

QoS y configuración del tráfico en modo bridge transparente

El propósito de este documento es describir la realización de un bridge transparente que es capaz de realizar QoS (Quality of Service) y gestión del ancho de banda en el tráfico de red que lo atraviesa.

La elección del modo bridge (en lugar del modo router) se justifica por la sencillez con que este componente puede ser introducido dentro de una topología de red sin tener que cambiar los parámetros de IP, como la de subred y la puerta de enlace predeterminada.

Como se muestra en el diagrama de la Figura 1, se añadirá el bridge de calidad del servicio “Qos” entre el router de Internet y el switch de nivel 2 a través del cual se conectan los ordenadores de la LAN. Tenga en cuenta que la simplicidad de la configuración elegida no afecta al funcionamiento y será posible aplicarlo en las topologías de redes más complejas. En cualquier caso, tener en cuenta que el procedimiento sigue siendo válido incluso si Zeroshell está configurado para actuar como router de capa 3 en lugar de bridge. Esto se debe a que QoS trabaja directamente en las tarjetas de red (Ethernet, VPN, PPPoE ...) y no dependen del modo de transmisión elegido (router o bridge).

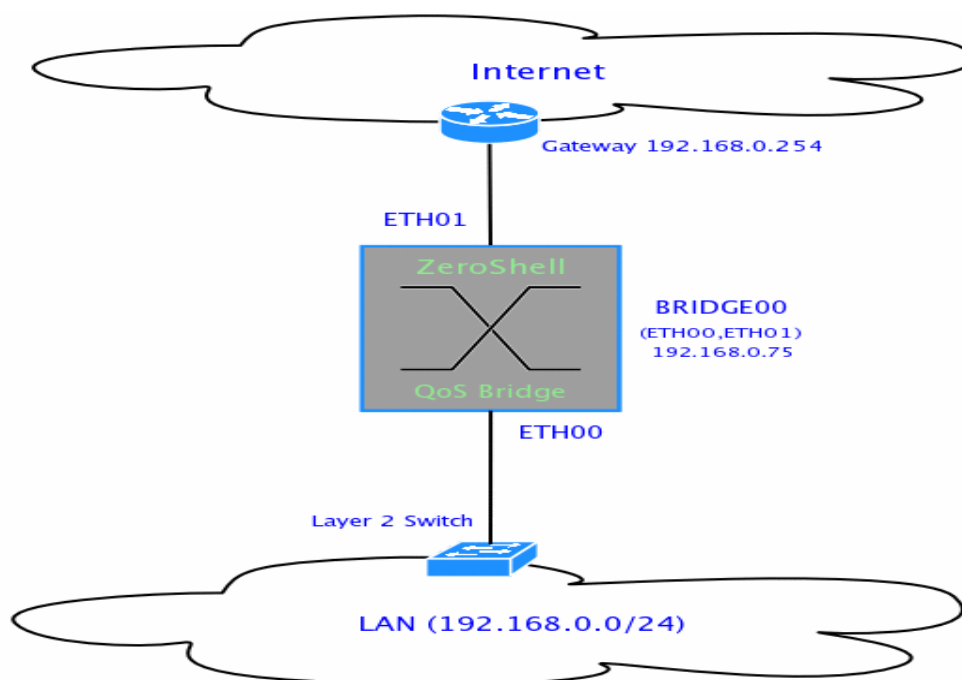


Figura 1. QoS y Traffic Shaping en modo bridge

En la configuración del siguiente ejemplo, vamos a crear un cierto número de tipos de tráfico a los que le asignaremos los parámetros de calidad de servicio, la prioridad, el ancho de banda mínimo garantizado en caso de congestión de red y el máximo ancho de banda cuando la red no este congestionada.

Vamos a utilizar los filtros de capa 7, que con el DPI (Deep Packet Inspection) pueden clasificar los tráficos, como VoIP y peer-to-Peer los cuales no son posibles interceptar mediante el uso de filtros en los puertos TCP y UDP.

En concreto, vamos a obtener los siguientes resultados:

- **Clasificar el trafico VoIP (Voz sobre IP), y el producido por la SIP, H323, Skype y MSN Messenger en una clase de alta prioridad y ancho de banda garantizado. Al hacerlo, el tiempo de latencia se reduce y por tanto la calidad de vídeo y reproducción de la voz es mayor;**
- **Limitar el ancho de banda máximo disponible para la transferencias de archivos P2P (Peer to Peer);**
- **Para evitar que el tráfico producido por Telnet y SSH shell se retrase. Se clasifica este tipo de tráfico dentro de una clase de alta prioridad y de baja latencia;**
- **Para clasificar el tráfico generado por las transferencias FTP y SMTP, en el que muchos de los grandes paquetes de datos se mueven a través de la red, pero que no necesitan una baja latencia. En este caso, tenemos que utilizar una clase con baja prioridad, pero sin límite de ancho de banda máximo.**

Para poner en orden las ideas, vamos a suponer tener un ancho de banda de Internet con 4 Mb/s de bajada y de 2 Mb/s de subida y asignar a las clases de calidad (Qos) los parámetros de la Tabla 1

QoS Clases	Protocolos	Prioridad	Garantizado	Maximo
VOIP	SIP, H323, Skype, MSN Messenger	Alta	1Mbit/s	
P2P	eMule, EDonkey, KaZaA, Gnutella, BitTorrent, Direct Connect	Baja		256Kbit/s
SHELL	ssh, telnet	Alta		
BULK	ftp, smtp	Baja		
DEFAULT	No clasificado	Media		

Tabla 1. Parámetros de las clases de calidad de servicio (Qos)

Antes de empezar a configurar el bridge en Zeroshell y llevar a cabo las políticas de calidad de servicio que queremos, es necesario tener en cuenta los siguientes conceptos:

