP Communicator - Informati
Unable to reach TFTP server.
Aceptar

Debemos especificar los parámetros de nuestro servidor TFTP, estos parámetros incluyen

Adaptador de red: sirve para generar el nombre del aparato.

Nombre del Aparato: Nombre que lo identificará, en caso de usar otro nombre, marcar la casilla de "Use this Device Name" y teclear el nombre del equipo.

**TFTP Servers** 

Aplican:

- Usar los servidores TFTP por default
- Usar los servidores TFTP especificados en las direcciones IP por las cuales podemos accesar a ellos, introducirlas y darle en OK.

La imagen del IP Communicator es la siguiente:



Aplicación de IP Communicator

## CONFIGURACIÓN DE LOS SERVICIOS DE TELEFONIA DEL ROUTER.

Cisco Call Manager Express es una versión compacta de la aplicación Cisco Call Manager Server. Call Manager corre en un servidor dedicado, mientras que Call Manager Express corre en un router. CME posee muchas de las funciones básicas de CM, lo cual puede ser todo lo que se necesite en una red pequeña sin un gran número de teléfonos, así como también ofrece una solución menos costosa.

CM y CME ambos actúan como servidores cuya función principal es establecer llamadas entre teléfonos, así como también muchas otras funciones relacionadas con voz. Un teléfono IP Cisco instalado requiere ya sea la instalación de CME o de CM para dar servicios de telefonía a los teléfonos IP.

Teléfonos IP de Cisco dependen principalmente en CM o CME durante su secuencia de arranque y su procedimiento de marcación para obtener servicios de configuración y de directorio.

Para habilitar la funcionalidad de CME en un router Cisco ejecutando la imagen de CME instalado, usar el comando **telephony-service** en el modo de configuración global.

Configuración servicio de telefonía:

### R1(config)# telephony-service R1(config-telephony)#

En nuestra simulación dentro del laboratorio de pruebas, inicialmente solo tendremos 2 hosts ejecutando Cisco IP Communicator, por lo tanto configuramos el número máximo de teléfonos IP con 2, usando el comando **max-ephones "numero"**. Configuramos también el número máximo de números en el directorio para ser 10, usando el comando **max-dn "numero"**.

Configuración de número de teléfonos y de números en el directorio:

## R1(config-telephony)# max-ephones 2 R1(config-telephony)# max-dn 10

Configuramos el periodo de tiempo para mantener viva la llamada, en nuestro caso serán 40 segundos, con el comando **keepalive "segundos"**. Este temporizador especifica cuanto esperara CME antes de considerar que un teléfono IP no puede ser alcanzado y tomara acción para finalizar el registro de la llamada.

### R1(config-telephony)# keepalive 40

Configuramos el mensaje de sistema usando el comando **system message "mensaje"**. Este mensaje aparecerá en los teléfonos asociados con CME.

#### R1(config-telephony)# system message Cisco VOIP

Después, le decimos al router que genere los archivos de configuración para los teléfonos que están asociados con el CME usando el comando **create cnf-files**. Le puede tomar un par de minutos al proceso de configuración ser habilitado.

### R1(config-telephony)# create cnf-files

SCCP, siglas de Skinny Client Control Protocol, es un protocolo propiedad de Cisco entre CME y Cisco IP Phones, SCCP define una arquitectura fácil y simple de usar, está diseñado como un protocolo de comunicaciones para extremos-finales de hardware.

Finalmente, configuramos la dirección fuente para SCCP usando el comando **ip source address "dirección" port "puerto"**. Usamos la dirección local del puerto Fast Ethernet con el número de puerto de 2000.

### R1(config-telephony)# ip source-address 172.16.10.1 port 2000

Cuando la configuración de CME referencia a un "ephone", se está refiriendo a un teléfono Ethernet conectado vía una red IP. Un ephone representa el teléfono físico, y puede ser asociado con una dirección MAC y otras propiedades físicas. Un teléfono tiene asociada una dirección MAC única asociada, para identificar de manera única un ephone en la red, referirse a la dirección MAC.

En la capa lógica del modelo VOIP, un número de directorio representa un teléfono lógico asociado con un número de teléfono y un nombre. Un teléfono IP de Cisco puede ser asociado con más de un número de directorio a la vez, efectivamente haciéndolo un aparato multi-líneas con cada línea teniendo su propio número de directorio. Para configurar un numero de directorio, usar el comando en modo de configuración global **ephone-dn "marca"**. Usaremos una marca de 1 para el primer teléfono:

## R1(config)# ephone-dn 1

En el modo de configuración del ephone-dn, usar el comando **number "numero"** para configurar el número de teléfono con 5001. Asignamos el nombre de "Host a" con el comando **name** "**nombre**". Este será el numero de directorio asociado con el teléfono del Host A, el cual configuraremos en breve.

### R1(config-ephone-dn)# number 5001 R1(config-ephone-dn)#name Host A

De manera similar configuramos el ephone-dn 2:

### R1(config)# ephone-dn 2 R1(config-ephone-dn)# number 5002 R1(config-ephone-dn)#name Host B

De esta manera se han configurado 2 ephone en el router con CME instalado, los cuales se les asigno un número para recibir y enviar llamadas, así como una etiqueta que actúa como identificador de nombre.

Antes de continuar configurando los teléfonos en el router, se necesita averiguar la dirección MAC de los hosts. En un equipo con sistema operativo se puede averiguar de la siguiente forma

- Inicio
- Ejecutar
- cmd

En la ventana de comando teclear ipconfig /all

C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7600] Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Users\Raven>ipconfig /all
Configuración IP de Windows
Nombre de host : RAVEN-PC Sufijo DNS principal : Tipo de nodo : difusión Enrutamiento IP habilitado : no Proxy WINS habilitado : no Lista de búsqueda de sufijos DNS: gateway.2wire.net
Adaptador de Ethernet MS LoopBack:
Sufijo DNS específico para la conexión : Descripción Adaptador de bucle invertido de M icrosoft
Dirección física
Configuración automática habilitada : sí Vínculo: dirección IPv6 local : fe80::69a5:6ed5:4e3:e0df%20(Preferido) Dirección IPv4 de configuración automática: 169.254.224.223(Preferido) Máscara de subred : 255.255.0.0

La cadena de caracteres hexadecimal de nombre Dirección física es la dirección MAC de la interfaz, anotamos la dirección MAC de ambos hosts, ya que los necesitaremos después.

En R1, entramos en el modo de configuración global, y después tecleamos el comando ephone

### R1(config)# ephone 1

Asociamos la dirección MAC con este ephone usando el comando mac-address "dirección".

#### R1(config-ephone)# mac-address 2000.4c4f.4f50

Usamos el comando **type "tipo"** para configurar el tipo de teléfono, en este caso como estamos usando IP Communicator para simular teléfonos Ethernet, usamos cipc como el tipo

#### R1(config-ephone)# type cipc

Asignamos el primer botón en el teléfono al número de directorio 1 usando el **comando button** "línea". Este comando asigna botones a líneas de teléfono, el formato para el comando de botón que usamos es 1:1. El primer 1 indica el primer botón. El segundo 1 representa el número de directorio 1 previamente configurado.
### R1(config-ephone)# button 1:1

Aplicamos una configuración similar para ephone 2.

R1(config-ephone)# ephone 2 R1 R1(config-ephone)# mac-address 0009.5B1B.67BD R1 R1(config-ephone)# type cipc R1 R1(config-ephone)# button 1:2

Después de la instalación de IP Communicator en ambos hosts, en el host A, marcamos la extensión 5002, tecleando los números en el teclado o usando el teclado visual en el IP Communicator, después tecleamos la tecla Dial.

En el host B, debemos escuchar el ring del teléfono cuando recibimos la llamada, clic en la tecla Answer para contestar.

En ambos teléfonos, los contadores de llamada se incrementaran mientras dura la llamada.

# CONFIGURACIÓN DEL WIRELESS ACCESS POINT.

1.- Accedamos al WAP por medio de HTML, nos pedirá un nombre de usuario y un password para poder configurarlo

Certificat	te Error: Navigation Blocked - Windo	ws Internet Expl	lorer		
00-	E https://172.21.1.252/		✓ +→ ×	Scoogle	
🙀 Favorites	Certificate Error: Navigation Blocked	1	<u>ن</u>	🔂 - 🖃 🚔 - Page -	Safety - Tools - 🔞 - 🂙
Favorites	Certificate Error: Navigation Blocked There is a problem with this The security certificate presented by The security certificate problems may in server. We recommend that you close in Click here to close this webpage Continue to this website (not re More information	website's se this website wai this website wai Connect to 172. The server 172.21. User name: Password:	Curity certificate. s not issued by a trusted certificates issued for a different website's 21.1.252 1.252 at level_15_access requires a word. Cisco Cisco Cok Cancel	Ate authority. address.	Safety - Tools - Q - "
https://172.21.	1.252/			Internet	<i>√</i> <sub>1</sub> + € 100% +

2.- Configuramos la dirección IP, la asociación y la identidad de red, también tenemos las opciones de configurar los radios de transmisión, y vemos las direcciones MAC de los radios y de la interfaz FastEthernet.

▼ 2 1172.21.1	1.252	👻 😵 Certificate Er	or 🔯 😽 🗙 🎦 Google		
es 🏾 🄏 Cisco IOS Serie	es AP - Home		🏠 🔹 🔝 🚽 🖃 🖶 🔹 Bage 🔹 Safety 🔹 Tools		
sco	Cisco Air	onet 1240AG Se	eries Access Point 🛛 🕅 €		
SS SET-UP	Hostname AP		AP uptime is 6 hours, 54 min		
SS SECURITY ORK MAP	Home: Summary Stat	us			
IATION DRK	Association				
ACES	Clients: 1		Infrastructure clients: 0		
ES	Network Identity				
ESS SERVICES	IP Address		172.21.1.252		
LOG	MAC Address		0017.e095.3264		
	Network Interfaces				
	Interface	MAC Address	Transmission Rate		
	FastEthernet	0017 e095 3264	100Mb/s		
	Radio0-802.11G	0017.0fda.f260	54.0Mb/s		
	Radio1-802.11A	0017 0fde f260	54.0Mb/s		
	Event Log				
	Time	Severity	Description		
	Feb 18 20:35:02.580	Information	Interface Dot11Radio0, Station AP 0018.de92.f0f4 Reassociated KEY_MGMT[NONE]		
	Feb 18 20:35:02.578	Information	Interface Dot11Radio1, Deauthenticating Station 0018.de92.f0f4 Reason: Sending station has left the BSS		
	Feb 18 17:58:53.164	Information	Interface Dot11Radio1, Station AP 0018,de92,f0f4 Associated KEY_MGMTINONE1		

3.- Le asignamos un nombre de Host a nuesto WAP, y configuramos también si recibira una dirección IP por servidor DHCP o tendra una dirección IP estatica, también configuramos que se tratara de un access point.

🕞 🗢 😰 https://17	2.21.1.252/ap_express-setup.stitnl	💽 😒 Certificate Error 🛛 🐼 🍫 🗶 🔧 😋	ogle
avorites 🏾 🌈 Cisco IO:	i Series AP - Express Set-Up	🚺 • 🗟 -	🖂 🖶 🔹 Page 🔹 Safety 🔹 Tools 👻 🌘
CISCO	Cisco Airone	t 1240AG Series Access P	oint 🛛 🔤 🗃
DME PRESS SET-UP	Hostname AP		AP uptime is 6 hours, 57 minutes
PRESS SECURITY	Express Set-Up		
ISOCIATION ETWORK TERFACES ICURITY IRVICES RELESS SERVICES STEM SOFTWARE ENT LOG	Host Name: MAC Address: Configuration Server Protoc IP Address: IP Subnet Mask: Default Gateway: SNMP Community:	AP         0017.e095.3264         ol:       ○         DHCP       ③         Static IP         172.21.1.252         255.255.255.0         172.21.1.253         defaultCommunity         ④       Read-Only       ○         Read-Only       ○       Read-Write	
	Radio0-802.11G		
	Role in Radio Network:	Access Point     Repeater     Root Bridge     Workgroup Bridge     Universal Workgroup	up Bridge Client MAC:

4.- Configuramos el SSID, así como también si queremos que nuestro WAP aparezca en las señales inalámbricas, también configuramos si queremos asignarle un identificador de VLAN, y el tipo de seguridad que usaremos, ya sea estática WEP, por autentificación EAP o por WPA.

Cisco IOS Series AP - Express Secu	ırity Set-Up - Windows I	internet Explorer		
🚱 💽 🔻 🙋 latter (172.21.1.252) av	express-security(shiril)	👻 😵 Certificate Error	🛛 🚱 🍫 🗙 🚼 Google	<b>₽</b> -
🙀 Favorites 🦷 🌈 Cisco IOS Series AP - Ex	press Security Set-Up		🙆 • 🗟 - 🖻	🖶 🔹 Page 🗸 Safety 🗸 Tools 🕇 🕢 🕇
CISCO	Cisco Airone	t 1240AG Ser	ies Access Poi	nt 🛛 🖻 🖆
HOME Hostnam	ne AP			AP uptime is 6 hours, 58 minutes
EXPRESS SECURITY				
NETWORK MAP Expres	ss Security Set-Up			
ASSOCIATION SSID (	Configuration			
INTERFACES				Baagaan
SERVICES				Deacon
WIRELESS SERVICES				
SYSTEM SOFTWARE 2. VL4	AN			
		C Enable VLAN	ID: (1-4094) [	Native VLAN
3. Sec	curity			
	O No Securi	ty		
	Static WE	P Key		
		Kev 1 💙 🖣		128 bit 💙
	C EAD Auth	optiontion		
		entication	1	
		RADIUS Server:	Address)	(Hostname or IP
		RADIUS Server		
		Secret:		
	O WPA			
		RADIUS Server		(Hostname or IP
		NADIOS Servel.	Address)	
one			😜 Interr	net 🦙 + 🔍 100% -

5.- Observamos las características configuradas de nuestro WAP, como la dirección IP, la máscara de red a la que pertenece, el default-Gateway, y la dirección MAC asignada, así como también el status de las interfaces de FastEthernet y de los 2 Radios, se observa el status del software y del hardware y datos de transmisión.

- e https://17	2.21,1,252;ap_network-if.sbtml	🖌 🐼 Certificate Error	🗟 😽 🗙 🚼 Google	
avorites 🖉 Cisco IOS	5 Series AP - Network Interfaces		🖓 • 🕤 - 🗆 🖶	▼ Page ▼ Safety ▼ Tools ▼ (
CISCO	Cisco Airo	net 1240AG Serie	s Access Point	13 5
ME PRESS SET-UP	Hostname AP		AP	uptime is 6 hours, 59 minutes
PRESS SECURITY		2.0004.01		
ETWORK MAP	Network Interfaces: Sum	imary		
ETWORK INTERFACES	System Settings			
P Address	IP Address ( Static )	172.21.1.252		
astEthernet	IP Subnet Mask	255.255.255.0		
Radio0-802.11G	Default Catavari	170.01.1.050	-	
ladio1-802.11A	Default Gateway	172.21.1.203		
RVICES	MAC Address	0017.e095.3264		
RELESS SERVICES	Interface Status	FastEthernet	Radio0-802.11G	Radio1-802 11A
STEM SOFTWARE				
ENTLOG	Soliware Status	Enabled	Enabled	Enabled
	Hardware Status	Up 🕯	Up 🖹	Up 🖹
	Interface Resets	2	1	1
	Receive		i	
	Input Rate Timespan	5 minute	5 minute	5 minute
	Input Rate (bits/sec)	0	0	0
	Input Rate (packets/sec)	0	0	0
	Time Since Last Input	00:00:00	00:00:00	03:59:32
	Total Packets Input	82089	14464	40116
	Total Bytes Input	47596870	1666682	4961272

6.- Configuramos el Radio de transmisión inalámbrica, lo habilitamos, verificamos que su status sea habilitado y levantado, el rol del radio en la red es de Access Point y configuramos los tiempos y cantidades para el envío de datos.

