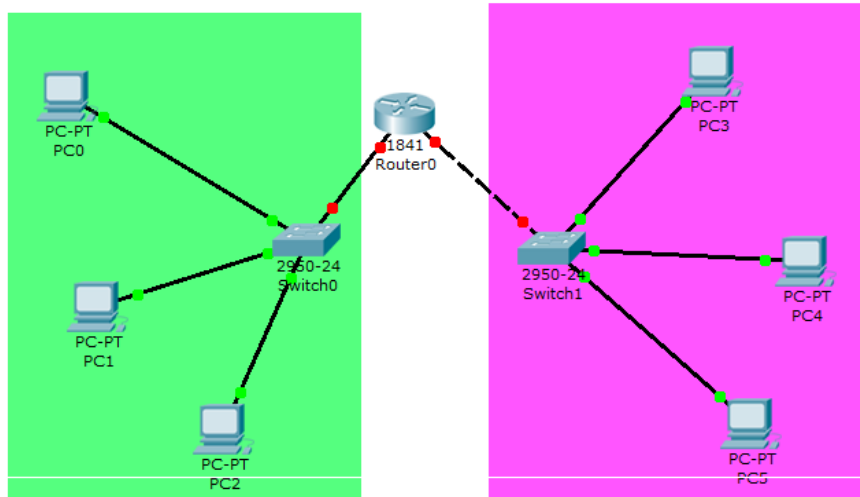


## ACTIVIDAD 2 – TEMA 3 – SAD

Router frontera:

a) Planteamiento escenario CISCO Packet Tracer: esquema.

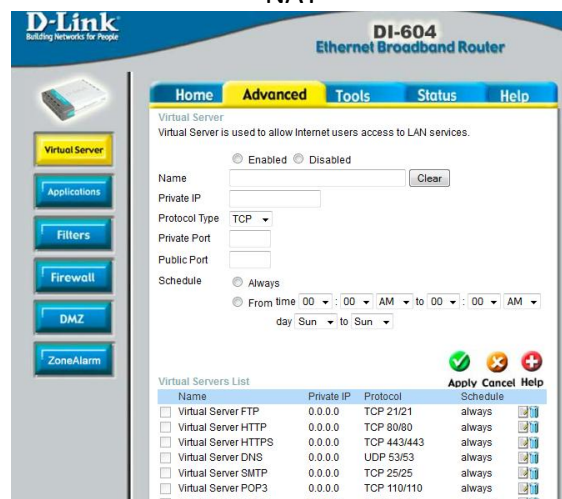


Realiza una comparativa entre los routers frontera atendiendo a las opciones de seguridad perimetral (NAT, Firewall, DMZ,...etc)

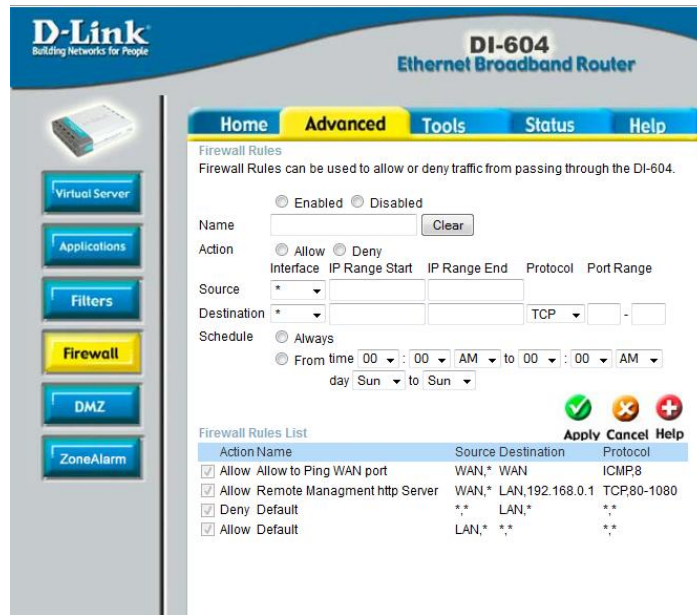
Router DLINK: [http://support.dlink.com/emulators/di604\\_reve](http://support.dlink.com/emulators/di604_reve)

Primero vamos a ver el Router DLink y vamos a ver Nat, Firewall y DMZ de cada uno de ellos

NAT



# FIREWALL



**D-Link**  
Building Networks for People

**DI-604**  
Ethernet Broadband Router

Home **Advanced** Tools Status Help

Firewall Rules  
Firewall Rules can be used to allow or deny traffic from passing through the DI-604.