- **Cuando una clase de QoS se aplica a una tarjeta de red, se controla el tráfico de salida de la tarjeta. En los paquetes entrantes no hay control.**
- **Mirando el punto anterior, se podría pensar que no es posible aplicar la QoS para el tráfico entrante, pero esto no es del todo cierto, porque se puede configurar el tráfico entrante desde la interfaz de ETH01 (figura 1) por el control de la salida del tráfico de la ETH00.**

En las siguientes secciones aprenderemos a configurar Qos en modo bridge transparente:

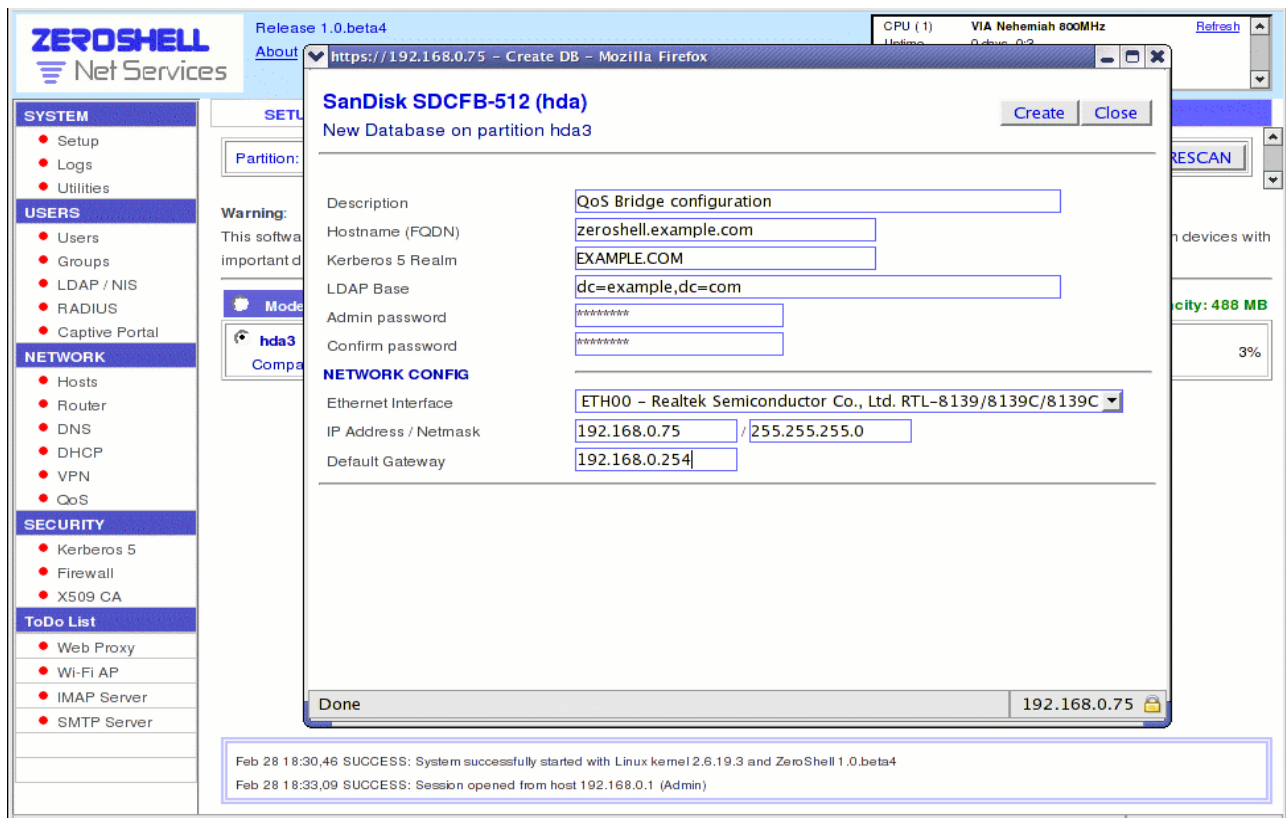
Hacer permanente nuestra configuración:

Para que la configuración de ZeroShell se vuelva permanente y se vuelve a cargar después del reinicio del sistema, es necesario crear y activar una base de datos.