Cisco IOS Series AP - Network In	terfaces - Windows Internet Exp	lorer			
C	ap_aetwork-If_802-11_L_shink	Certificate Error	🗟 🚧 🗙 🚼	Google	P -
🚖 Favorites 🏾 🏾 🏀 Cisco IOS Series AP -	Network Interfaces		🙆 • 📾	- 🖃 🖶 - Page -	Safety + Tools + 🔞 + 🂙
CISCO	Cisco Aironet 124	0AG Serie	es Access	Point	12 🗧 🦳
HOME	RADIO0-802.11G STATUS		SETTINGS	CARRIER BUSY TES	T
EXPRESS SET-UP EXPRESS SECURITY Hostna	me AP			AP uptime is	s 6 hours, 59 minutes
ASSOCIATION + NETWORK INTERFACES	ork Interfaces: Radio0-802.11G S	ettings			
IP Address Enab	le Radio:	Enable	O Dis	sable	
Radio0-802.11G Curre	ent Status (Software/Hardware):	Enabled	Up 🏫		
Radio1-802.11A     Role       SECURITY     +       SERVICES     +       WIRELESS SERVICES     +       SYSTEM SOFTWARE     +       EVENT LOG     +	in Radio Network:	Access Point     Access Point     Access Point     Access Point     Access Point     Repeater     Non-Root Bridge     Non-Root Bridge     Non-Root Brid     Workgroup Bri     Universal Work     (HHHH, HHHH, HHH     Scanner	(Fallback to Radi (Fallback to Repe ith Wireless Clien Ige with Wireless idge kgroup Bridge C IHH)	o Shutdown) eater) tts Clients lient MAC:	
Data	Rates:	BestRange	Best Throug	hput Default	
	1.0Mb/sec	Require	O Ena	able C	) Disable
Done	2 0Mb/sec	Require	∩ Enz	able 🤇	) Disable 🛛 🗡

7.- Abrimos el administrador global de SSID donde aparece la lista SSID, su nombre en la red para difusión, en este caso es Visitantes, si pertenece a alguna VLAN, si tiene un respaldo, y la interface de radio por la cual da el servicio inalámbrico,, en este caso usas los 2 radios 0-802 y 1-802, así como la forma de autentificarse los clientes para el uso del WAP.



8.- Vemos la versión del IOS de Cisco que está corriendo en el WAP, sus especificaciones técnicas tales como el numero de modelo, el numero de ensamblaje, la firma del software, la versión del sistema de software y el tiempo desde que el sistema está levantado, también vemos el nombre de nuestro WAP, en este caso es AP.



9.- Ahora procedemos a abrir las conexiones de red en nuestro equipo, después en redes inalámbricas, si observamos la lista, vemos que aparece la red llamada Visitantes, que es la que está difundiendo el WAP en nuestra LAN, es una red con seguridad habilitada y debemos de poseer algún tipo de autenticación válida para conectarnos a ella, la cual después nos permitirá estar en red con los demás equipos conectados al Switch, el WAP le da funcionalidades inalámbricas a nuestra red local.



### INTRODUCCIÓN A VPN.

Una VPN es una Red Privada Virtual que usa una red pública (usualmente Internet) para conectar sitios remotos o usuarios entre sí. En lugar de usar una conexión dedicada del mundo real, como una conexión privada que se renta a un ISP, una Red Privada Virtual utiliza conexiones "virtuales" enrutadas a través de Internet de la red privada de la compañía hasta el sitio remoto o el empleado.

¿Qué conforma una VPN?

Existen 2 tipos comunes de VPNs:

- Acceso Remoto: También conocida como "Virtual Private Dial-up Network (VPDN), es una conexión de tipo usuario-a-LAN, usada por una compañía que tiene empleados que necesitan conectarse a la red privada de varios sitios remotos. Típicamente, una corporación que desea instalar una VPN grande de acceso remoto, provee de alguna forma de una cuenta dial-up de Internet a sus usuarios usando un Proveedor de Servicios de Internet (ISP). Los Tele conmutadores pueden entonces marcar un número 1-800 para alcanzar el Internet y usar su software de cliente VPN para accesar a la red corporativa. Un buen ejemplo de una compañía que necesita una VPN de Acceso-Remoto seria una enorme firma con cientos de agentes de ventas en el campo. VPNs de Acceso Remoto permiten conexiones seguras, encriptadas entre una compañía privada y usuarios remotos a través de un proveedor de servicios alterno.
- Sitio a Sitio: A través del uso de equipos dedicados y encriptación a grande escala, una compañía puede conectar múltiples sitios fijos sobre una red pública como Internet. Cada sitio necesita solo una conexión local a la misma red pública, así se ahorrara dinero en líneas privadas de ISP. VPNs sitio a sitio pueden ser categorizadas en intranets o extranet. Una VPN sitio a sitio, construida entre oficinas de la misma compañía se dice que es una VPN intranet, mientras que una VPN construida para conectar la compañía a su socio o cliente es referida como una VPN extranet.

Una VPN bien diseñada puede beneficiar enormemente a una compañía. Por ejemplo, puede:

- Extender la Conectividad Geográfica
- Reducir los costos operacionales comparándolos con WANs tradicionales
- Reducir los tiempos de transito y los costos de viaje para usuarios remotos.
- Improvisar Productividad
- Simplificar la topología de la red
- Proveer oportunidades de desarrollo global
- Proveer soporte de tele conmutadores

Las siguientes características son necesitadas en una VPN bien diseñada:

- Seguridad
- Confiabilidad
- Escalabilidad
- Administración de la red

- Administración de la política

### Tecnologías de VPN

Una VPN bien diseñada usa diferentes métodos en orden para mantener la conexión y los datos seguros.

Confidencialidad de datos: Este es quizá el servicio más importante dado por cualquier implementación de una VPN. Debido a que los datos privados viajan a través de una red pública, la confidencialidad de datos es vital y puede ser obtenida encriptando los datos. Este es el proceso de tomar todos los datos que una computadora está enviando a otra y codificarlos en una forma que solo la otra computadora podrá decodificar.

La mayoría de las VPNs usan uno de los siguientes protocolos para dar encriptación:

- IPsec: El protocolo de seguridad de Internet (Internet Protocol Security Protocol) da características de seguridad aumentada como algoritmos de encriptación fuerte y autentificación más comprensiva. IPsec tiene dos modos de encriptación: túnel y transporte. Modo de túnel encripta el encabezado y la carga de cada paquete mientras el modo de transporte solo encripta la carga. Solo sistemas que son compatibles con IPsec pueden tomar ventaja de este protocolo. También, todos los aparatos deben usar una llave común o certificado y deben tener políticas de seguridad similares habilitadas.
- L2TP/IPsec Llamado comúnmente L2TP sobre IPsec, este provee la seguridad del protocolo IPsec sobre el túnel de Layer 2 Tunneling Protocol (L2TP). Inicialmente fue usado para VPNs de acceso remoto con sistemas operativos Windows 2000, ya que Windows 2000 contiene un cliente nativo de IPsec y L2TP.

Integridad de Datos: Así como es importante que los datos sean encriptados sobre una red pública, es también así de importante verificar que los datos no hayan sido cambiados durante su transporte. Por ejemplo, IPsec tiene un mecanismo para asegurar que la porción de datos encriptados del paquete, o todo el encabezado y la porción de datos del paquete, no hayan sido alterados. Si alguna alteración es detectada, el paquete es descartado.

Autentificación del origen de los datos: Es extremadamente importante verificar la identidad de la fuente de donde provienen los datos. Esto es necesario para protegerse contra un número de ataques que dependen de la suplantación de la identidad del receptor.

Túnel de los datos/ Confidencialidad del flujo de tráfico: "Tunneling" es el proceso de encapsular un paquete entero dentro de otro paquete y enviarlo sobre la red. Es útil en casos donde es deseable esconder la identidad del aparato que origina el tráfico. Por ejemplo, un aparato que usa IPsec encapsula tráfico que pertenece a un número de hosts detrás de él, y le agrega su propio encabezado arriba de los paquetes existentes. Al encriptar el paquete original y el encabezado, el aparato de "tunneling" efectivamente esconde la fuente actual del paquete. Solo el receptor permitido puede determinar la fuente verdadera, después de descartar el encabezado adicional y desencriptar el encabezado original. Todos los protocolos de encriptación mencionados anteriormente también usan "tunneling" como un medio para transferir los datos encriptados a través de la red pública. Es importante saber que el "tunneling" por sí solo no le da seguridad a los datos.

El paquete original solo es encapsulado dentro de otro protocolo y aun puede ser visible con un aparato de captura de paquetes si no es encriptado.

Tunneling requiere tres protocolos:

- Protocolo Pasajero: Los datos originales que son guardados
- Protocolo de Encapsulamiento: El protocolo que es usado para envolver los datos originales.
- Protocolo de Transporte: El protocolo que es usado por la red sobre la cual la información está viajando.

El paquete original (protocolo pasajero) es encapsulado dentro del protocolo de encapsulamiento, el cual después es puesto dentro del encabezado del protocolo de transporte (usualmente IP) para la transmisión sobre la red pública. Cabe destacar que el protocolo de encapsulamiento frecuentemente también lleva la encriptación de los datos.

Para VPNs de sitio a sitio, el protocolo de encapsulamiento es usualmente IPsec o GRE (Generic Routing Encapsulation). GRE incluye información sobre qué tipo de paquete se esta encapsulando y información sobre la conexión entre el cliente y el servidor.

Para VPNs de acceso remoto tunneling normalmente toma lugar usando un protocolo punto a punto (PPP), el cual es parte de la suite de protocolos TCP/IP, PPP es el transportador para otros protocolos IP cuando se están comunicando sobre la red entre la computadora servidor y un sistema remoto.

AAA: Es usado AAA (autenticación, autorización y anotación) para un acceso más seguro en una VPN de acceso remoto. Sin la identificación de usuario, cualquiera que se siente con una laptop/PC con software pre configurado de cliente VPN puede establecer una conexión segura hacia la red remota. Sin embargo, con autentificación de usuario, un nombre de usuario valido y un password deben ser ingresados antes de que la conexión sea completada. Nombres de usuarios y Passwords pueden ser almacenados en el equipo terminal de la VPN, o en un servidor AAA externo, el cual puede proveer de autentificación a otros servicios, como Windows NT, Novell, etc.

Cuando una petición para establecer un túnel llega de un cliente dial-up, el aparato de la VPN solicita un nombre de usuario y un password. Esto puede ser validado localmente, o enviado al servidor AAA externo, el cual verifica:

- Quien soy (autenticación)
- Que estoy permitido realizar (autorización)
- Que estoy haciendo(anotación)

## IMPLEMENTACIÓN DE UNA VPN.

### VPN en GNS3

Una red privada virtual (VPN) es una manera segura de conectarse a una red de área local (LAN) en un lugar remoto usando Internet o cualquier red pública no segura para transportar los paquetes de datos de la red de manera privada usando encriptación

La encriptación es el proceso de transformar información usando un algoritmo (cifrador) para hacerlo no legible a cualquiera excepto a aquellos que tienen una llave. El resultado del proceso es información encriptada.

L a VPN usa autenticación para denegar el acceso a usuarios no autorizados, y la encriptación para prevenir a usuarios no autorizados que puedan leer los paquetes de red privados. La VPN puede ser usada para enviar cualquier tipo de tráfico de red de manera segura, incluyendo voz, video o datos.

VPN son frecuentemente usadas por usuarios remotos o compañías con oficinas remotas para compartir datos privados y recursos de red.

Técnicamente, el protocolo de la VPN encapsula transferencias de datos de red usando un método seguro de criptografía entre dos o más aparatos de red los cuales se encuentran en redes diferentes, para mantener los datos privados mientras pasan por los routers de Internet o una Wide Área Network (WAN).

Algunos protocolos de seguridad de la VPN son:

- IPsec: Internet Protocol Security, desarrollado originalmente para IPv6, es usado ampliamente con IPv4.
- Transport Layer Security: TLS puede hacer un túnel para todo el trafico de una red de trabajo, o abrir una conexión segura individual.
- Datagram Transport Layer Security, es usado en la próxima generación de los productos VPN de Cisco.
- Microsoft Point-to-Point Encryption, compatible con varias versiones del sistema operativo de Windows, también Microsoft introdujo Secure Socket Tunneling Protocol (SSTP), el cual hace un túnel con el protocolo Point-to-Point a través de un canal seguro.
- SSH VPN: SSH ofrece un túnel de VPN para asegurar conexiones remotas a una red o a enlaces multi redes.

## DIAGRAMA DE LA INGENIERÍA DE LA VPN



Figura 1: Diagrama de una topología entre 2 sitios sobre Internet.

En el diagrama anterior se describe aproximadamente la topología de la simulación de una red del mundo real en GNS3.

El ISP (Internet Service Provider) se encarga de dar la IP Publica a cada sitio (SitioA y SitioB), el router tiene esa dirección IP en su interfaz serial externa, la cual se conecta a Internet, y a un router del ISP, del otro lado de la topología, se encuentra el SitioB, el cual también tiene una dirección pública en su router externo, asignada por el ISP, la interfaz externa del router se conecta a la salida a Internet y a un router del ISP, no necesariamente es el mismo router del ISP al cual se conecta el SitioA, pueden haber varios routers del ISP entre cada uno de ellos.

En cada sitio, hay una red privada LAN, la cual necesita conectarse a la otra red privada del otro sitio, esta se conecta a la interfaz interna del router que se conecta al exterior, por medio de una interfaz de conexión Fast Ethernet, usuarios dentro de esta LAN en el SitioA necesitan conectarse a otros usuarios dentro de la LAN en el SitioB, por medio de la VPN.

Para permitir el acceso a la VPN solo a usuarios autorizados, dentro del router se crea una lista de acceso, con el segmento de red autorizado para conectarse por medio de la VPN a otro sitio por Internet, solo los usuarios que estén dentro del rango de direcciones IP autorizadas podrán conectarse por el túnel seguro, si un equipo con una dirección diferente a la permitida, no podrá usar el túnel para la transferencia de datos seguros, esta medida se aplica con el fin de controlar los usuarios y el trafico que se transmite a través de la VPN, por ejemplo evitar congestionar el túnel con datos cuya prioridad no sea la seguridad sobre Internet, o que usuarios hagan uso del túnel para enviar datos cuya prioridad sea mínima, así como restringir el acceso a los datos enviados o recibidos por medio del túnel de la VPN.

### TRANSFERENCIA DE DATOS DE MANERA NO SEGURA SOBRE INTERNET



Figura 2: Ejemplo de conexión de un sitio a otro por Internet.

En la imagen se da una vista aproximada de que ruta se le da a un paquete de red a través de Internet, los paquetes de red viajan por muchos routers antes de llegar a su destino, por lo tanto es necesario el túnel de la VPN para encriptar los datos y asegurar una manera segura para que viajen a través de la red.