Enabled  Disabled

Name

Action  Allow  Deny

Interface IP Range Start IP Range End Protocol Port Range

Source \*

Destination \*   TCP  -

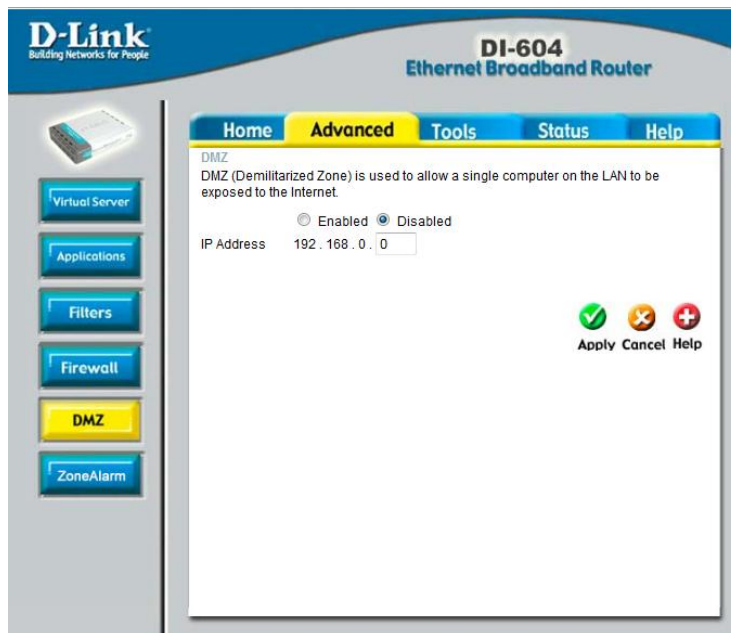
Schedule  Always

From time 00 : 00 AM to 00 : 00 AM  
day Sun to Sun

Firewall Rules List

Action Name	Source	Destination	Protocol
<input checked="" type="checkbox"/> Allow Allow to Ping WAN port	WAN,*	WAN	ICMP8
<input checked="" type="checkbox"/> Allow Remote Management http Server	WAN,*	LAN,192.168.0.1	TCP,80-1080
<input checked="" type="checkbox"/> Deny Default	**	LAN,*	**
<input checked="" type="checkbox"/> Allow Default	LAN,*	**	**

# DMZ



**D-Link**  
Building Networks for People

**DI-604**  
Ethernet Broadband Router

Home **Advanced** Tools Status Help

DMZ  
DMZ (Demilitarized Zone) is used to allow a single computer on the LAN to be exposed to the Internet.

Enabled  Disabled

IP Address 192 . 168 . 0 . 0

# Router LINKSYS: <http://ui.linksys.com/files/WRT54GL/4.30.0/Setup.htm>

## NAT

The screenshot shows the 'Setup' page for a Linksys WRT54GL router, specifically the 'Advanced Routing' section. The 'Static Routing' tab is active. The 'Gateway' dropdown is set to 'Gateway'. The 'Select set number' is '1 ()'. The 'Enter Route Name' field is empty. The 'Destination LAN IP' is '0.0.0.0', 'Subnet Mask' is '0.0.0.0', and 'Default Gateway' is '0.0.0.0'. The 'Interface' is 'LAN & Wireless'. A 'Show Routing Table' button is at the bottom left. On the right, there is a help section with the following text: 'Operating Mode : If the router is hosting your Internet connection, select Gateway mode; if another router exists on your network, select Router mode. Select Set Number: This is the unique route number, you may set up to 20 routes. Route Name: Enter the name you would like to assign to this route. Destination LAN IP: This is the remote host to which you would like to assign the static route. Subnet Mask: Determines the host and the network portion. More...'. 'Save Settings' and 'Cancel Changes' buttons are at the bottom.

## FIREWALL

The screenshot shows the 'Security' page for a Linksys WRT54GL router, specifically the 'Firewall' section. The 'Firewall Protection' is set to 'Enable'. Under 'Block WAN Requests', the following options are checked: 'Block Anonymous Internet Requests', 'Filter Multicast', 'Filter Internet NAT Redirection', and 'Filter DENY (Port 113)'. On the right, there is a help section with the text: 'Firewall Protection : Enable or disable the SPI firewall. More...'. 'Save Settings' and 'Cancel Changes' buttons are at the bottom.

## DMZ

The screenshot shows the 'Applications & Gaming' page for a Linksys WRT54GL router, specifically the 'DMZ' section. The 'DMZ' option is set to 'Disable'. The 'DMZ Host IP Address' is '192.168.1.0'. On the right, there is a help section with the text: 'DMZ : Enabling this option will expose your router to the Internet. All ports will be accessible from the Internet. More...'. 'Save Settings' and 'Cancel Changes' buttons are at the bottom.