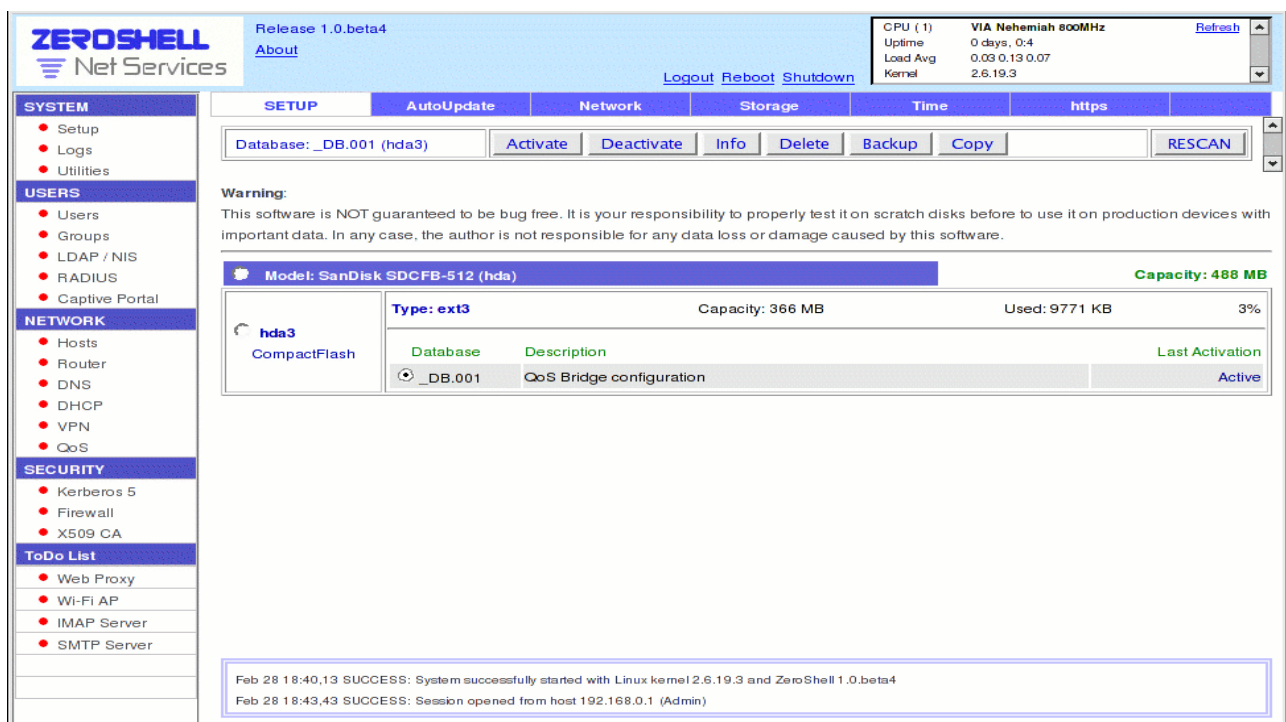
Si usas una versión Live CD es necesario tener un lugar donde guardar la configuración tal como un USB o un HD. Si en cambio usas una versión Compact Flash puedes guardarla en ella. Debido a su mayor estabilidad debes utilizar un sistema de archivos ext3 o ReiserFS. Puedes crear y formatear la unidad desde la interfaz grafica de zeroshell, pero ten cuidado si la unidad contiene datos importantes.

Los pasos para crear y activar la base de datos son los siguientes:

- **En la sección [Setup] -> [Storage] seleccionar la partición en la que crear la base de datos y pulse el botón [Crear DB];**
- **En la ventana que aparece (ver la imagen) insertar una descripción de la base de datos, escriba y confirme la contraseña del usuario admin, compruebe que la dirección IP 192.168.0.75 se configura en el ETH00 de interfaz de red y configurar la puerta de enlace predeterminada a 192.168.0.254.**



- **Pulse el botón [create] para proceder a la generación de bases de datos.**
- **Activar la base de datos seleccionándola y presionando el botón [Activate]. El sistema se reinicia con la nueva configuración (ver la imagen).**



Cuando haya terminado esta fase, puedes estar seguro de que la configuración será permanente.

Creando el bridge BRIDGE00(ETH00,ETH01):

Ahora hay que crear el BRIDGE00 y agregarle las tarjetas de red ETH00 y ETH01 de modo que el tráfico en la capa 2 pueda ser enviado entre ellas. Sin embargo, tenga en cuenta que cuando una tarjeta se convierte en miembro de un puente, automáticamente pierde cualquier IP y configuración de VLAN.

Esto es un problema si estamos conectados a la interfaz grafica de Zeroshell a través de una de las tarjetas que queremos añadir al Bridge.

Solucion:

En la consola de Zeroshell hay una opción llamada "Create a Bridge" que permite migrar automáticamente la configuración (IPs y VLAN) de la tarjeta de red que has elegido a la nueva configuración Bridge. Zeroshell tarda unos 15 segundos en crear la nueva configuración, tiempo durante el cual se pierde la conexión.

Los pasos necesarios para crear el BRIDGE00 (ETH00, ETH01) son los siguientes:

- **Accede al menú y pulse la tecla "B" correspondientes a la función "crear un puente". Si no has sido autenticado se te pedirá la contraseña de administrador. A continuación, pulse la tecla "Y" para confirmar. Elige la interfaz de ETH00 presionando la tecla "1". El puente se ha creado y ha heredado la IP 192.168.0.75 de la ETH00. Después de unos segundos la conectividad entre el navegador en el que está usando la Web GUI y Zeroshell quedara establecida.**

Ahora agregue la tarjeta ETH01 al BRIDGE00. Para hacer esto, utilizando la interfaz gráfica de usuario Web, vaya a la sección [Setup] -> [Network], y pulse el botón [Configure] perteneciente al BRIDGE00 y mueve la tarjeta ETH01 de la lista "Available interfaces" a los componentes del Bridge. (ver la imagen 1) confirmar pulsando el boton "confirm" y la tarjeta ETH01 sera movida a los componentes del Bridge. (ver la imagen 2).