Cuando los datos son enviados de nuestra computadora, siempre está abierta a ataques. Se puede activar un firewall, el cual ayuda a proteger los datos moviéndose dentro nuestra red, evitando que sean corrompidos o interceptados por entidades fuera de la red, pero una vez que los datos se mueven fuera de la red – cuando enviamos datos a alguien via e-mail o nos comunicamos con un individuo sobre Internet- el firewall no protege mas los datos.

En este punto, los datos se exponen a hackers usando una variedad de métodos para robar no solo los datos transmitidos, sino también información de la red, y archivos de seguridad. Algunos de los métodos más comunes son:

1.- Falsificación de la dirección MAC:

Los paquetes transmitidos por una red, ya sea la red local o Internet, son precedidos por un encabezado de paquete. Estos encabezados de paquetes contienen información sobre el destino y

el origen del paquete. Un hacker puede usar esta información para falsificar una dirección MAC permitida en la red. Con esta dirección MAC el hacker puede interceptar información destinada para otro usuario.

2.- Captura por "sniffers" de datos:

Es un método usado por los hackers para obtener datos de la red mientras viajan a través de redes no seguras, como Internet. Herramientas para este tipo de actividad, como analizadores de protocolos, y herramientas de diagnostico de red, son frecuentemente instaladas en sistemas operativos y permiten ver el contenido de los datos en texto plano.

3.- Ataques de "hombre en medio".

Una vez que el hacker ha falsificado y revisado suficiente información, el ahora puede realizar un ataque de "hombre en el medio". Este ataque es realizado cuando los datos están siendo transmitidos de una red a otra, usando esta información para darle otra ruta a los datos y que el hacker aparezca como el destinatario original. De esta manera los datos aparentemente llegan a su destinatario intencionado.

Estos son solo algunos métodos, y día a día los hackers desarrollan nuevos métodos. Mientras sea fue de la seguridad de nuestro firewall, los datos están expuestos constantemente a ataques mientras viaja por Internet.

Los datos que viajan por internet frecuentemente pasaran por muchos routers y servidores alrededor del mundo antes de llegar a su destino final. Es un largo camino para datos inseguros, y es donde la VPN sirve su propósito para su transferencia segura de un sitio a otro.

## CONFIGURACIÓN DE LA VPN EN AMBOS SITIOS.

Es necesario configurar en cada equipo los parámetros necesarios para que se pueda crear el túnel de la VPN, de manera que ambos estén comunicados para que formen los "Endpoints" de la VPN, esto es, que sean los 2 extremos del túnel que se formara para la transferencia segura de los paquetes de red.

Cabe destacar que ciertos parámetros dentro de los routers de ambos sitios deben ser idénticos para que se pueda formar de forma correcta el túnel de la VPN, esto es, que si un parámetro no es igual al parámetro en el otro lado, como la llave compartida, no se formara el túnel para la encriptación de los paquetes de red, estos parámetros son de vital importancia, y aseguran que ambos sitios tengan acceso a la VPN.

La configuración en cada router se ajusta a las direcciones IP de los sitios, tanto a la dirección IP pública asignada por el ISP, como a la dirección IP privada de la LAN por la cual se comunicaran los usuarios en cada sitio.

## **CONFIGURACIÓN DEL ROUTER EN EL SITIO A**

Los parámetros más destacados a configurar en el router son los siguientes:

```
hostname SiteA
boot-start-marker
boot-end-marker
!
enable password 123
!
no aaa new-model
memory-size iomem 5
!
!
j cef
```

i-- Definimos un nombre de host para el Router en el Sitio A, así como un password para su configuración.

crypto isakmp policy 1 hash md5 encryption des authentication pre-share

```
crypto isakmp key secretkey address 11.11.11.1
!
!
```

Definimos una política de Internet Security Association Key Management Protocol, el número después de la política indica la prioridad dentro de nuestra configuración de la VPN, siendo un numero del 1 al 100, y el 1 es la prioridad más alta.

Usamos el algoritmo md5 para el hash, y para la encriptación usamos el algoritmo des, estos algoritmos nos ayudan a encriptar la información y a enviarla a través del túnel de nuestra VPN, para cifrar el contenido de los paquetes de red.

La autenticación se usara por medio de una llave pre compartida, es decir, ambos sitios deberán usar la misma llave para que puedan conectarse por la VPN; esta llave puede ser cualquier carácter alfanumérico.

La llave compartida es un parámetro que debe ser igual en ambos routers, y esta se configura hacia una dirección IP específica sobre la cual se creara el túnel de la VPN.

En este caso estamos definiendo él parámetro de la llave con el nombre de secretkey.

El receptor remoto con el cual se compartirá la llave tiene la dirección IP pública de 11.11.11.1, que corresponde al Sitio B.

crypto ipsec transform-set cm-transformset-1 ah-md5-hmac esp-des esp-md5-hmac crypto map cm-cryptomap local-address Serial 0/0 !

En esta parte definimos el "transform-set" que usaremos para la configuración de la VPN "Un transform-set" es una combinación aceptable de protocolos de seguridad y algoritmos que se utilizaran para la seguridad de IPsec.

Se especifican 3 conjuntos de transformaciones, de hasta 3 protocolos cada una, en nuestro caso los 3 conjuntos son:

ah-md5-hmac esp-des esp-md5-hmac

Estos son combinaciones aceptables de protocolos de seguridad, algoritmos y otras configuraciones a aplicarse a un tráfico protegido.

Los "transform-set" deben ser definidos usando este comando para poder ser incluido después en una entrada de crypto-map.

En nuestro caso, definimos el nombre de nuestro set de transformaciones como "cm-transformset-1".

Después, especificamos y nombramos la interfaz a ser usada por nuestro crypto-map, para el tráfico seguro de red por la VPN.

Nuestro crypto-map se llama cm-cryptomap, este nombre identifica a cada set cuando se crea el crypto-map.

Usamos como identificador de interfaz a la interfaz Serial 0/0, sobre la cual se aplicaran las politicas del crypto-map, cabe destacar que esta es nuestra interfaz del Sitio A conectada a Internet.

! crypto map cm-cryptomap 1 ipsec-isakmp match address 100 set peer 11.11.11.1

set transform-set cm-transformset-1 set security-association lifetime seconds 3600 set security-association lifetime kilobytes 4608000 !

En esta parte definimos que crypto-map se usa, la lista de acceso a la VPN, la dirección IP del receptor y el "transform-set" asociado.

Cuando usamos nuestro crypto-map "cm-cryptomap", las palabras ipsec-isakmp le dicen al router que este crypto-map es un Ipsec crypto-map, es decir un túnel con políticas y características del Protocolo de IP Seguro.

Se declara un emisor con la dirección IP de 11.11.11.1, que es la dirección que corresponde a la interfaz externa del Sitio B sobre el cual queremos crearla VPN, cabe destacar que aunque tenemos solo un receptor en este crypto-map, se pueden especificar múltiples emisores dentro de un crypto-map dado.

El comando "match-address" significa que se usara la lista de acceso 100 en orden para determinar que trafico es relevante para enviar sobre el túnel al otro sitio.

El segmento de red de esa lista de acceso identifica a los equipos permitidos para enviar tráfico de red a través de la VPN, restringiendo a equipos cuya IP no esté dentro del rango de la permitida en la lista de acceso.

Con el comando set transform-set, asociados nuestro set definido con el nombre de cmtransformset-1 a nuestro crypto-map, esto es, todas las políticas, algoritmos y parámetros configurados en el set, se aplican al crypto-map, siendo 1 el de más prioridad, en caso de tener varios sets.

Definimos la asociación de seguridad de tráfico de nuestra VPN, con el comando:

set security-association: cuando especificamos el parámetro con segundos, indica el numero de segundos que tiene una asociación de seguridad activa antes de expirar.

Cuando especificamos el parámetro en kilobytes, indicamos el volumen de trafico (en Kbps) que puede pasar entre 2 emisores de Ipsec usando una asociación de seguridad antes de que esa expire, en nuestro caso son 4608000 kilobytes.

Este comando solo esta disponible para entradas de crypto-map de ipsec-isakmp solamente.

Las asociaciones de seguridad usan llaves secretas compartidas. Estas llaves y sus correspondientes asociaciones de seguridad expiran al mismo tiempo.

Las asociaciones de seguridad funcionan de la siguiente manera:

Cuando el router recibe una petición de negociación del emisor, usara el valor mas pequeño del tiempo de vida ya sea propuesto por el emisor, o el tiempo de vida configurado localmente, como el tiempo de vida de la nueva asociación de seguridad.

La asociación de seguridad (y sus correspondientes llaves) expiraran de acuerdo a que ocurra primero, ya sea que los segundos para su uso expiren o después de que la cantidad de tráfico en kilobytes sea mayor al límite propuesto.

Una nueva asociación de seguridad es negociada, antes de que ambos parámetros de tiempo y cantidad lleguen a su límite, para que este lista cuando la asociación actual expire. La nueva

asociación de seguridad es negociada ya sea 30 segundos antes de que el tiempo de vida en segundos expire, o cuando el volumen de tráfico por el túnel este a 256 kilobytes de alcanzar su valor máximo permitido en su tiempo de vida.

```
interface Serial0/0
description connected to Internet
ip address 10.10.10.1 255.255.255.252
no shutdown
serial restart-delay 0
no fair-queue
crypto map cm-cryptomap
interface Serial0/1
no ip address
shutdown
serial restart-delay 0
interface Serial0/2
no ip address
shutdown
serial restart-delay 0
interface Serial0/3
no ip address
shutdown
serial restart-delay 0
interface FastEthernet 1/0
description connected to EthernetLAN
ip address 192.168.1.1 255.255.255.0
no shutdown
duplex auto
speed auto
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
```

!

l

!

l

ļ

ļ

```
93
```

Configuramos las interfaces del router del SitioA, la interfaz SerialO/O se conecta a Internet, esta interfaz contiene la dirección IP pública asignada por el ISP, y se especifica como parámetro dentro de la creación de la VPN.

En esta interfaz aplicamos el crypto-map definido anteriormente en nuestro router, este cryptomap contiene los parámetros, los protocolos de encapsulamiento y encriptamiento y las lista de acceso permitidas para conectarse a la VPN.

La interfaz Fast Ethernet se conecta a la LAN local, en las cuales se encuentran los usuarios permitidos para usar la VPN; estos se restringen por una lista de acceso, en la cual, si queremos que por esta interfaz accedan a la VPN; entonces debe estar la dirección IP dentro del rango de IP permitidas en la lista, para que usuarios accedan a la VPN.

```
!
ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 Serial0/0
!
!
```

Activamos el servidor HTTP dentro de nuestro router.

La ruta será un ruteo estático, la default es 0.0.0.0, mas agregamos la interfaz por la cual saldrá todo el tráfico de red, para encontrar la ruta optima a su destino, por medio de los routers del ISP.

En este caso la interfaz por la cual sale el tráfico de red, y busca la ruta optima, es la interfaz Serial 0/0.

```
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
control-plane
!
I
I
line con 0
exec-timeout 0 0
password 123
login
line aux 0
line vty 04
password 123
login
!
I
end
```

Se crea la lista de acceso la cual define el rango de direcciones IP con acceso a la VPN, tanto las que se conectaran del lado local del túnel, como las que estarán del otro lado del túnel de forma remota, en este caso las direcciones de las redes permitidas son:

- 192.168.1.0
- 192.168.2.0

Para el Sitio B tenemos prácticamente las mismas configuraciones, excepto por las direcciones IP, en este caso tenemos la dirección publica de 11.11.11.1 y nuestra red privada a conectarse por la VPN es la dirección 192.168.2. los demás parámetros como se menciono anteriormente, deben ser idénticos en algunas configuraciones:

```
hostname SiteB
!
boot-start-marker
boot-end-marker
!
enable password 123
!
no aaa new-model
memory-size iomem 5
!
!
j
ip cef
```

En este caso el nombre de nuestro router en el Sitio B es SiteB.

```
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key secretkey address 10.10.10.1
ļ
I
crypto ipsec transform-set cm-transformset-1 ah-md5-hmac esp-des esp-md5-hmac
crypto map cm-cryptomap 1 ipsec-isakmp
set peer 10.10.10.1
set transform-set cm-transformset-1
match address 100
L
L
La dirección IP de nuestro emisor remoto corresponde a la 10.10.10.1
Comparte la misma llave compartida "secretkey".
Se configura el mismo "transform-set" que en el Sitio A.
```

```
interface Serial0/0
description connected to Internet
```

ip address 11.11.11.1 255.255.255.252 no shutdown serial restart-delay 0 no fair-queue crypto map cm-cryptomap ļ interface Serial0/1 no ip address shutdown serial restart-delay 0 I interface Serial0/2 no ip address shutdown serial restart-delay 0 ļ interface Serial0/3 no ip address shutdown serial restart-delay 0 l interface FastEthernet1/0 description connected to EthernetLAN\_1 ip address 192.168.2.1 255.255.255.0 no shutdown duplex auto speed auto I interface FastEthernet2/0 no ip address shutdown duplex auto speed auto I interface Serial3/0 no ip address shutdown serial restart-delay 0 ļ interface Serial3/1 no ip address shutdown serial restart-delay 0 ļ interface Serial3/2 no ip address shutdown serial restart-delay 0

```
!
interface Serial3/3
no ip address
shutdown
serial restart-delay 0
!
```

La interfaz serial por la cual se conecta el router a Internet tiene la dirección IP de 11.11.11.1 en esta interfaz se aplica el crypto-map definido anteriormente, de manera similar que se aplico en el Sitio A.

La interfaz Fast Ethernet se conecta a la LAN local, en las cuales se encuentran los usuarios permitidos para usar la VPN; estos se restringen por una lista de acceso, en la cual, si queremos que por esta interfaz accedan a la VPN; entonces debe estar la dirección IP dentro del rango de IP permitidas en la lista.

```
ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 Serial0/0
!
!
```

Se activa el servidor HTTP, y se define la ruta estática por default, así como la salida por la interfaz Serial0/0 a Internet.

```
access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

!

!

control-plane

!

line con 0

exec-timeout 0 0

password 123

login

line aux 0

line vty 0 4

password 123

login

end
```

Se define la lista de acceso de las direcciones IP local y remota las cuales se permitirá el acceso por la VPN, estas direcciones IP restringe a usuarios cuyo equipo no tenga una dirección IP en este rango el uso de la VPN, permitiendo solo a usuarios permitidos el uso de la VPN para así reducir trafico no deseado y permitir protocolos de seguridad y encriptamiento sobre paquetes con prioridad en ambos lados del túnel.



Figura 3: Diagrama de la simulación de la VPN en GNS3

Pruebas para verificar la correcta creación de la VPN.

En primer lugar debemos verificar que exista una conexión activa entre la red privada del Sitio A y la red privada del Sitio B, para verificar que se creó de manera exitosa un enlace sobre Internet para unir 2 sitios para su intercambio de paquetes de red.

Ping es una utilidad diagnostica en redes de computadoras que comprueba el estado de la conexión del host local con uno o varios equipos remotos por medio del envió de paquetes ICMP de solicitud y de respuesta. Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada.

Ejecutando un ping de solicitud, el host local envía un mensaje ICMP, incrustado en un paquete IP. El mensaje ICMP de solicitud incluye, además del tipo de mensaje y el código del mismo, un número identificador y una secuencia de numero de 32 bits, que deberán coincidir con el mensaje ICMP de respuesta; además de un espacio opcional para datos.

En nuestro primer caso se envía un ping de nuestro Sitio A al Sitio B, el ping tiene como interfaz origen la dirección IP 192.168.1.1, como interfaz destino la dirección IP 192.168.2.1

Desde el router del sitio A, mandamos un ping a la dirección privada del sitio B, de la siguiente manera:

Dynamips(2): SiteA, Console port \*Mar 1 00:26:53.527: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up SiteA# SiteA#ping Protocol [ip]: Target IP address: 192.168.2.1 Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y Source address or interface: 192.168.1.1 Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]: Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds: Packet sent with a source address of 192.168.1.1 .... Success rate is 100 percent (5/5), round-trip min/avg/max = 24/90/188 ms Ξ SiteA# SiteA#

Figura 4 : Ping del Sitio A al Sitio B

Tenemos como parámetros:

Target IP address: 192.168.2.1 Dirección IP a la cual queremos llegar.

Source address or interface: 192.168.1.1 Dirección IP de nuestra red origen.

Confirmamos que lleguen los paquetes de regreso, lo cual es confirmado con el siguiente parámetro:

Packet sent with a source address of 192.168.1.1 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 24/90/188 ms

Tenemos un suceso del 100% por lo tanto hay una conexión establecida entre el Sitio A y el Sitio B.

Ahora debemos verificar la conexión establecida entre el Sito B y el Sitio A, el sitio B tiene como dirección IP de su interfaz privada la dirección 192.168.2.1, que es la dirección origen, y tiene como objetivo la dirección IP 192.168.1.1

Desde el router del sitio B, mandamos un ping a la dirección privada del sitio A, de la siguiente manera:

B Dynamips(1): SiteB, Console port	3
SiteB#ping	
Protocol [ip]:	
Target IP address: 192.168.1.1	
Repeat count [5]:	
Datagram size [100]:	
Timeout in seconds [2]:	
Extended commands [n]: y	
Source address or interface: 192.168.2.1	
Type of service [0]:	
Set DF bit in IP header? [no]:	
Validate reply data? [no]:	
Data pattern [0xABCD]:	
Loose, Strict, Record, Timestamp, Verbose[none]:	
Sweep range of sizes [n]:	
Type escape sequence to abort.	
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:	
Packet sent with a source address of 192.168.2.1	
11111	
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/108/212 ms	
SiteB#	
SiteB#	
SiteB#	≡
SiteB#	
SiteB#	-

Figura 5: Ping del Sitio B al Sitio A.

Tenemos como parámetros:

Target IP address: 192.168.1.1 Dirección IP a la cual queremos llegar.

Source address or interface: 192.168.2.1 Dirección IP de nuestra red origen.

Confirmamos que lleguen los paquetes de regreso, lo cual es confirmado con el siguiente parámetro:

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds: Packet sent with a source address of 192.168.2.1 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 32/108/212 ms SiteB#

Tenemos un suceso del 100% por lo tanto hay una conexión establecida entre el Sitio B y el Sitio A.

Ahora verificamos la creación del túnel de la VPN entre los 2 sitios.

Debemos checar que las 2 fases de la VPN estén levantadas, de acuerdo con los comandos:

- show crypto isakmp sa
- show crypto ipsec sa

Para el Sitio A:

🛃 Dynamips(2	): SiteA, Console port			
SiteA#show	crypto is			<u>^</u>
SiteA#show	crypto isakmp sa			
dst.	src	state	conn-id slot status	
10.10.10.1	11.11.11.1	QM_IDLE	1 0 ACTIVE	
		_		
SiteA#				
SiteA#show	cry			
SiteA#show	crypto ips			
SiteA#show	crypto ipsec sa			
SiteA#show	crypto ipsec sa			
interface:	Serial0/0			
Crypto	map tag: cm-cryptom	ap, local ad	dr 10.10.10.1	
protect	ed vrf: (none)			
local	ident (addr/mask/pro	t/port): (19)	2.168.1.0/255.255.255.0/0/	0)
remote	ident (addr/mask/pro	t/port): (19)	2.168.2.0/255.255.255.0/0/	0) =
current	peer 11.11.11.1 por	t 500		· =
PERMI	 T, flags={origin is ;	acl,}		
#pkts (	encaps: 14, #pkts en	crypt: 14, #	pkts digest: 14	
#pkts (	decaps: 14, #pkts de	crypt: 14, #	pkts verify: 14	
#pkts	compressed: 0, #pkts	decompresse	d: 0	
#pkts	not compressed: 0, #	pkts compr.	failed: 0	τ.

Figura 6: Comandos para verificar status túnel Sitio A

Para el Sitio B:

```
х
Dynamips(1): SiteB, Console port
SiteB#sho crypt
                                                                                ٠
SiteB#sho crypto isa
SiteB#sho crypto isakmp sa
dst
                               state
                                             conn-id slot status
              src
10.10.10.1
               11.11.11.1
                              QM_IDLE
                                                   1 0 ACTIVE
SiteB#sh crypto ipsec sa
SiteB#sh crypto ipsec sa
interface: Serial0/0
   Crypto map tag: cm-cryptomap, local addr 11.11.11.1
  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.2.0/255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.1.0/255.255.0/0/0)
  current peer 10.10.10.1 port 500
    PERMIT, flags={origin is acl,}
   #pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
   #pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0
```



En la primera fase, el STATUS esta en activo en ambos Sitios, lo que indica que la primera fase de la VPN

Para la segunda fase observamos:

#pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
#pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14

Los paquetes recibidos se decapsulan y se decriptan por el túnel, así mismo, los paquetes enviados también se encapsulan y se encriptan por el túnel IPsec de la VPN, lo cual quiere decir que nuestro túnel está levantado, y con ellos está funcionando la VPN del Sitio A y Sitio B.

Ahora podemos enviar datos de manera seguro sobre Internet de un sitio a otro.

### INTRODUCCIÓN A CALIDAD DE SERVICIO.

Muchas aplicaciones de datos son basadas en el protocolo TCP. Si un segmento TCP es descartado, la fuente lo retransmite después de que pasa un periodo de tiempo y no se recibe un mensaje de que ese segmento fue recibido. Por lo tanto, aplicaciones basadas en TCP tienen alguna tolerancia a caída de paquetes. La tolerancia de aplicaciones de video y voz comparada con la tolerancia de datos es mínima. Como resultado. La red debe tener mecanismos activados para que en cualquier momento de congestión en la red, los paquetes encapsulando video y voz reciban tratamiento prioritizado y no son descartados.

Fallas en la red afectan todas las aplicaciones y las deshabilitan. Sin embargo, redes bien diseñadas tienen redundancia construida dentro de sí, para que cuando una falla ocurra, la red puede reenrutar paquetes a través de caminos alternos (redundancia) hasta que los componentes que fallaron sean reparados. El tiempo total que toma notar la falla, construir caminos alternos, y empezar a re-enrutar los paquetes debe ser lo suficientemente corto para que las aplicaciones de voz y video no sufran y no molesten a los usuarios. De nuevo, las aplicaciones de datos usualmente no esperan la red recuperada de una manera tan rápida como lo esperan las aplicaciones de voz y video.

Basado en la información precedente, se puede concluir que 4 conflictos mayores desafían a las redes de las empresas:

- Ancho de Banda disponible: Muchas aplicaciones simultáneas de datos, voz y video compiten por el ancho de banda de los enlaces dentro de las redes de la empresa.
- End-to-end delay: Muchas acciones y factores contribuyen al tiempo total que le toma a los paquetes de datos o voz alcanzar su destino. Por ejemplo compresión, empaquetamiento, serializacion, propagación, procesamiento (switching) y descompresión, todos contribuyen para el retraso total en la transmisión de VOIP.
- Variación de retraso (jiter)- Basado en la cantidad de tráfico concurrente y la actividad, mas la condición de la red, paquetes del mismo flujo pueden experimentar una diferente cantidad de retraso mientras viajan por la red.
- Perdida de paquetes: Si el volumen de tráfico agota la capacidad de una interface, link o aparato, paquetes pueden ser descartados. Ráfagas repentinas o fallas son usualmente responsables por esta situación.

Estos son los problemas mayores a los que se puede enfrentar una empresa dentro de su red de trabajo, las soluciones para cada uno de ellos son diferentes, dependiendo el objetivo perseguido y el problema a resolver.

#### DISPONIBILIDAD DE ANCHO DE BANDA.

Paquetes usualmente fluyen a través del mejor camino de la fuente al destino. El máximo ancho de banda de ese paquete es equivalente al ancho de banda del link con el ancho de banda más pequeño.



Figura 1: Rutas para envió de paquetes dentro de una red.

La figura 1 muestra que R1-R2-R3-R4 es el mejor camino entre el cliente y el servidor. En este camino, el ancho de banda máximo es de 10 Mbps porque es el ancho de banda del link con el menor ancho de banda en ese camino. El promedio de ancho de banda disponible es el ancho de banda máximo dividido entre el número de flujos.

La ausencia de suficiente ancho de banda causa retraso, perdida de paquetes y bajo rendimiento de aplicaciones. Los usuarios de aplicaciones en tiempo real (voz y video) detectan esto de inmediato. Se puede solucionar este problema de disponibilidad de ancho de banda de maneras numerosas:

- Aumento (mejora) de enlace de ancho de banda: Efectivo pero costoso.
- Clasificación del tráfico y desplegar técnicas de mecanismos de encolamiento: Envió de paquetes importantes primero.
- Uso de técnicas de compresión: Compresión de carga de capa 2, compresión de encabezado TCP, y de CRTP son algunos ejemplos.

El aumento del enlace de ancho de banda es sin duda benéfico, pero no siempre puede ser realizado rápidamente y tiene implicaciones costosas. Aquellos que solo incrementan ancho de banda cuando es necesarios notan que su solución no es muy efectiva en tiempos de ráfagas pesadas de red, sin embargo en ciertos escenarios, aumentar el ancho de banda puede ser la primera acción necesaria.

La clasificación del tráfico, combinado con administración de la congestión, es un enfoque efectivo para dar adecuadas medidas de ancho de banda para aplicaciones empresariales.

Compresión de enlace, compresión de encabezado TCP son diferentes tipos de técnicas de compresión que pueden reducir el ancho de banda consumido en ciertos enlaces, y así incrementar su eficacia. Cisco IOS soporta los algoritmos de capa 2 Stacker y Predictor de compresión, los cuales comprimen la carga del paquete. El uso de compresión por hardware siempre es preferido sobre la compresión por software, como la compresión usa muchos recursos de CPU, e impone otros retrasos es usualmente recomendada solamente en enlaces lentos.

#### End-to-end delay

El end-to end delay o retraso punto a punto es la suma de los diferentes tipos de retrasos que afectan los paquetes de un camino de red o de una aplicación. Cuatro de los más importantes tipos de retraso que conforman el retraso punto a punto son los siguientes:

- Retraso de procesamiento
- Retraso de encolamiento
- Retraso de serializacion
- Retraso de propagación

Retraso de procesamiento es el tiempo que le toma a un aparato, como un router o un Switch de Capa 3 realizar todas las tareas necesarias para mover un paquete de su interface de entrada a su interface de salida. El tipo de CPU, la utilización del CPU, el modo de Switch, la arquitectura del router, y las características configuradas en el aparato afectan el retraso de procesamiento.

Retraso de encolamiento es la cantidad de tiempo que un paquete gasta en la cola de salida de una interface de un router. El número de paquetes esperando en la cola, las reglas de la cola, y el ancho de banda de la interface afectan el retraso de encolamiento.

Retraso de serializacion es el tiempo que toma enviar todos los bits de una trama al medio físico para su transmisión a través de la capa física. El tiempo que le toma a los bits de esa trama cruzar el enlace físico es llamado el retraso de propagación.

#### Perdida de paquetes:

Perdida de paquetes ocurre cuando un aparato de red como un router no tiene más espacio en buffer en una interface (cola de salida) para recibir los nuevos paquetes y termina descartándolos. Un router puede tirar algunos paquetes para hacer espacio a los que tengan prioridad alta. Algunas veces un reset de una interface causa que los paquetes sean descartados.

TCP reenvía los paquetes descartados, mientras, reduce el tamaño de la ventana de envió y retrasa los envíos en tiempos de congestión y alto volumen de tráfico de red. Si un paquete perteneciente a una transferencia de archivo basada en UDP es descartado, todo el archivo puede que tenga que volver a ser reenviado. Esto crea más tráfico en la red, y puede congestionar la red y alterar al usuario.

Durante una llamada de VoIP, perdida de paquetes puede resultar en interrupción de audio. Una videoconferencia tendrá imágenes distorsionadas o borrosas y su audio estará fuera de sincronización con el video si los paquetes se caen u ocurre retraso prolongado. Cuando el

volumen de tráfico de red y la congestión son muy pesados, las aplicaciones experimentan caída de paquetes y retrasos prolongados. Solo con la configuración adecuada de QoS se pueden evitar estos problemas, o de menos los limitan a paquetes de baja prioridad.

En un router Cisco, en tiempos de congestión y caída de paquetes, podemos insertar el comando:

### #show interface

Y observar que en esa o en todas las interfaces, ciertos contadores se han incrementado más que lo usual, los contadores son los siguientes:

- Output drop: Este contador muestra el número de paquetes caídos, ya que la cola en salida en la interface estaba llena al momento de la llegada de los paquetes. También se le conoce como tail drop.
- Input queue drop: Si el CPU es sobre utilizado y no puede procesar paquetes entrantes, la cola de entrada de una interface puede llenarse, y el numero de paquetes caídos en este escenario serán reportados como caídas de entrada.
- Ignore: Es el número de tramas ignoradas debido a ausencia de espacio en el buffer.
- Overrun: El CPU debe reservar suficiente espacio de buffer para que paquetes entrantes puedan ser guardados y procesados por turnos. Si el CPU se empieza a ocupar mucho, puede no guardar el suficiente espacio de buffer de manera rápida y termina descartando paquetes. El número de paquetes descartados por esta razón se le llama overruns.
- Frame error: Tramas con error de chequeo de redundancia cíclica (CRC), tramas más pequeñas que el estándar y tramas gigantes son usualmente descartadas, y su total es reportado como errores de trama.

Se pueden usar muchos métodos para combatir la pérdida de paquetes, todos derivados de QoS, de estos métodos, algunos protegen la pérdida de paquetes en todas las aplicaciones, mientras que otros protegen clases específicas de la perdida de paquetes. Los siguientes son ejemplos de enfoques para evitar o disminuir perdida de paquetes:

- Aumento del enlace de ancho de banda: Alto ancho de banda resulta en envíos más rápidos de paquetes.
- Aumento del espacio de buffer: Ingenieros en redes deben examinar las configuraciones del buffer en las interfaces de los aparatos de red como los routers para ver si sus tamaños y configuraciones son apropiados. Cuando se tiene el problema de caída de paquetes, es conveniente considerar un aumento en el espacio de buffer de la interface.
- Reservación de ancho de banda: Herramientas que permiten a los ingenieros en redes reservar ciertas cantidades de ancho de banda para una clase específica de tráfico de red. Mientras sea reservado el suficiente ancho de banda para una clase de tráfico red, paquetes de red que pertenezcan a esa clase no serán victimas de caída de paquetes.

La mayoría de las compañías que conectan sitios remotos a través de una conexión WAN transfieren aplicaciones basadas tanto en TCP como en UDP entre esos sitios, en estos casos es conveniente hacer ingeniería de red para evitar perdida de paquetes por congestión en la red, así como prioridades, ya que pueden haber paquetes que sean importantes y deban llegar todos a su destino de forma correcta y ordenada.