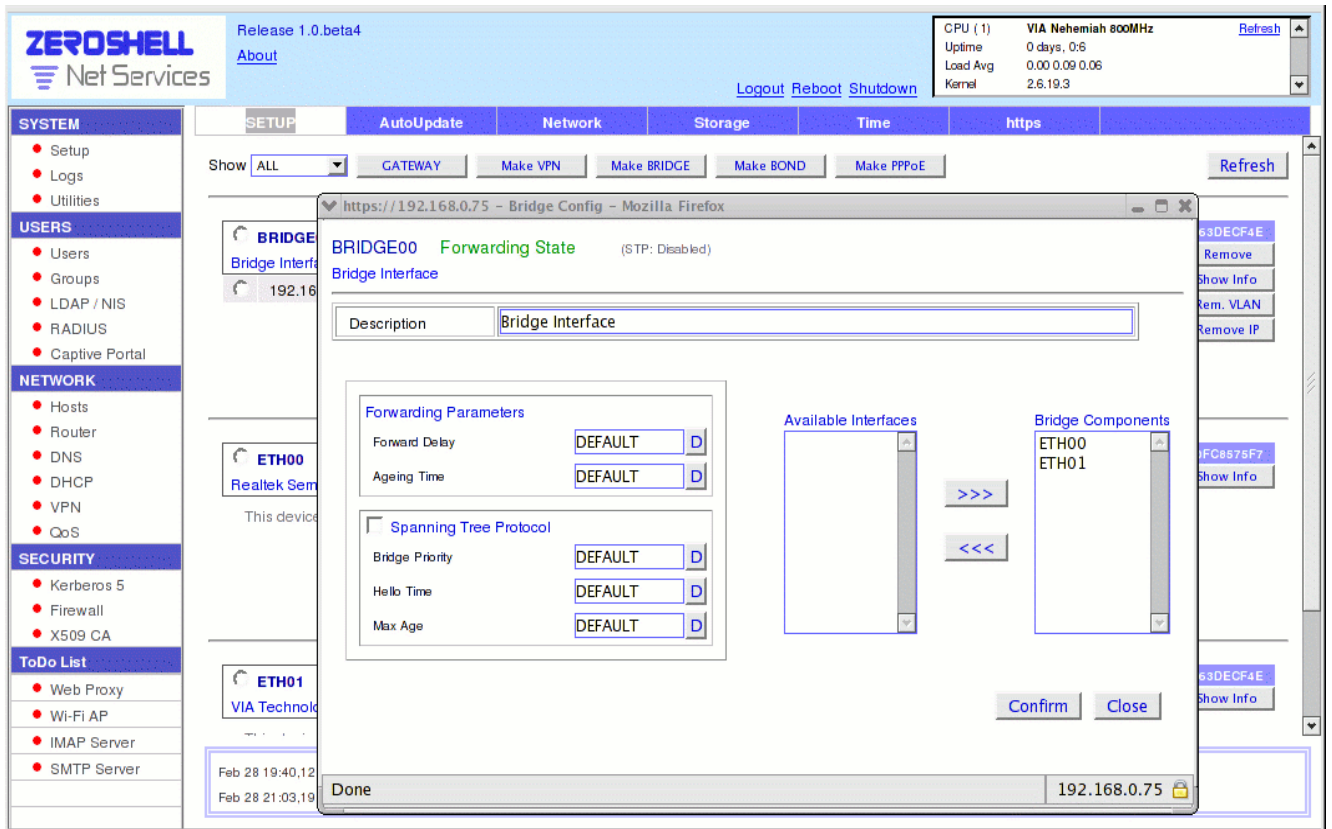


Imagen 1

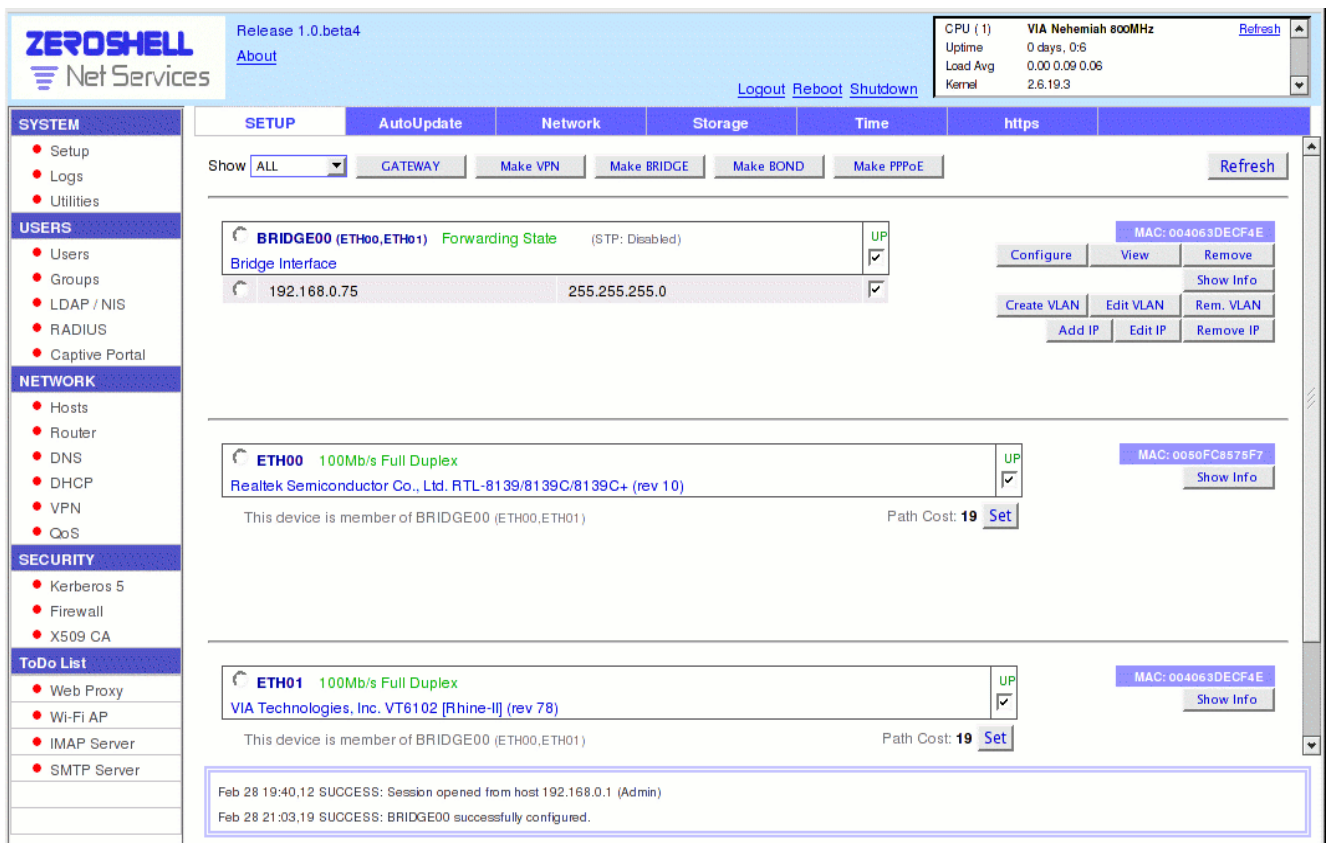


Imagen 2

Asignación del ancho de banda global para las tarjetas de red en modo Bridge.