### **CISCO QOS**

La definición más reciente que utiliza Cisco en su material educativo para QoS es:

"QoS es la habilidad de la red de proveer un servicio mejor o especial a un conjunto de usuarios o aplicaciones o ambos a expensas de otros usuarios o aplicaciones o ambos."

#### Implementando QoS

Son necesarios 3 pasos principales:

- 1.- Identificar el tipo de tráfico y sus requerimientos.
- 2.- Clasificar tráfico basado en los requerimientos identificados.
- 3.-Definir políticas para cada clase de tráfico.

Aunque muchas aplicaciones y protocolos en común existen entre las redes empresariales, dentro de cada red, los volúmenes y porcentajes de esos tráficos varía. Además, cada empresa puede tener sus propios tipos de aplicaciones únicas. Por lo tanto el primer paso para implementar QoS es una empresa es estudiar y descubrir los tipos de tráfico y definir los requerimientos de cada tipo de trafico identificado.

Si dos, tres o más tipos de tráfico tienen importancia y requerimientos idénticos, no es necesario definir una clase de tráfico para cada uno de ellos.

La clasificación de tráfico, el cual es el segundo paso en implementar QoS, definirá una nueva clase de tráfico. Las aplicaciones que se agrupen en diferentes clases tienen diferentes requerimientos, y la red debe de cumplirlos con diferentes tipos de servicios. La definición de cómo cada clase de trafico es atendida se llama la política de red (network policy).

Definir e implementar la política de QoS para cada clase es el paso 3 de implementar QoS. Los 3 pasos son explicados a detalle a continuación.

Paso 1: Identificar tipos de tráfico y sus requerimientos

Identificar tipos de tráfico y sus requerimientos, es el primer paso para implementar QoS, se compone de los siguientes pasos:

- Realizar una auditoría de red: Es recomendado que se realice la auditoria durante la hora ocupada o en periodo de congestión, pero también es importante que se realice en otras horas. Ciertas aplicaciones se ejecutan durante horas lentas de negocio a propósito. El método más simple para esto es observar el CPU y las utilizaciones del enlace y conducir la auditoria durante los periodos generales de carga pesada de red.
- Realizar una auditoría de negocio y determinar la importancia de cada aplicación: El modelo de negocio y logros dicta los requerimientos del negocio. De ahí podemos derivar la definición de clases de tráfico y los requerimientos para cada clase. Este paso considera cuando el retraso o la descartacion de paquetes es aceptable. El ingeniero en redes debe determinar la importancia relativa de diferentes aplicaciones.

 Definir los niveles de servicios apropiados para cada clase de tráfico: Para cada clase de tráfico, un nivel de servicio específico puede definir disponibilidad de recursos o reservaciones. Ancho de banda mínimo garantizado, garantizado retraso de punto a punto y preferencia de caída comparativa son unas de las características que se pueden definir para cada nivel de servicio.

Paso 2: Clasificar el trafico basado en los requerimientos identificados.

La definición es las clases de trafico no necesitan ser generales, deben incluir los tipos de trafico que son observados durante la auditoria de la red. Se pueden clasificar decenas o cientos de variaciones de tráfico en muy pocas clases. El tipo de tráfico o aplicaciones dentro de la misma clase debe estar en línea con objetivos de negocios.

El tráfico de voz tiene requerimientos específicos, y es casi siempre en su propia clase. Muchos casos de estudio han mostrado los meritos de usar una o todos de las siguientes clases de tráfico dentro de una red empresarial:

- Clase de voz (VoIP): trafico de voz tiene requerimientos específicos de ancho de banda, y su retraso y caídas deben ser eliminados o al menos minimizados. Por lo tanto, esta clase es la clase con la prioridad más alta, pero tiene ancho de banda limitado.
- Clase de tráfico de Misión Critica: Aplicaciones de negocios críticos son puestas en una de 2 clases. Se deben identificar los requerimientos de de banda ancha para ellas.
- Clase de señalamiento de tráfico: Señalamiento de tráfico, configuración de llamadas por voz y video son frecuentemente puestos en una clase separada, se deben identificar los requisitos de cada uno de ellos.
- Clases de tráfico de aplicaciones transaccionales: Estas aplicaciones, si existen, incluyen aplicaciones interactivas, de bases de datos y servicios similares que necesitan atención especial. Se deben también identificar los requerimientos de ancho de banda para las aplicaciones. Aplicaciones de ERP (Enterprise Resource Planning) como Peoplesoft y SAP son ejemplos de estos tipos de aplicaciones.
- Clase de tráfico de Best-Effort: Todo el tipo de tráfico no definido son considerados de Best-Effort (Mejor Esfuerzo) y reciben lo que queda de ancho de banda de una interface.
- Clase de tráfico Scavenger: Esta clase de aplicaciones será asignada en una clase con ancho de banda limitado. Esta clase Scavenger (Carroñera) es considerada inferior a la clase de trafico Best-Effort. Aplicaciones de transferencia cliente a cliente, de juegos y de redes sociales son puestas en esta clase.

Paso 3: Definir políticas para cada clase de tráfico:

Después de que las clases de tráfico han sido formadas, basado en la auditoria de la red y los objetivos de negocios, el paso final de implementar QoS en una empresa es dar una definición amplia de red para el nivel de servicio de QoS que debe ser asignado a cada clase de tráfico. Esto es llamado "Definiendo una política de QoS", entre sus objetivos tiene completar las siguientes tareas:
- Configurar el límite máximo de ancho de banda
- Configurar el límite mínimo ancho de banda de una clase.
- Asignar un nivel de prioridad relativa a una clase.
- Aplicar la administración de congestión, evasión de congestión, y muchas otras tecnologías de QoS a una clase.

Métodos de Implementación de QoS.

Legado de Línea de comandos (CLI)

Configuración por CLI requirió al usuario iniciar sesión en el router vía consola usando una terminal, o vía una línea virtual usando una aplicación de Telnet. Debido a que este método no era modular, CLI no permitía a los usuarios la separación completa de la clasificación de tráfico de la definición de la política de red, y de como la política es aplicada.

La configuración por CLI inicia identificando, clasificando y prioritizando el trafico. Después, se selecciona una de las herramientas disponibles y apropiadas de QoS como la compresión de enlace o un mecanismo de encolamiento disponible como la prioritizacion adecuada de encolamiento.

Finalmente se aplican de pocas a muchas líneas de código aplicando los mecanismos de QoS seleccionados para las interfaces.

CLI de QoS Modular (MQC)

Un modelo mejorado de CLI, permite la utilización de las herramientas más recientes de QoS y las características disponibles en los IOS modernos de Cisco. Con MQC, la clasificación de tráfico y la definición de políticas son realizadas de manera separada.

La política de tráfico es definida después de las clases de tráfico. Diferentes políticas pueden referenciar a las mismas clases de tráfico, tomando ventaja de código reutilizable. Cuando una o más políticas son definidas, se pueden aplicar a muchas interfaces, promoviendo el rehúso de código.

MQC separa la clasificación de tráfico de la definición de políticas, y es compatible con la mayoría de las plataformas del IOS de Cisco. Con MQC, las políticas definidas son aplicadas a interfaces en lugar de que muchos comandos tecleados lo sean.

Implementar QOS con MQC involucra 3 grandes pasos:

Paso 1: Definir clases de trafico usando el comando **class-map**. Este paso divide el tráfico identificado de la red en un número de clases nombradas.

Paso 2: Definir las políticas de QoS para las clases de trafico definidas usando el comando **policy-map**. Este paso involucra ligar las características de QoS a las clases de tráfico. Define el trato que se le dará a las clases de tráfico definidas.

Paso 3: Aplicar las políticas definidas en la dirección entrante o saliente de cada interface o subinterface deseada, usando el comando **service-policy**. Este paso define cuando las políticas definidas son aplicadas.

Cada class-map, la cual tiene un nombre único, está compuesta de uno o más enunciados de igualdad. Uno o todos los enunciados de igualdad deben ser iguales, dependiendo de las condiciones que contengan con los comandos **match-any** o **match-all**. Si no está configurado en el class map especificado, match-all es aplicado por default.

A continuación tenemos 2 ejemplos de mapas de clase. El primer mapa de clase se llama VOIP. Este mapa de clase especifica la lista de acceso 100 concordante con tráfico está clasificada como VoIP. El segundo mapa de clase se llama Aplicaciones-Negocios. Especifica que la lista de acceso 101, concordante con ese tráfico, está clasificada como Aplicaciones-Negocios.

class-map VOIP match access-group 100 i class-map Aplicaciones-Negocios match access-group 101 i

Nótese que ambas de las clases tienen solo un enunciado de "match", cuando solo un enunciado "match" existe, "match-all" y "match-any" contienen el mismo resultado. Sin embargo si existe más de un solo enunciado de igualdad, usar match-any o match-all hacen una gran diferencia, match-any significa que solo uno de los enunciados necesita ser cumplido, y match all significa que todos los enunciados deben ser cumplidos para unir el paquete a la clase.

El opuesto de **match** es la condición **no-match**.

Se crean políticas de tráfico asociando los requisitos de QoS requeridos a las clases de tráfico definidas por clases de mapas: se usa el comando **policy-map** para hacerlo. Un mapa de política asocia políticas de QoS para hasta 256 clases de tráfico (cada una definida por una clase).

El siguiente ejemplo exhibe un mapa de política llamado Politica-Empresa. Este mapa de política especifica que el trafico clasificado como VOIP es asignado a una cola de prioridad que tiene un ancho de banda garantizado de 256 Kbps Politica-Empresa también enuncia que el trafico clasificado como Politica-Empresa es asignado a un WFQ con un ancho de banda garantizado de 256 Kbps De acuerdo a este mapa de política, el trafico restante, clasificado como **class-default** será asignado a una cola que obtenga el resto del ancho de banda disponible.

WFQ= Weighted Fair Queuing (Encolamiento de Peso Justo) es una de las tecnologías premier de Cisco. Es un algoritmo de encolamiento basado en flujo que realiza dos cosas simultáneamente: organiza tráfico interactivo en el frente de la cola para reducir el tiempo de respuesta, y comparte de manera justa el ancho de banda restante entre altos flujos de ancho de banda.

Se utiliza dentro de los mapas de política, para que se le asigne tráfico enunciado dentro de un mapa, para organización y repartición de ancho de banda entre las clases de tráfico.

Ejemplo de mapa de políticas:

policy-map Politica-Empresa class VOIP priority 256 i class Aplicaciones-Negocios bandwith 256 class class-default fair-queue i

Si configuramos un mapa de políticas que incluya un enunciado de clase seguido del nombre de un mapa de clase que no exista, mientras el enunciado contenga una condición, un mapa de clase es creado e insertado en la configuración con ese nombre automáticamente. Si, dentro de un mapa de política, no hacemos referencia a **class-default**, cualquier tráfico que las clases definidas no concuerden con él seguirá siendo tratado como trafico de class-default.

Un mapa de política es aplicado en una interface en la dirección entrante o saliente usando el comando **service-policy** (y la dirección especificada usando las palabras clave **input** u **output**). Se puede aplicar un mapa de política definido y configurado a más de una interface. Reutilizando mapas de clase y mapas de política es altamente recomendado porque promueve la estandarización y reduce las oportunidades de errores. El siguiente ejemplo muestra que el mapa de política Politica-Empresarial es aplicado a la interface serial 1/0 de un router en la dirección saliente.

Ejemplo de política de servicio:

interface serial 1/0 service-policy output Politica-Empresarial i

Los siguientes comandos nos permiten desplegar y verificar clases de QoS y políticas que configuramos usando MQC:

show class-map- Este comando despliega todos los mapas de clase configurados.

show policy-map- Este comando despliega todos los mapas de política configurados.

**show policy-map interface** "interfaz"- Este comando despliega el mapa de políticas que es aplicado a una interface en particular usando el comando **service-policy**. Este comando también despliega estadísticas de QoS de la interfaz.

Estos comandos ayudan a levantar los 3 pasos de QoS del servicio MQC, y con ayuda de los comandos para desplegar información sobre los mapas de clase y política, así como de cada interface con MQC habilitado, se puede determinar si existe algún problema con MQC habilitado en la interfaz, así como para problemas de soporte de ingeniería en redes.

#### AutoQoS

AutoQoS es un valor agregado en las características del IOS de Cisco. Después de que es habilitado en un aparato, AutoQoS automáticamente genera los comandos de la configuración de QoS para el aparato. Después fue introducido AutoQoS Discovery, el cual analiza tráfico de red activo mientras se deje correr y genera clases de tráfico basadas en el tráfico que ha sido procesado. Después se habilita la característica de AutoQoS. AutoQoS usa las clases de tráfico formadas por AutoQoS Discovery para generar la política de QoS en la red, y aplicarla. Basado en el tipo de interfaz, AutoQoS también puede agregar características como fragmentación y multienlace a la configuración de la interface.

La ventaja principal de AutoQoS es que simplifica la tarea de la configuración de QoS. Administradores de red que no tengan un conocimiento muy profundo de los comandos de QoS y características pueden usar AutoQoS para implementar estas características de manera precisa y consistente. AutoQoS participa en todos los aspectos principales del despliegue de QoS:

- Clasificación: AutoQoS para empresas, a través de AutoQoS Discovery, automáticamente descubre aplicaciones y protocolos usando NBAR( Network Based Application Recognition)
- Generador de política: Da el trato apropiado de tráfico gracias a las políticas de QoS que auto genera. Listas de acceso, mapas de clase y mapas de política, los cuales normalmente tienen que ser tecleados manualmente, son generados automáticamente por AutoQoS.
- Configuración: Es habilitada por la entrada de un solo comando, auto qos, en la interface.
   En cuestión de segundos, comandos apropiados para clasificar, marcar y prioritizar se aplican a los paquetes, y se siguen agregando a la configuración apropiadamente.
- Monitoreo y Reportes: Genera reportes del sistema, trampas SNMP y reportes en general.
- Consistencia: Los comandos generados en diferentes routers, usando AutoQoS, son consistentes e interoperables.

Usar AutoQoS requiere de algunos prerrequisitos. Antes de que podamos habilitar AutoQoS en una interface, se debe asegurar que las siguientes tareas han sido completadas:

- Cisco Express Forwarding está habilitado. CFE es el prerrequisito para NBAR.
- NBAR está habilitado. AutoQoS usa NBAR para el descubrimiento de tráfico y su clasificación.
- Configurar correctamente el ancho de banda en la interfaz.

Después de que estas tareas han sido completadas, AutoQoS puede ser configurado y habilitado en la interfaz deseada. El siguiente ejemplo muestra una interfaz serial que ha sido configurada con ancho de banda, dirección IP, CEF y AutoQoS

Ejemplo de configuración de AutoQoS en una interface:

ip cef interface serial 1/0 bandwith 256 ip address 10.1.1.1 255.255.255.252

#### auto qos voip

Nótese que el comando **auto qos voip** se aplica a la interfaz serial 1/0. Cuando tecleamos el comando auto qos en una interfaz, el router construye los mapas de clase (basados en el resultado del descubrimiento de la red) y después crea y aplica un mapa de política en la interface.

#### SCRIPT DE QOS

En primer lugar se procedió a hacer un análisis de los puertos utilizados por el Xbox 360, esto a fin de crear una lista de acceso que solo tuviera permitido los puertos utilizados por el Xbox 360, los puestos usados en el 360 para juego en línea son:

Puerto 88 (UDP) Puerto 3074 (UDP y TCP) Puerto 53 (UDP y TCP) Puerto 80 (TCP).