La asignación del ancho de banda global para cada una de las tarjetas de red es una operación fundamental para el buen funcionamiento de QoS. De hecho, ya que el sistema no es capaz de estimar de forma dinámica la disponibilidad de ancho de banda real, es necesario indicar una estimación basada en el ancho de banda que se distribuirá a las siguientes clases de QoS. Tenga en cuenta que si el ancho de banda real disponible en un momento dado es inferior al estimado, la QoS en ese momento no funcionara bien.

Los pasos necesarios para asignar el ancho de banda global para las interfaces ETH00 y ETH01 son los siguientes:

- En la sección [QoS] -> [Interface Manager], haga clic en el botón [Global Bandwidth] relacionados con la tarjeta ETH00. En el formulario que aparece (ver la imagen) establecer el ancho de banda máximo y el garantizado a 4 Mbits/s y confirme haciendo clic en el botón [Save];

The screenshot displays the Zeroshell Net Services web interface. The top navigation bar includes 'Quality of Service', 'Interface Manager', 'Class Manager', 'Classifier', 'Statistics', and 'L7 Filter'. The left sidebar lists various system, user, network, and security settings. The main content area shows the configuration for interface ETH00, which is a 100Mb/s Full Duplex Realtek Semiconductor Co., Ltd. RTL-8139/8139C/8139C+ (rev 10). The QoS status is 'Disabled' with a maximum bandwidth of 100Mbit/s and a guaranteed bandwidth of 100Mbit/s (Assigned: 0%). A table lists the default class for unclassified traffic with a medium priority. A 'Global Bandwidth' dialog box is open for ETH00, showing input fields for 'Maximum' and 'Guaranteed' bandwidth, both set to 4 Mbit/s. The dialog also has 'Save' and 'Close' buttons. At the bottom, a log shows two successful messages: 'QoS successfully disabled for the interface ETH01' and 'Last changes to the QoS configuration successfully activated'.

- Haga clic en el botón [Global Bandwidth] relacionado con la tarjeta de red ETH01 y establece el ancho de banda máximo y garantizado a 2 Mbit/s.
- Para activar la configuración del ancho de banda global, haga clic en el botón [Activate last Changes].

Creación de los tipos de QoS

Utilice el Administrador de la sección [QoS] -> [Class Manager] (ver la imagen) para crear los Qos que necesitas. Ten en cuenta que inicialmente sólo existe la clase DEFAULT en la que se envía el tráfico sin clasificar.

The screenshot displays the Zeroshell Net Services interface. The top navigation bar includes tabs for Quality of Service, Interface Manager, Class Manager, Classifier, Statistics, and L7 Filter. The Class Manager window is open, showing a table of existing QoS classes and a form to create a new one. The table lists the following classes:

Class	Description	Priority	Max Bandwidth	Guaranteed	On
BULK	Large data transfer	Low			<input checked="" type="checkbox"/>
DEFAULT	Default class for unclassified traffic	Medium			<input checked="" type="checkbox"/>
P2P	File sharing peer to peer	Low	256Kbit/s		<input checked="" type="checkbox"/>
SHELL	Interactive shell traffic	High			<input checked="" type="checkbox"/>
VOIP	Voice over IP	High		1Mbit/s	<input checked="" type="checkbox"/>

The form for creating a new class is currently empty, with fields for Description, Priority (set to Low), Maximum bandwidth (set to kbit/s), and Guaranteed bandwidth (set to kbit/s). The interface also shows a sidebar with navigation menus and a top navigation bar with tabs for Quality of Service, Interface Manager, Class Manager, Classifier, Statistics, and L7 Filter. The Class Manager window is open, showing a table of existing classes and a form to create a new one. The table lists the following classes:

Los pasos a seguir para crear las Qos son los siguientes:

- **Haga clic en el botón [New] de "Class Manager" y escriba VOIP como nombre de la clase. Escribir la descripción de "Voz sobre IP" y luego definir la prioridad en alta y el ancho de banda garantizado de 1 Mbit/s. Guarda la clase haciendo clic en "Save".**
- **Crear la clase P2P utilizando el mismo procedimiento que en el paso anterior, con la descripción " File sharing peer to peer " y luego establecer la prioridad en baja y el ancho de banda garantizado a 256 kbit/s;**
- **Crear la clase Qos SHELL con la descripción de " Interactive shell traffic " y establecerla a alta prioridad;**
- **Crear la clase QoS "BULK" con la descripción " Large data transfer " y establecerla a baja prioridad;**