Esos puertos se agregaron a una lista de acceso creada con el fin de filtrar únicamente el tráfico de red recibidos por esos puertos, la lista de acceso creada es:

access-list 130 permit udp any any eq 88 access-list 130 permit udp any any eq 3074 access-list 130 permit tcp any any eq 3074 access-list 130 permit tcp any any eq 80

Para el tráfico de VOIP usamos la siguiente lista de acceso:

access-list 120 permit tcp any any eq 1720 access-list 120 permit tcp any any range 11000 11999 access-list 120 permit udp any any eq 1719 access-list 120 permit udp any any eq 1718 access-list 120 permit tcp any any eq 5060 access-list 120 permit udp any any eq 5060 access-list 120 permit tcp any any range 2000 2002 access-list 120 permit udp any any eq 2427 access-list 120 permit tcp any any eq 2428 access-list 120 permit udp any any range 16384 32767

Por medio de esta lista de acceso que filtra el trafico del Xbox 360 se aplicara la calidad de servicio a nivel de capa 2, es decir, QoS estará habilitado en el Switch "Core", siendo el núcleo este de toda nuestra red local.

Definición de los class-map y los policy-map.

Definiremos 4 mapas de clases de tráfico de red, estos se usan para clasificar el tráfico similar de red, a los cuales se les quiera aplicar un trato específico, en nuestro caso, de las 4 clases, 2 son para Voz y son 2 para datos (Xbox 360); de Voz, una clase es para clasificar el trafico entrante y

darle una prioridad y otra para su salida hacia fuera de la red loca, simétricamente lo mismo con la clase de datos del Xbox 360, una para aspectos de clasificación y la otra para su salida. Las clases definidas son:

class-map match-any XBOX-IN match access-group 130 class-map match-any VOIP-IN match access-group 120 class-map match-all VOIP-OUT match ip precedence 4 class-map match-all XBOX-OUT match ip precedence 5 !

La clase XBOX-IN se enlaza a la lista de acceso marcada con el número 130. Esta lista controla el tráfico de red que proviene de los puertos para el juego en línea del Xbox 360.

La clase VOIP-IN le da trato a los paquetes de red de protocolos usados para la telefonía de Voz sobre IP.

La clase VOIP-OUT le da salida a los paquetes que se marcaron con una prioridad de 4, para que reciban el trato específico a su número de prioridad, este trato incluye asignación de ancho de banda.

La clase XBOX-OUT le da salida a los paquetes marcados con una prioridad de 5, en nuestro caso 5 es la prioridad más alta de un paquete, e incluye asignación de ancho de banda mayor sobre los demás paquetes de la red.

Después de tener definidas nuestras clases, ahora debemos definir las políticas a aplicarse a esas clases, los policy-map definen el trato que se la dará a ciertas clases, por trato puede ser el porcentaje de ancho de banda asignado, la prioridad de precedencia IP asignada a esa clase y el tipo de paquete marcado.

policy-map QOS-OUT class XBOX-OUT bandwidth percent 65 class VOIP-OUT bandwidth percent 25 policy-map QOS-IN class XBOX-IN set ip precedence 5 class VOIP-IN set ip precedence 4

La política QOS\_OUT se aplica a la clase XBOX-OUT, esta política le asignará a los paquetes dentro de esa clase un porcentaje de ancho de banda de 65, garantizando el mínimo para que el juego en línea este estable, independientemente de las aplicaciones que también tomen del ancho de banda en la red local.

También aplicamos esta política a la clase de VOIP-OUT, en esta clase se maneja el trafico de voz, y se le asigna un ancho de banda del 25%, garantizando el mínimo para una llamada con calidad de voz aceptable.

La política QOS-IN contiene a la clase de XBOX-IN, en esta política se encargan de marcar los paquetes en su llegada al Switch, para posteriormente darles prioridad de numero 5, es decir marca los paquetes del Xbox 360 con el numero 5, la prioridad más alta, por lo tanto en nuestra estructura de calidad de servicio, el ancho de banda mayor siempre lo tendrá el Xbox 360, después utilizaremos este marcado al momento de que los paquetes reciban el ancho de banda definido en la política de salida.

También contiene a la clase de VOIP-IN, en esta política también se marcan los paquetes de voz para su asignación de ancho de banda, los paquetes son marcados con una prioridad de 4, por lo tanto la voz es el segundo servicio de red con más recursos en nuestra estructura de QoS.

Procedemos ahora a aplicar las políticas de calidad de servicio en los puertos del Switch Core que administra la red local, estos puertos son en total 48, en 47 de estos puertos se aplicara el mapa de QOS-IN, es decir se clasifica el trafico y se marcan los paquetes, de acuerdo a si son de voz, de Xbox 360 o de las demás aplicaciones de la red, es en este lugar cuando se marcan las prioridades sobre las cuales se dará porcentaje de ancho de banda en la interfaz de salida hacia el router, en esa interfaz, la número 48, se aplica la política QOS-OUT, se asigna el ancho de banda especificados en las políticas y se envían por el medio de transmisión, siendo los paquetes con el numero de precedencia de 5 con los de mayor prioridad.

Politica QOS-IN aplicada en una interfaz:

interface FastEthernet0/3 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN

En este puerto se conecta un equipo con IP Communicator, el cual pertenece a la VLAN de voz y la de datos, se configura en modo de acceso, es decir permite que otro equipo esté conectado en este puerto, pero es deshabilitado si se conecta otro Switch en ese puerto, se le asignara una dirección IP por DHCP, esta configurado por portfast para el spanning-tree, es decir para un que este habilitado antes que el arranque de un sistema operativo de un equipo conectado a él.

El comando service-policy input QOS-IN indica que en este puerto se está aplicando una política de servicio de QoS de nombre QOS-IN y es una política de entrada, es decir se aplica conforma van entrando los paquetes de red.

Ahora los comandos:

wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5

Usamos el comando wrr-queue bandwidth para asignar pesos a las colas de banda ancha en los puertos 10/100 Ethernet. En cada uno por default está asignado el valor de 25, un cuarto del total del ancho de banda por cada uno, 1 es "Cola seleccionada" y los demás, el 0 y 1 es el valor de CoS

En este caso usamos los parámetros 10, 20, 70 y 1, 1 determina el radio de la frecuencia en el cual el administrador procesa los paquetes.

El comando wrr-queue cos-map 1 0 1 asigna valores de clase de servicio para seleccionar una de las colas de egreso.

En el primer caso, el valor identificador es 1, el valor puede ser de 1 a 4.

Los segundos valores son los valores de clase de servicio que son mapeados para seleccionar un ejemplo, la tabla por default de los valores mapeados es:

Valor de CoS	Cola Seleccionada
0, 1	1
2, 3	2
4, 5	3
6, 7	4

# DESCRIPCIÓN DE LOS VIDEOS DEMOSTRATIVOS.

Video 1.- Topología de la red.

En nuestro primer video, demostramos la topología de la red que se utilizo para el desarrollo del proyecto terminal, en primer ligar mencionaremos brevemente los equipos utilizados para esta tarea:

- 2 Routers Cisco C1751
- 1 Switch Cisco 3550
- 1 Wireless Access Point
- 1 Modem Router 7200 de Telmex
- 3 Computadoras (2 Laptop y una de escritorio)
- 1 Router Virtual en GNS3 (instalado en una de las laptop)

En primera instancia, los 2 routers Cisco separan nuestras 2 redes (Sitio A y Sitio B), a cada una de estas redes le corresponde un segmento de dirección de ip, siendo en el Sitio A la 172.21.1.0/24 y en el Sitio B la 172.22.1.0/24, a través de los routers conectados entre sí por medio del cable serial se forma la VPN para enlazar los sitios y permitir que cada usuario en cada sitio, si tiene los suficientes privilegios, pueda usar la VPN para el envío de datos de forma segura sobre Internet o sobre una red mayor.

En cada sitio hay un equipo con privilegios suficientes para usar la VPN, así como en cada sitio existe voz sobre IP (VOIP) la cual viaja a través de la VPN, llega al otro sitio, y establece un canal de voz para realizar la llamada telefónica entre ambos usuarios en las 2 redes, los paquetes de VOIP se encapsulan, se encriptan y se envían a través de la VPN para evitar que sean descifrados o capturados en un ataque de red, estos paquetes son recibidos al otro lado de la red, son desencapsulados y son re dirigidos al usuario con quien se estableció previamente el canal de comunicación para VOIP.

En el Sitio A, se encuentra un Switch para administración de la LAN, todos los equipos se conectan a él, lo llamamos Switch "CORE" porque es el núcleo, y de ahí se redirige el trafico, ya sea al Access-Point el cual da servicios de Wireless, este previamente se configuró para que estuviera dentro de la red; en el Switch también se manejan listas de acceso para restringir usuarios o puertos y se tienen configuradas 2 VLANS:

Vlan100 Descripción: VLAN-Datos

Vlan200 Descripción: VLAN-Voz

Estas VLAN's permiten dividir lógicamente a la red del Sitio a para permitir que 2 acciones de realicen de forma óptima:

- Separar el trafico de Broadcast entre los equipos dentro de la red
- Dividir a los usuarios que utilicen la red para el juego en línea (Xbox 360) de los usuarios que utilicen la red para telefonía de IP (VOIP).

También se tiene configurado un servidor DHCP, que se encarga de asignar direcciones de un conjunto de direcciones IP a los equipos, en nuestro caso el único que no recibe dirección IP debido a que está configurado de manera estática es el Xbox 360, ya que por motivos de aspectos de NAT (Network Address Translation) es necesario que se habiliten unos puertos en el router para su conexión al servidor de Xbox Live.

En la red, existe una laptop con 2 interfaces físicas Ethernet de red. Esta computadora tiene instalado el GNS3, y dentro de él se encuentra un router virtual, en el cual se instalo Call Manager Express para administrar los servicios de telefonía en ambos lados de la VPN, se conecta el router CME, llamémoslo así al router virtual en GNS3, a nuestra red por medio de una interfaz Ethernet de la laptop, la otra sirve para instalar el IP Communicator en ella, y que también la maquina sirva como un usuario que decide hacer una llamada al otro lado de la VPN.

Call Manager Express asigna 2 extensiones a los 2 usuarios entre los cuales se desea establecer una llamada, las extensiones son:

- Sitio A extensión numero 007
- Sitio B extensión numero 008

Las extensiones son asignadas por medio de la identificación de la dirección MAC address en los equipos, CME asigna la extensión, y cuando un usuario desea establecer una llamada, recibe la petición CME, lo envía al Switch y lo redirecciona al usuario interesado en recibir la llamada, de ahí la petición regresa al CME; después al Switch, después se envía al router, se encapsulan y se envían los paquetes a través de la VPN, llega al otro sitio, se desencapsulan, se descifran y se envían al usuario con quien está establecida la llamada de VOIP.

La llamada se realiza del Sitio B, se marca la extensión 007, la petición pasara por los 2 routers, llegara al Switch y de ahí se redireccionará al CME, este revisa quien tiene asignada la extensión 007 por medio de las direcciones MAC, y reenvía el paquete al Switch, este lo envía a la interfaz de red con la dirección MAC asociada, y finalmente llega al usuario 007. Quien ve que la llamada es del otro lado de la VPN, y contesta, probando que la telefonía sobre IP está en buen funcionamiento.

La red local mostrada esta en el Sitio A, del otro lado de los 2 routers en el sitio B se tiene un equipo de computo, pero este puede ser otro sitio en otro lugar o otra red, etc.

Para fines del proyecto, la calidad de servicio se encuentra dentro de la LAN, es donde toma parte los aspectos más importantes del proyecto, puesto que es donde administramos el ancho de banda por medio de calidad de servicio, en este lado se encuentra de igual forma un Xbox 360 conectado al Switch por un puerto Ethernet, este Xbox 360 se conecta del Switch al router, y de ahí al modem ruteador de Telmex, el cual tiene asignado una dirección IP y un ancho de banda predeterminado por el ISP, que en este caso nuestro proveedor de servicios es Telmex, este modem solo tiene una conexión con el router de la LAN, ningún otro equipo, ya sea el WAP, otra computadora o inclusive el Xbox 360 están conectados directamente a él, todos se conectan al Switch Core, el cual les da el tratamiento necesario para aplicar la calidad de servicio, esta se aplica a nivel de capa 2, el Xbox 360 envía sus paquetes de red para conectarse a otros usuarios en Internet a través del Switch, después del router, y finalmente por el modem de Telmex. Video 2.- Aplicación y Verificación de la Calidad de Servicio en nuestra LAN.

En primer lugar se clasifico el tráfico de red en 3 grupos principales

1.- Grupo de Xbox 360
 2.- Grupo de VOIP
 3.-Clases de trafico "Scavenger"

Se realizó un marcado para darle prioridad a los paquetes de Xbox 360 y después para los paquetes de VOIP, este marcado permitió asignar ancho de banda preferencial de un 65 % para Xbox 360, y de un 25% para VOIP, lo demás se reparte entre las clases de tráfico que no fueron marcadas.

Los comandos que definieron el marcado para Xbox 360 y Voip son:

Set ip precedence 5: El de más alto rango, todos los paquetes de Xbox 360 saldrán con este marcado para que sean la prioridad en nuestra red local.

Set ip precedence 4: El siguiente en prioridad en nuestra LAN, utiliza un marcado de 4, quiere decir que no es más importante que el servicio de Xbox 360 para juego en línea.

Se procedió a establecer una sesión de juego en línea con el titulo Modern Warfare 2, y se verificó que se estableciera la sesión y empezáramos a jugar en línea para ver que tanto estaba de óptimo nuestro ancho de banda, los juegos en línea estuvieron con buena calidad, no se sufrió retraso o alguna pausa en el juego, la sesión se realizo con 18 jugadores de todo el mundo conectados, es decir, estábamos jugando en tiempo real con otros 17 jugadores, sin sufrir pausas o sin que se nos cayera la conexión debido a problemas de falta de ancho de banda o de conexión defectuosa.

En nuestra LAN se empezó a generar mucho tráfico de red para verificar que la calidad de servicio diferenciara paquetes con prioridad de los que no, se genera una llamada de VOIP del Sitio A al Sitio B, la cual paso por el túnel formado por la VPN entre los dos routers, lo cual también consumió ancho de banda ya que se envía la llamada de nuestra red local al otro lado de la VPN, en otros equipos de nuestra LAN se abrieron páginas de videos en internet, un ping constante, una descarga de archivo pesado, todo esto para saturar la red, cabe destacar que todos los equipos de nuestra LAN, incluyendo el Xbox 360 están conectados al Switch

Entramos al router principal vía telnet para verificar que los paquetes están siendo marcados y están siendo enviados a través de la interfaz externa del router hacia el modem de Telmex para su salida a Internet, después de un cierto periodo de tiempo, las aplicaciones que no tenían prioridad, al acabarse su ancho de banda, empiezan a actuar de manera fallida y la red local, así como las conexiones entre esos usuarios se empiezan a deteriorar, ya que se termina el ancho de banda disponible para que tales aplicaciones puedan conectarse a Internet.

El marcado de los paquetes de Xbox 360 se realiza en el Switch, de ahí se redirecciona al router que procederá a ver qué paquetes tienen prioridad unos sobre los otros, y también tiene la función de administrar bien el ancho de banda no asignado entre las aplicaciones que no sean de Xbox 3600 de VOIP.