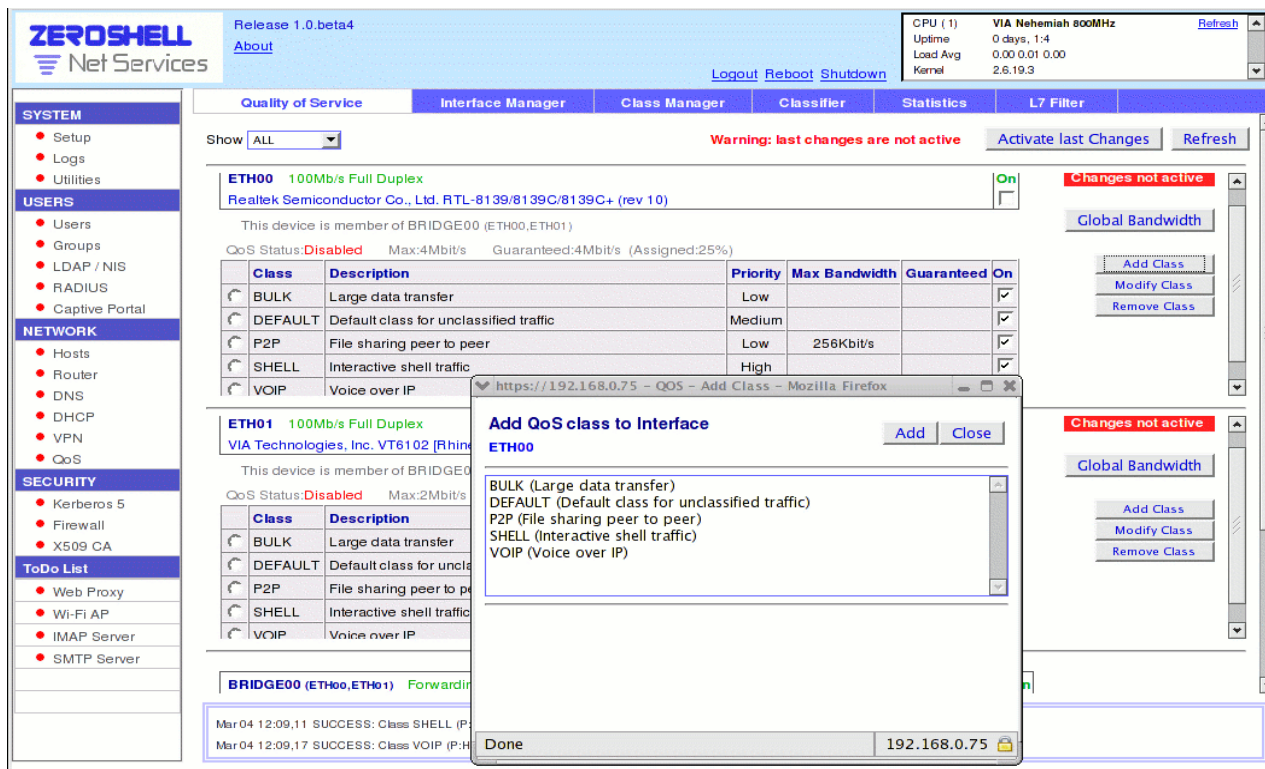
No se debe cambiar la configuración de la clase "Default" porque queremos que todo el tráfico sin clasificar tenga prioridad media y esto ya está establecido en esta clase.

Añadiendo clases Qos a las tarjetas del Bridge.

Ahora es el momento de asignar las clases de QoS creados en los pasos anteriores para las tarjetas de red, cuyo tráfico de salida se desea controlar.

Los pasos para llevarlo a cabo son las siguientes:

- **Clic en [QoS] -> [Interface Manager], y [Add Class] relacionadas con la interfaz ETH00. Desde la ventana de diálogo que aparece (ver la imagen), haga clic en el botón [Add] para las Qos VoIP, P2P, SHELL y BULK;**



- **Añadir las mismas clases a la interfaz ETH01 con el mismo procedimiento del paso anterior;**
- **Activar Qos para ETH00 y ETH01 haciendo clic en los cuadros debajo de "On";**
- **Guarde los cambios haciendo clic en el botón [Activate last Changes].**

Tenga en cuenta que ha activado Qos directamente en (ETH00, ETH01) pero no en BRIDGE00.

En este punto Qos está trabajando en el bridge, pero todo el tráfico saliente es de la clase DEFAULT, ya que todavía no se ha clasificado el tráfico. En los pasos siguientes vamos a hacer eso.

Vinculando los tipos de tráfico a Qos.

Para enlazar un servicio en el que desea aplicar la QoS a una clase se debe usar el "Classifier".

Los pasos a seguir para clasificar el tráfico son las siguientes:

- **Selecciona el clasificador de la sección [QoS] -> [Classifier] (ver la imagen).**

ZEROSHELL Net Services Release 1.0.beta4

CPU (1) VIA Nehemiah 800MHz
Uptime 0 days, 0:7
Load Avg 0.00 0.06 0.05
Kernel 2.6.19.3

Logout Reboot Shutdown

Quality of Service Interface Manager Class Manager Classifier Statistics L7 Filter

Chain: QoS Policy: None Chain: QoS [New] [Remove] [View] [Show Log]

Save Cancel Enabled

QoS Rules [Add] [Change] [Delete]

Seq	Input	Output	Description	QoS Class	Log	Active
1	*	*	MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 ipp2p v0.8.2 --kazaa --gnu --edk --dc --bit MARK set 0xe	P2P	no	<input checked="" type="checkbox"/>
2	*	*	MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 LAYER7 I7proto sip MARK set 0xd	VOIP	no	<input checked="" type="checkbox"/>
3	*	*	MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 LAYER7 I7proto h323 MARK set 0xd	VOIP	no	<input checked="" type="checkbox"/>
4	*	*	MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 LAYER7 I7proto skype MARK set 0xd	VOIP	no	<input checked="" type="checkbox"/>
5	*	*	MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 LAYER7 I7proto msnmessenger MARK set 0xd	VOIP	no	<input checked="" type="checkbox"/>
6	*	*	MARK tcp opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 tcp dpt:22 MARK set 0xf	SHELL	no	<input checked="" type="checkbox"/>
7	*	*	MARK tcp opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 tcp dpt:23 MARK set 0xf	SHELL	no	<input checked="" type="checkbox"/>
8	*	*	MARK tcp opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 tcp dpt:25 MARK set 0xf	SHELL	no	<input checked="" type="checkbox"/>
9	*	*	MARK tcp opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 tcp spt:23 MARK set 0xf	BULK	no	<input checked="" type="checkbox"/>
10	*	*	MARK tcp opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 tcp spt:25 MARK set 0x10	BULK	no	<input checked="" type="checkbox"/>
11	*	*	MARK all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 LAYER7 I7proto ftp MARK set 0x10	BULK	no	<input checked="" type="checkbox"/>

Mar 04 21:52:19 SUCCESS: Chain QoS successfully saved.
Mar 04 21:57:19 SUCCESS: Chain QoS successfully saved.

- **Pulse el botón [Add] para insertar la primera regla en el clasificador relacionada con el intercambio de archivos P2P. En la ventana de diálogo que aparece (ver la imagen) marcar todos los peer-to-peer.**

ZEROSHELL Net Services Release 1.0.beta4

CPU (1) VIA Nehemiah 800MHz
Uptime 0 days, 0:7
Load Avg 0.00 0.06 0.05

https://192.168.0.75 - Firewall Rule config - Mozilla Firefox

QoS Apply to: Routed and Bridged Packets Sequence: 1 [Confirm] [Close]

Packet Matching

Description	Value	Not
Input	[Dropdown]	<input type="checkbox"/>
Output	[Dropdown]	<input type="checkbox"/>
Source IP (*)	[Text]	<input type="checkbox"/>
Destination IP	[Text]	<input type="checkbox"/>
Fragments	<input type="checkbox"/> match only second and further fragments	<input type="checkbox"/>
Source MAC	[Text]	<input type="checkbox"/>

Protocol Matching Not ALL Match all Layer 4 Protocols

Connection State NEW ESTABLISHED RELATED INVALID UNTRACKED Not

Time Matching From [Dropdown] to [Dropdown] [Mon] [Tue] [Wed] [Thu] [Fri] [Sat] [Sun]

Peer-to-Peer eMule,EDonkey,Kademlia KaZaA,FastTrack Gnutella BitTorrent Direct Connect

Layer 7 Filter Protocol Description Not [L7 Manager]

TARGET CLASS [P2P] [LOG] [Second] Burst [Dropdown]

NOTES: (*) The IP addresses can be single IP (ex. 192.168.0.15), network address (ex. 192.168.0.0/255.255.255.0 or 192.168.0.0/24) and IP range (ex. 192.168.0.19-192.168.0.73)
(**) TCP and UDP ports can be single port (ex. 88) and port range (ex. 1903:1973)

Done 192.168.0.75

Mar 04 18:54:06 SUCCESS: Session opened from host 192.168.0.1 (Admin)

- **Seleccione la clase de destino P2P y, a continuación, haga clic en el botón [Confirm] para confirmar la regla;**
- **Ahora es el momento de clasificar el tráfico VoIP. Comienza con el protocolo SIP que lo identifique con el L7-filtro y el Qos VoIP como objetivo (ver la imagen).**

The screenshot displays the ZeroShell Firewall Rule configuration interface. The main window is titled "QoS" and shows a rule configuration for "SIP - Session Initiation Protocol - Internet telephony - RFC 3261". The "TARGET CLASS" is set to "VOIP". The interface includes sections for Packet Matching, Protocol Matching (set to ALL), Connection State, Time Matching, Peer-to-Peer, and Layer 7 Filter. A sidebar on the left lists system, users, network, and security settings. A status bar at the bottom shows system logs.

- **Usando el mismo procedimiento, se debe clasificar en la clase VoIP, los protocolos de H323, Skype a Skype y MSN Messenger;**

Para clasificar el tráfico interactivo en la Qos Shell que tiene una baja latencia utiliza las características de un servidor ssh que escucha en el puerto TCP 22 y el telnet en el puerto TCP 23. Se necesitan cuatro reglas, ya que el clasificador debe clasificar los paquetes con puerto de origen y destino iguales a estos valores (22 y 23). Este es un ejemplo de estas reglas.

https://192.168.0.75 - Firewall Rule config - Mozilla Firefox

QoS Apply to **Routed and Bridged Packets** Sequence **6**

Description	Value	Not
Input		<input type="checkbox"/>
Output		<input type="checkbox"/>
Source IP (*)		<input type="checkbox"/>
Destination IP		<input type="checkbox"/>
Fragments	<input type="checkbox"/> match only second and further fragments]	<input type="checkbox"/>
Source MAC		<input type="checkbox"/>

Protocol Matching Not
TCP Not
 Source Port Not Dest. Port Not Opt Not
 Flags Not **SYN** **ACK** **FIN** **RST** **URG** **PSH**

Connection State NEW ESTABLISHED RELATED INVALID UNTRACKED Not

Time Matching From to Mon Tue Wed Thu Fri Sat Sun

Peer-to-Peer eMule,EDonkey,Kademlia KaZaA,FastTrack Gnutella BitTorrent Direct Connect

Layer 7 Filter **Protocol Description** Not

TARGET CLASS **SHELL** LOG / **Second** Burst

NOTES: (*) The IP addresses can be single IP (ex. 192.168.0.15), network address (ex. 192.168.0.0/255.255.255.0 or 192.168.0.0/24) and IP range (ex. 192.168.0.19-192.168.0.73)
 (**) TPC and UDP ports can be single port (ex. 88) and port range (ex. 1903:1973)

Done 192.168.0.75

- **Para clasificar la mayor parte del tráfico generado por las transferencias de correo electrónico se utiliza la característica de que un servidor SMTP escucha en el puerto 25/tcp (ver la imagen);**

https://192.168.0.75 - Firewall Rule config - Mozilla Firefox

QoS Apply to **Routed and Bridged Packets** Sequence **10**

Description	Value	Not
Input		<input type="checkbox"/>
Output		<input type="checkbox"/>
Source IP (*)		<input type="checkbox"/>
Destination IP		<input type="checkbox"/>
Fragments	<input type="checkbox"/> match only second and further fragments]	<input type="checkbox"/>
Source MAC		<input type="checkbox"/>