Teclearemos un comando llamado show interfaces precedence el cual nos dice que numero de paquetes marcados en especifico se están usando, y si siguen enviándose, ya están marcados los paquetes pero debemos ver qué cantidades de un tráfico en especifico están siendo enviadas o recibidas en el medio de transmisión.

Select Telnet 172.21.1.254	- 🗆	×
Router-A# Router-A# Router-A#sh ver		<b>^</b>
Router-A#sh version Cisco IOS Software, C1700 Software (C1700-ADVENTERPRISEK9-M), Version 12.4(2 RELEASE SOFTWARE (fc2)	5c),	
Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986–2010 by Cisco Systems, Inc. Compiled Thu 11-Feb-10 22:24 by prod_rel_team		
ROM: System Bootstrap, Version 12.2(7r)XM2, RELEASE SOFTWARE (fc1)		
Router-A uptime is 17 hours, 22 minutes System returned to ROM by power-on System image file is "flash:c1700-adventerprisek9-mz.124-25c.bin"		
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you		
agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.		
A summary of U.S. laws governing Cisco cryptographic products may be found a http://www.cisco.com/wwl/export/crypto/tool/stqrg.html	t:	
If you require further assistance please contact us by sending email to export@cisco.com.		
Cisco 1751-V (MPC860P) processor (revision 0x400) with 118576K/12496K bytes	of m	
Processor board ID FOC08251KDF (2769955525), with hardware revision 0000 MPC860P processor: part number 5, mask 2 I Ethernet interface		
1 FastEthernet interface 2 Samial(supc/asupc) interfaces		
32K bytes of NURAM. 32768K bytes of processor board System flash (Read/Write)		
Configuration register is 0x2102		
Router-A#sh interfaces pre FastEthernet0/0 LAN-A Invut		
Precedence 0: 446457 packets, 45333426 bytes Precedence 4: 428058 packets, 66058112 bytes Precedence 5: 133579 packets, 19454051 bytes		
Router-A#		
Router-A# Router-A#		-

Se muestran en esta figura los 3 tipos de paquetes usados en nuestra red local, y para muestra de su funcionamiento vemos que si se realizo el marcado de los paquetes, ya que cada vez los contadores de los paquetes van aumentando conforme se envían datos en la LAN.

Precedence 0 corresponden a los paquetes de red procesados que corresponden a las aplicaciones de red que no son de voz o de Xbox 360, ejemplo: pings, páginas de video como Youtube, torrents, Messenger y Facebook.

Estos paquetes no reciben ancho de banda específico, toman el que está disponible después de que se asigno ancho de banda a los paquetes del Xbox 360 y a VOIP, por lo tanto no tienen ninguna prioridad en nuestro entorno.

Precedence 4 corresponden a los paquetes de voz que provienen del IP Communicator y del Call Manager Express, para establecer una llamada entre los 2 usuarios en ambos lados de la VPN, también genera trafico de red ya que pasa por el Switch, llega al router del Sitio A, viaja a través del cable serial al router del Sitio B, y después llega al usuario en la PC en ese lado de la VPN, de regreso pasa por el mismo camino, llega al Sitio A y después a la computadora con el otro IP Communicator, estos paquetes en el Switch reciben la calidad de servicio, se marcan con el valor de ip precedence de numero 4, y en su salida hacia el router se les asigna un 25% del ancho de banda disponible, lo que garantiza que ningún otro servicio tome de ese ancho de banda garantizado, esto permite un envió y recepción de paquetes de VOIP con QoS.

Precedence 5 corresponden a los paquetes provenientes del Xbox 360 para la conectividad con el servicio de Xbox Live, estos paquetes tienen la prioridad máxima en nuestra LAN, los paquetes viajan del puerto Ethernet del Xbox 360 a un puerto Ethernet de nuestro Switch que está asignado a la VLAN de datos, de ahí son marcados, por numero de puerto, con el valor de ip precedence de 5, este paquete se irá incrementando conforme la calidad de servicio está siendo aplicada, este paquete de valor 5 tiene un ancho de banda garantizado de 65% y ningún otro servicio puede tomar del 65% de ancho de banda del Xbox 360, es el servicio con la prioridad más alta en nuestra LAN, y siempre debe tener calidad optima; así mismo en el video se muestra que la sesión de juego siempre está en buena calidad, no se pausa ni se detiene, así como no se interrumpe la conexión durante el juego multijugador.

Se tiene un generador de trafico de red para intentar saturar el ancho de banda en nuestra red local, esto para tratar de afectar la sesión en línea del Xbox 360, pero como estos paquetes de trafico de red del generador no tienen prioridad, no reciben tratamiento especial, y son clasificados dentro de la clase con precedencia 0, la cual recibe un ancho de banda mínimo, así que no dañan o afectan el servicio multijugador en línea.

Finalmente en el video se muestra como mientras se están ejecutando el generador de tráfico, la llamada de VOIP entre los 2 usuarios, la descarga de videos en Youtube, el ping constante a Internet y la descarga de algunos torrents, el servicio de Xbox Live sigue constante y en calidad optima, ya que la calidad de servicio separa los diferentes tráficos y no permite que los paquetes no marcadas con precedencia 5 utilicen el ancho de banda de 65% reservado para el Xbox 360, la sesión de juego se muestra optima, y sin fallos de conexión, la calidad de servicio está siendo aplicada, y se demuestra con el video que a pesar de todo el tráfico que podamos tener en nuestra red, si un servicio tiene prioridad, en este caso el del Xbox Live, ninguna otra aplicación usara el ancho de banda mínimo garantizado para el servicio prioritizado, siendo esta una solución atractiva para darle prioridades a los diferentes servicios de red en una LAN.

El cambio de Host en el juego en línea se realiza de manera rápida, y se reanuda el servicio sin ningún contratiempo, este cambio se realizo debido a que se designa a un jugador como el nuevo anfitrión de juego, como se observa en el video esto sucede de manera rápida y no perdemos la conectividad con el juego ya que la calidad de servicio se sigue aplicando aun si se restablece la conexión debido a un cambio en los servidores de Xbox Live.

## SCRIPTS DE SWITCH, ROUTER A, ROUTER B, ROUTER GNS3 Y WAP.

## SH RUN DEL SWITCH CORE-A

Core-A# Core-A#sh ver Cisco Internetwork Operating System Software IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(22)EA10, RELEASE SOFTWARE (fc2) Copyright (c) 1986-2007 by cisco Systems, Inc. Compiled Tue 08-May-07 12:07 by myl Image text-base: 0x00003000, data-base: 0x006D3E20

ROM: Bootstrap program is C3550 boot loader

Core-A uptime is 17 hours, 48 minutes System returned to ROM by power-on System image file is "flash:/c3550-i9q3l2-mz.121-22.EA10.bin"

cisco WS-C3550-48 (PowerPC) processor (revision C0) with 65526K/8192K bytes of memory. Processor board ID CHK0622W1E5 Last reset from warm-reset Running Layer2/3 Switching Image

Ethernet-controller 1 has 12 Fast Ethernet/IEEE 802.3 interfaces

Ethernet-controller 2 has 12 Fast Ethernet/IEEE 802.3 interfaces

Ethernet-controller 3 has 12 Fast Ethernet/IEEE 802.3 interfaces

Ethernet-controller 4 has 12 Fast Ethernet/IEEE 802.3 interfaces

Ethernet-controller 5 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 6 has 1 Gigabit Ethernet/IEEE 802.3 interface

48 FastEthernet/IEEE 802.3 interface(s)2 Gigabit Ethernet/IEEE 802.3 interface(s)

The password-recovery mechanism is enabled. 384K bytes of flash-simulated non-volatile configuration memory. Base ethernet MAC Address: 00:09:E8:11:94:80 Motherboard assembly number: 73-5701-06 Power supply part number: 34-0967-01 Motherboard serial number: CAT06210A7D Power supply serial number: LIT062000QG Model revision number: C0 Motherboard revision number: B0 Model number: WS-C3550-48-SMI System serial number: CHK0622W1E5 Configuration register is 0x10F Core-A# Core-A# Core-A# Core-A# Core-A#sh cdp ne Core-A#sh cdp neighbors Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone Device ID Local Intrfce Holdtme Capability Platform Port ID 169 1751-V Router-A Fas 0/48 RS Fas 0/0 Router-CME Fas 0/1 151 R S I 3640 Fas 0/0 Fas 0/45 AIR-AP1242Fas 0 AP.Raven 166 ΤI Core-A# Core-A# Core-A# Core-A# Core-A# Core-A#sh run Core-A#sh running-config Building configuration... Current configuration : 17202 bytes version 12.1 no service pad service timestamps debug uptime service timestamps log uptime service password-encryption 1 hostname Core-A enable secret 5 \$1\$y0jA\$BktUlmiXzuVS9YGCqx0xh1 ١ username admin privilege 15 password 7 0822455D0A16 ip subnet-zero ip routing ip dhcp excluded-address 172.21.1.250 172.21.1.255 ip dhcp excluded-address 172.21.2.250 172.21.2.255 1 ip dhcp pool DHCP-Datos

```
network 172.21.1.0 255.255.255.0
  default-router 172.21.1.254
  dns-server 4.2.2.2 8.8.8.8
ip dhcp pool DHCP-Voz
 network 172.21.2.0 255.255.255.0
  dns-server 4.2.2.2 8.8.8.8
  default-router 172.21.2.253
!
no ip domain-lookup
mls qos
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
١
class-map match-any XBOX-IN
 match access-group 130
class-map match-any VOIP-IN
 match access-group 120
class-map match-all VOIP-OUT
 match ip precedence 4
class-map match-all XBOX-OUT
 match ip precedence 5
١
!
policy-map QOS-OUT
 class XBOX-OUT
 bandwidth percent 65
 class VOIP-OUT
 bandwidth percent 25
policy-map QOS-IN
 class XBOX-IN
  set ip precedence 5
 class VOIP-IN
  set ip precedence 4
!
١
interface FastEthernet0/1
switchport access vlan 200
switchport mode access
wrr-queue bandwidth 10 20 70 1
wrr-queue cos-map 1 0 1
wrr-queue cos-map 2 2 3
wrr-queue cos-map 3 4 6 7
```

wrr-queue cos-map 4 5 priority-queue out service-policy input QOS-IN interface FastEthernet0/2 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN ١ interface FastEthernet0/3 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/4 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN 1 interface FastEthernet0/5 switchport access vlan 100 switchport mode access switchport voice vlan 200

wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/6 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/7 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN 1 interface FastEthernet0/8 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN

!

interface FastEthernet0/9 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/10 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/11 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN ١ interface FastEthernet0/12 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3

wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN 1 interface FastEthernet0/13 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/14 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN ١ interface FastEthernet0/15 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/16 switchport access vlan 100

switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/17 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/18 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/19 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out

spanning-tree portfast service-policy input QOS-IN ١ interface FastEthernet0/20 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/21 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN ۱ interface FastEthernet0/22 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/23 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1

wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/24 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/25 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/26 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN ١

interface FastEthernet0/27 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/28 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN ۱ interface FastEthernet0/29 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN 1 interface FastEthernet0/30 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7

wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/31 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/32 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/33 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN ١ interface FastEthernet0/34 switchport access vlan 100 switchport mode access

switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/35 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN ١ interface FastEthernet0/36 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/37 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast

service-policy input QOS-IN interface FastEthernet0/38 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/39 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/40 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/41 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1

wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/42 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN ١ interface FastEthernet0/43 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN interface FastEthernet0/44 switchport access vlan 100 switchport mode access switchport voice vlan 200 wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out spanning-tree portfast service-policy input QOS-IN ١ interface FastEthernet0/45

description AP switchport access vlan 100 switchport mode access wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out service-policy input QOS-IN interface FastEthernet0/46 description XBOX360 switchport access vlan 100 switchport mode access wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out service-policy input QOS-IN ١ interface FastEthernet0/47 description CCM-Express switchport access vlan 200 switchport mode access wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out service-policy input QOS-IN 1 interface FastEthernet0/48 description Salida-LAN-A switchport access vlan 100 switchport mode access wrr-queue bandwidth 10 20 70 1 wrr-queue cos-map 1 0 1 wrr-queue cos-map 2 2 3 wrr-queue cos-map 3 4 6 7 wrr-queue cos-map 4 5 priority-queue out max-reserved-bandwidth 100 service-policy output QOS-OUT

```
!
interface GigabitEthernet0/1
switchport mode dynamic desirable
interface GigabitEthernet0/2
switchport mode dynamic desirable
interface Vlan1
no ip address
shutdown
١
interface Vlan100
description VLAN-Datos
ip address 172.21.1.253 255.255.255.0
interface Vlan200
description VLAN-Voz
ip address 172.21.2.253 255.255.255.0
١
ip classless
ip route 0.0.0.0 0.0.0.0 172.21.1.254
ip http server
access-list 120 permit tcp any any eq 1720
access-list 120 permit tcp any any range 11000 11999
access-list 120 permit udp any any eq 1719
access-list 120 permit udp any any eq 1718
access-list 120 permit tcp any any eq 5060
access-list 120 permit udp any any eq 5060
access-list 120 permit tcp any any range 2000 2002
access-list 120 permit udp any any eq 2427
access-list 120 permit tcp any any eq 2428
access-list 120 permit udp any any range 16384 32767
access-list 130 permit udp any any eq 88
access-list 130 permit udp any any eq 3074
access-list 130 permit tcp any any eq 3074
access-list 130 permit udp any any eq domain
access-list 130 permit tcp any any eq domain
access-list 130 permit tcp any any eq www
1
line con 0
line vty 04
login local
line vty 5 15
login
!
end
```

### SH RUN DEL ROUTER-A

Router-A# Router-A#sh ve Router-A#sh version Cisco IOS Software, C1700 Software (C1700-ADVENTERPRISEK9-M), Version 12.4(25c), RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2010 by Cisco Systems, Inc. Compiled Thu 11-Feb-10 22:24 by prod\_rel\_team

ROM: System Bootstrap, Version 12.2(7r)XM2, RELEASE SOFTWARE (fc1)

Router-A uptime is 17 hours, 36 minutes System returned to ROM by power-on System image file is "flash:c1700-adventerprisek9-mz.124-25c.bin"

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco 1751-V (MPC860P) processor (revision 0x400) with 118576K/12496K bytes of memory. Processor board ID FOC08251KDF (2769955525), with hardware revision 0000 MPC860P processor: part number 5, mask 2 1 Ethernet interface 1 FastEthernet interface 2 Serial(sync/async) interfaces 32K bytes of NVRAM. 32768K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

Router-A# Router-A#sh cdp ne Router-A#sh cdp neighbors Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater Device ID Local Intrfce Holdtme Capability Platform Port ID Router-B Ser 1/1 166 RS 1751-V Ser 0/1 RSI WS-C3550- Fas 0/48 Core-A Fas 0/0 166 Router-A# Router-A# Router-A# Router-A#sh run Router-A#sh running-config Building configuration... Current configuration : 2943 bytes version 12.4 service timestamps debug datetime msec service timestamps log datetime msec service password-encryption hostname Router-A ! boot-start-marker boot-end-marker ! enable secret 5 \$1\$5R6g\$gpZ1w8XK5X1KQwxd/PSmD0 no aaa new-model ip cef ! ! 1 ١ no ip domain lookup ip auth-proxy max-nodata-conns 3 ip admission max-nodata-conns 3 ! ! ١ ! 1 !