Protocol Matching Not
TCP Not
 Source Port Not Dest. Port Not Opt Not
 Flags Not **SYN** **ACK** **FIN** **RST** **URG** **PSH**

Connection State NEW ESTABLISHED RELATED INVALID UNTRACKED Not

Time Matching From to Mon Tue Wed Thu Fri Sat Sun

Peer-to-Peer eMule,EDonkey,Kademlia KaZaA,FastTrack Gnutella BitTorrent Direct Connect

Layer 7 Filter **Protocol Description** Not

TARGET CLASS **BULK** LOG / **Second** Burst

NOTES: (*) The IP addresses can be single IP (ex. 192.168.0.15), network address (ex. 192.168.0.0/255.255.255.0 or 192.168.0.0/24) and IP range (ex. 192.168.0.19-192.168.0.73)
 (**) TPC and UDP ports can be single port (ex. 88) and port range (ex. 1903:1973)

Done 192.168.0.75

- Aunque el FTP utiliza el puerto 21/tcp para intercambiar los comandos, las transferencias tienen lugar en puertos aleatorios y por lo tanto la manera más fácil de clasificar es la clase BULK, es mediante el uso de la capa 7 del filtro (ver la imagen).

The screenshot shows the Firewall Rule configuration interface. The main configuration area is titled "QoS" and includes several sections:

- Apply to:** Routed and Bridged Packets
- Sequence:** 11
- Packet Matching:**
 - Input: [Dropdown]
 - Output: [Dropdown]
 - Source IP (*): [Text Field]
 - Destination IP: [Text Field]
 - Fragments: match only second and further fragments
 - Source MAC: [Text Field]
- Protocol Matching:** ALL (Match all Layer 4 Protocols)
- Connection State:** NEW, ESTABLISHED, RELATED, INVALID, UNTRACKED, Not
- Time Matching:** From [Dropdown] to [Dropdown], Mon, Tue, Wed, Thu, Fri, Sat, Sun
- Peer-to-Peer:** eMule, EDonkey, Kademia, KaZaA, FastTrack, Gnutella, BitTorrent, Direct Connect
- Layer 7 Filter:** Protocol Description: FTP - File Transfer Protocol - RFC 959
- TARGET CLASS:** BULK, LOG / Second Burst

NOTES:

- (*) The IP addresses can be single IP (ex. 192.168.0.15), network address (ex. 192.168.0.0/255.255.255.0 or 192.168.0.0/24) and IP range (ex. 192.168.0.19-192.168.0.73)
- (**) TCP and UDP ports can be single port (ex. 88) and port range (ex. 1903:1973)

Done 192.168.0.75

- Guardar y activar las reglas que has creado haciendo clic en el botón [Save].

Nota: la clasificación del tráfico es una de las operaciones más complejas que participan en la construcción de QoS "sistema de calidad de servicio" No siempre es fácil identificar el tipo de conexión utilizando como filtro único parámetros como las direcciones IP y los numerosos puertos TCP / UDP. De hecho, a menudo hemos utilizado los filtros de capa 7 (I7-filter project) que son capaces de inspeccionar la carga de los paquetes usando expresiones regulares para clasificar el tráfico de la capa de aplicación. Sin embargo, no se debe abusar en el uso del filtro L7, por dos razones. En primer lugar, este tipo de control, que aplica al contenido de los paquetes consume más CPU que los filtros de direcciones IP y puertos TCP / UDP y por lo tanto no podrían funcionar bien en sistemas basados en procesadores lentos. La segunda es que para algunos protocolos los filtros L7 tienen el problema del sobre emparejamiento que es cuando un paquete que no pertenece a un protocolo se identifica como parte de él.

En general, usted no debe usar los filtros de capa 7, cuando es posible identificar una conexión utilizando otros tipos de condiciones.

Supongamos, por ejemplo, que en su situación todas las videoconferencias H.323 utilicen el mismo MCU (Multipoint Conferencing Unit): en este caso, en vez de identificar las conexiones H.323 con el L7-filtro, pueden ser clasificadas con la dirección IP de la MCU.

Ver las estadísticas de Qos

En este punto, Qos está trabajando en modo bridge y el tráfico debería ser clasificado en las clases Qos que ha creado. Para asegurarse de que la clasificación de Qos funciona bien, puede ver las estadísticas en la sección [QoS] -> [Statistics] (ver la imagen).

Interface/Class	Priority	Maximum	Guaranteed	Traffic Sent (bytes)	Rate
ETH00	--	4Mbit/s	4Mbit/s	5156888	3696bit
BULK	Low	--	--	223643	16bit
DEFAULT	Medium	--	--	4067410	16bit
P2P	Low	256Kbit/s	--	0	0bit
SHELL	High	--	--	59782	5584bit
VOIP	High	--	1Mbit/s	806053	0bit
ETH01	--	2Mbit/s	2Mbit/s	17938886	20432bit
BULK	Low	--	--	11479526	16bit
DEFAULT	Medium	--	--	6057182	1104bit
P2P	Low	256Kbit/s	--	0	0bit
SHELL	High	--	--	211368	33696bit
VOIP	High	--	1Mbit/s	190810	0bit

Para cada tarjeta de red en la cual Qos esta activada, usted puede ver las clases Qos asociadas y para cada clase puede ver la configuración (prioridad, máximo ancho de banda y ancho de banda garantizado) así como la cantidad de bytes que se envían fuera de la clase y el tipo, es decir, el número de bits por segundo que se transmiten de la clase. Además, es posible mostrar el gráfico sobre el tráfico saliente clasificado por tipo de tráfico.