! ! !

```
!
!
!
1
١
username admin privilege 15 password 7 02050D480809
۱
!
!
class-map match-any XBOX-IN
match access-group 130
class-map match-all VOIP-OUT
match ip precedence 4
class-map match-all XBOX-OUT
match ip precedence 5
!
policy-map QOS-OUT
class XBOX-OUT
 bandwidth percent 65
class VOIP-OUT
 bandwidth percent 25
policy-map QOS-IN
class XBOX-IN
 set ip precedence 5
!
1
!
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key secretkey address 189.181.115.242
!
crypto ipsec transform-set vpntran ah-md5-hmac esp-des esp-md5-hmac
crypto map vpnmap 1 ipsec-isakmp
set peer 189.181.115.242
set transform-set vpntran
match address 110
!
1
interface Ethernet0/0
ip address 192.168.1.63 255.255.255.0
ip nat outside
```

```
ip virtual-reassembly
full-duplex
max-reserved-bandwidth 100
service-policy input QOS-IN
service-policy output QOS-OUT
interface FastEthernet0/0
description LAN-A
ip address 172.21.1.254 255.255.255.0
ip accounting precedence input
ip nat inside
ip virtual-reassembly
ip tcp adjust-mss 1350
speed auto
max-reserved-bandwidth 100
service-policy output QOS-OUT
interface Serial1/0
no ip address
shutdown
interface Serial1/1
description Interfaz WAN
mtu 1400
bandwidth 1300
ip address 189.181.115.241 255.255.255.252
ip tcp adjust-mss 1350
crypto map vpnmap
max-reserved-bandwidth 100
service-policy output QOS-OUT
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip route 172.21.2.0 255.255.255.0 172.21.1.253
ip route 172.22.1.0 255.255.255.0 Serial1/1
١
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static tcp 172.21.1.251 80 interface Ethernet0/0 80
ip nat inside source static udp 172.21.1.251 53 interface Ethernet0/0 53
ip nat inside source static tcp 172.21.1.251 53 interface Ethernet0/0 53
ip nat inside source static tcp 172.21.1.251 3074 interface Ethernet0/0 3074
ip nat inside source static udp 172.21.1.251 3074 interface Ethernet0/0 3074
ip nat inside source static udp 172.21.1.251 88 interface Ethernet0/0 88
```

```
access-list 1 permit 172.21.0.0 0.0.3.255
access-list 110 permit ip 172.21.0.0 0.0.3.255 172.22.1.0 0.0.0.255
access-list 130 permit udp any any eq 88
access-list 130 permit udp any any eq 3074
access-list 130 permit tcp any any eq 3074
access-list 130 permit udp any any eq domain
access-list 130 permit tcp any any eq domain
access-list 130 permit tcp any any eq www
!
!
!
control-plane
!
!
!
!
!
1
!
!
!
line con 0
line aux 0
line vty 0 4
login local
!
end
```

## SH RUN DEL ROUTER-B

Router-B# Router-B#sh ver Cisco IOS Software, C1700 Software (C1700-ADVENTERPRISEK9-M), Version 12.4(25c), RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2010 by Cisco Systems, Inc. Compiled Thu 11-Feb-10 22:24 by prod\_rel\_team

ROM: System Bootstrap, Version 12.2(1r)XE1, RELEASE SOFTWARE (fc1)

Router-B uptime is 17 hours, 37 minutes System returned to ROM by power-on System image file is "flash:c1700-adventerprisek9-mz.124-25c.bin"

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco 1751-V (MPC860P) processor (revision 0x300) with 114688K/16384K bytes of memory. Processor board ID JAD072802GP (366878482), with hardware revision 0000 MPC860P processor: part number 5, mask 2 1 FastEthernet interface 2 Serial(sync/async) interfaces 32K bytes of NVRAM. 32768K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

Router-B# Router-B#sh cdp ne Router-B#sh cdp neighbors Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
Holdtme Capability Platform Port ID Device ID Local Intrfce Ser 0/1 RS 1751-V Router-A 145 Ser 1/1 Communica Realtek RTL8139/810x SEP0019215533FF Fas 0/0 127 Η Fami Router-B# Router-B# Router-B#sh run Building configuration... Current configuration : 2100 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec service password-encryption hostname Router-B ! boot-start-marker boot-end-marker ! enable secret 5 \$1\$uryk\$1D2WtZP6N6t9ry2AE0ACh1 no aaa new-model memory-size iomem 20 ip cef ! ! ! ١ no ip domain lookup ip auth-proxy max-nodata-conns 3 ip admission max-nodata-conns 3 ١ ١ ! ١ 1 ! ١ ! ! !

!

S - Switch, H - Host, I - IGMP, r - Repeater

145

```
!
!
!
username admin privilege 15 password 7 0822455D0A16
!
!
class-map match-any VOIP-IN
match access-group 120
class-map match-all VOIP-OUT
match ip precedence 4
1
!
policy-map QOS-OUT
class VOIP-OUT
 bandwidth percent 50
policy-map QOS-IN
class VOIP-IN
 set ip precedence 4
!
!
1
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key secretkey address 189.181.115.241
!
crypto ipsec transform-set vpntran ah-md5-hmac esp-des esp-md5-hmac
crypto map vpnmap 1 ipsec-isakmp
set peer 189.181.115.241
set transform-set vpntran
match address 110
1
!
1
interface FastEthernet0/0
description LAN-B
ip address 172.22.1.254 255.255.255.0
speed auto
service-policy input QOS-IN
١
interface Serial0/0
no ip address
shutdown
```

```
no fair-queue
interface Serial0/1
description WAN
mtu 1350
bandwidth 1300
ip address 189.181.115.242 255.255.255.252
ip tcp adjust-mss 1350
clock rate 1300000
crypto map vpnmap
service-policy output QOS-OUT
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 Serial0/1
!
no ip http server
no ip http secure-server
!
access-list 110 permit ip 172.22.1.0 0.0.0.255 172.21.0.0 0.0.3.255
access-list 120 permit tcp any any eq 1720
access-list 120 permit tcp any any range 11000 11999
access-list 120 permit udp any any eq 1719
access-list 120 permit udp any any eq 1718
access-list 120 permit tcp any any eq 5060
access-list 120 permit udp any any eq 5060
access-list 120 permit tcp any any range 2000 2002
access-list 120 permit udp any any eq 2427
access-list 120 permit tcp any any eq 2428
access-list 120 permit udp any any range 16384 32767
!
!
!
control-plane
1
١
1
۱
١
line con 0
line aux 0
line vty 0 4
login local
!
end
```

### SH RUN DEL ROUTER-CME

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router-CME
١
boot-start-marker
boot-end-marker
1
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
no ip domain lookup
1
!
1
interface FastEthernet0/0
ip address 172.21.2.250 255.255.255.0
duplex auto
speed auto
1
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.21.2.253
1
!
!
!
!
!
control-plane
!
```

```
!
!
!
telephony-service
max-ephones 4
max-dn 10
ip source-address 172.21.2.250 port 2000
system message VPN con VOIP Proyecto Terminal
create cnf-files version-stamp Jan 01 2002 00:00:00
keepalive 45
max-conferences 4 gain -6
!
!
ephone-dn 1
number 007
name VPNSitioA
!
!
ephone-dn 2
number 008
name VPNSitioB
1
!
ephone 1
mac-address 0060.6E56.69C4
type CIPC
button 1:1
!
!
!
ephone 2
mac-address 0019.2155.33FF
type CIPC
button 1:2
1
!
1
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
!
!
end
```

#### SH RUN DEL AP

AP# AP#sh ver AP#sh version Cisco IOS Software, C1240 Software (C1240-K9W7-M), Version 12.4(25d)JA, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2010 by Cisco Systems, Inc. Compiled Thu 09-Dec-10 15:39 by prod\_rel\_team

ROM: Bootstrap program is C1240 boot loader BOOTLDR: C1240 Boot Loader (C1240-BOOT-M) Version 12.3(7)JA1, RELEASE SOFTWARE (fc1)

AP uptime is 6 hours, 41 minutes System returned to ROM by power-on System image file is "flash:/c1240-k9w7-mx.124-25d.JA/c1240-k9w7-mx.124-25d.JA"

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

cisco AIR-AP1242AG-A-K9 (PowerPCElvis) processor (revision A0) with 25590K/7168K bytes of memory. Processor board ID FTX1021B3QQ PowerPCElvis CPU at 262Mhz, revision number 0x0950 Last reset from power-on 1 FastEthernet interface 2 802.11 Radio(s)

32K bytes of flash-simulated non-volatile configuration memory.Base ethernet MAC Address: 00:17:E0:95:32:64Part Number: 73-9925-04PCA Assembly Number: 800-26579-04

PCA Revision Number : A0 PCB Serial Number : FOC10201JG4 Top Assembly Part Number : 800-26804-02 Top Assembly Serial Number : FTX1021B3QQ **Top Revision Number** : B0 Product/Model Number : AIR-LAP1242AG-A-K9 Configuration register is 0xF AP# AP# AP#sh cdp ne AP#sh cdp neighbors Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater Device ID Local Intrfce Holdtme Capability Platform Port ID Core-A Fas 0 173 R S I WS-C3550- Fas 0/45 AP# AP# AP# AP#sh run AP#sh running-config Building configuration... Current configuration : 3337 bytes version 12.4 no service pad service timestamps debug datetime msec service timestamps log datetime msec service password-encryption 1 hostname AP logging rate-limit console 9 enable secret 5 \$1\$vR1Q\$M5pw18XPxKGT7QljMefkX0 1 no aaa new-model ip domain name Raven ! ! dot11 syslog dot11 ssid Visitantes authentication open guest-mode

```
!
!
crypto pki trustpoint TP-self-signed-3767874148
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-3767874148
revocation-check none
rsakeypair TP-self-signed-3767874148
!
!
crypto pki certificate chain TP-self-signed-3767874148
certificate self-signed 01
```

30820240 308201A9 A0030201 02020101 300D0609 2A864886 F70D0101 04050030 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274

51512F30 2D060555 04051526 494F552D 55656C66 2D556967 6E65642D 45657274 69666963 6174652D 33373637 38373431 3438301E 170D3039 30323138 31373439 30365A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37363738 37343134 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100E91A B2895D66 75C38429 5068D7D5 616E463B D1AA0A1B DCF60445 DDCA31A3

2B0974E0 392483DA A0F9799C 5CE95970 5150FF09 BB2BD590 96198BA6 7DBC42D4

504862FF 59AEC448 2ED39C09 48CA6CD0 7D197E2E F1BB4EAB 03761F68 4D565759

137491AE 04DB1825 9F8784D4 5EC94327 9F783902 88D1261E 02F69F4E 269C742C A34F0203 010001A3 68306630 0F060355 1D130101 FF040530 030101FF 30130603 551D1104 0C300A82 0841502E 52617665 6E301F06 03551D23 04183016 801406AC 762F1EF9 C6BC1031 B7792ADB CDBDD7C1 6E17301D 0603551D 0E041604 1406AC76

2F1EF9C6 BC1031B7 792ADBCD BDD7C16E 17300D06 092A8648 86F70D01 01040500

03818100 463CE710 58DE3BBB F74E42B1 509265A9 856102CF 3A3C3D06 3E00F6BA

F654CE2E 0A019052 BCA38B1D 947E1F82 F0D8C541 58A097F0 E7E76437 046ED9CD

97748CFD E20F4DD6 6B73E0BB DFD19C55 12891D5A 95367EAF F6B416E6 D7D2315C

4245212F 55B551F7 093DB811 5C4090FC 6E5674FE AFB12180 9DD98369 927E5B98 63B36245

```
quit
username admin privilege 15 password 7 02050D480809
١
1
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption key 1 size 40bit 7 F0A59DEBF9F2 transmit-key
encryption mode wep mandatory
1
ssid Visitantes
١
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
interface Dot11Radio1
no ip address
no ip route-cache
!
encryption key 1 size 40bit 7 54F2CCEDFCCE transmit-key
encryption mode wep mandatory
ssid Visitantes
dfs band 3 block
channel dfs
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
1
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
```

```
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
١
interface BVI1
ip address 172.21.1.252 255.255.255.0
no ip route-cache
!
ip default-gateway 172.21.1.253
no ip http server
ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
login local
!
end
```

# FOTO DE LA TOPOLOGÍA DE LA RED.



Equipos:

- 2 Laptop con tarjetas de red Ethernet RJ-45 Sistema Operativo Windows 7.
- 2 Routers Cisco 1700
- 1 Switch Cisco 3550
- 1 Xbox 360
- 1 Computadora de Escritorio HP
- 1 Cisco Wireless Access Point.

### CONCLUSIONES.

La voz sobre IP es una forma útil, practica y escalable de establecer llamadas de teléfono entre distintos usuarios, ya sea en la misma red o en diferentes subredes, de manera que se puedan reducir los gastos por las tarifas de telefonía normal, es de costo más bajo y pueden utilizarse en muchos lugares con conexiones de red local a otros equipos o sobre Internet

La tecnología de la VPN nos permite darle un forma segura de viajar a los paquetes de nuestra red que viajen sobre Internet para llegar a otro destinatario, ya que encriptan y encapsulan los paquetes de manera que nadie pueda descifrarlos o accesar a su contenido si no tienen la llave adecuada para esta acción, de igual manera nos permiten restringir a usuarios dentro de una red para el envió de datos de manera segura de un sitio a otro.

La implementación de QoS nos habilita la mejora de un servicio de red en una red en la cual exista mucho tráfico tanto entrante o saliente debido a la utilización del ancho de banda por diversas aplicaciones, al darle preferencia y prioridad a una o unas aplicaciones, garantizamos un ancho de banda siempre disponible para su optima transmisión y envió de datos sobre la red, lo cual restringe a las demás aplicaciones sin prioridad a ocupar en su mayoría el ancho de banda, lo que asegura un mejor rendimiento de las aplicaciones vitales en las redes y telecomunicaciones.

## **BIBLIOGRAFIA.**

- [1].- http://support.microsoft.com/kb/978618/
- [2]. http://www.cisco.com/en/US/docs/internetworking/technology/handbook/VPN.html

[3]- <u>http://www.binbert.com/blog/2010/08/emulating-cisco-routers-%E2%80%93-using-dynamics-and-gns3/</u>

- [4]- http://es.scribd.com/doc/396087/CCNA-1-y-2
- [5]. http://www.joshgentry.com/cisco/cisco.htm
- [6]- http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/
- [7]- http://www.routergeek.net/content/view/50/37/
- [8]- http://ciscogeek.org/create-vpn-over-internet/
- [9]- http://wiki.treck.com/IKE\_Policies
- [10]- http://www.youtube.com/watch?v=-Cp7dZ5j6u4
- [11]- http://www.cisco.com/en/US/products/ps6120
- [12]- http://www.dslreports.com/faq/14243

[13]- <u>http://ezinearticles.com/?Cisco-CCNA-Certification:-Static-Routing-</u> <u>Tutorial&id=145138</u>

- [14]- http://tftpd32.jounin.net/tftpd32\_download.html
- [15]- http://ciscogeek.org/install-call-manager-express-cme/
- [16]- http://brendon.davis.to/2010/02/05/cisco-gos-for-dummies/
- [17]- http://forums.whirlpool.net.au/archive/549836
- [18]- http://www.ciscopress.com/articles/article.asp?p=1182471
- [19]- <u>http://www.i-1.nl/blog/?p=145</u>
- [20]- <u>http://www.ciscopress.com/articles/article.asp?p=1182471&seqNum=4</u>
- [21]- http://www.ciscopress.com/articles/article.asp?p=731327&seqNum=2
- [22]- http://www.javvin.com/protocolSCCP.html