# Router TP-LINK: [http://www.tp-link.com/Resources/simulator/WR842ND \(UN\)1.0/index.htm](http://www.tp-link.com/Resources/simulator/WR842ND%20(UN)1.0/index.htm)

## NAT

TP-LINK®
300Mbps Multi-Function Wireless N Router  
Model No. TL-WR842ND

- Status
- Quick Setup
- WPS
- Network
- Wireless
- DHCP
- VPN
- USB Settings
- Forwarding
- Security
- Parental Control
- Access Control
- Advanced Routing
- Static Routing List
- System Routing Table
- Bandwidth Control
- IP & MAC Binding
- Dynamic DNS
- System Tools

Static Routing

ID	Destination Network	Subnet Mask	Default Gateway	Status	Modify
1	172.31.130.30	255.255.255.0	172.31.70.1	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

Add New... Enable All Disable All Delete All

---

Previous Next

Static Routing Help

A static route is a pre-determined path that network information must follow to reach a specific host or network. Use the Static Routing page to add or delete a route.

**To add static routing entries:**

1. Click the **Add New...** button.
2. Enter the following data:
  - **Destination Network** - The Destination IP Address is the address of the network or host that you want to assign to a static route.
  - **Subnet Mask** - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
  - **Default Gateway** - This is the IP address of the default gateway device that allows for the contact between the Router and the network or host.
3. Select the **Enabled** in the **Status** pull-down list.
4. Click the **Save** button to save the changes.

**To modify or delete an existing entry:**

1. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Modify** column.

Click the **Enable All** button to enable all entries.

Click the **Disable All** button to disable all entries.

Click the **Delete All** button to delete all entries.

## FIREWALL

TP-LINK®
300Mbps Multi-Function Wireless N Router  
Model No. TL-WR842ND

- Status
- Quick Setup
- WPS
- Network
- Wireless
- DHCP
- VPN
- USB Settings
- Forwarding
- Security
- Basic Security
- Advanced Security
- Local Management
- Remote Management
- Parental Control
- Access Control
- Advanced Routing
- Bandwidth Control
- IP & MAC Binding
- Dynamic DNS

Basic Security

**Firewall**

**SPI Firewall:**  Enable  Disable

**VPN**

**PPTP Passthrough:**  Enable  Disable

**L2TP Passthrough:**  Enable  Disable

**IPSec Passthrough:**  Enable  Disable

**ALG**

**FTP ALG:**  Enable  Disable

**TFTP ALG:**  Enable  Disable

**H323 ALG:**  Enable  Disable

**RTSP ALG:**  Enable  Disable

Save

Basic Security Help

You can configure the Basic Security Settings on this page.

**Firewall** - Here you can enable or disable the Router's firewall.

- **SPI Firewall** - Stateful Packet Inspection (SPI) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world, you can disable it.

**VPN** - VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the Router.

- **PPTP Passthrough** - PPTP Passthrough, Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, click Enable.
- **L2TP Passthrough** - Layer Two Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer Two level. To allow L2TP tunnels to pass through the Router, click Enable.
- **IPSec Passthrough** - Internet Protocol security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the Router, click Enable.

**ALG** - It is recommended to enable Application Layer Gateway (ALG)

## DMZ

TP-LINK®
300Mbps Multi-Function Wireless N Router  
Model No. TL-WR842ND

- Quick Setup
- WPS
- Network
- Wireless
- DHCP
- VPN
- USB Settings
- Forwarding
- Virtual Servers
- Port Triggering
- DMZ
- UPnP
- Security
- Parental Control
- Access Control
- Advanced Routing
- Bandwidth Control
- IP & MAC Binding
- Dynamic DNS
- System Tools

DMZ

Current DMZ Status:  Enable  Disable

DMZ Host IP Address:

Save

Virtual Servers Help

Virtual servers can be used for setting up public services on your LAN. A virtual server is defined as a service port, and all requests from Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP address because its IP address may change when using the DHCP function.

- **Service Port** - The numbers of External Service Ports. You can enter a service port or a range of service ports (the format is XXX-YYY.XXX is Start port, YYY is End port).
- **Internal Port** - The Internal Service Port number of the PC running the service application. You can leave it blank if the Internal Port is the same as the Service Port, or enter a specific port number when Service Port is a single one.
- **IP Address** - The IP address of the PC running the service application.
- **Protocol** - The protocol used for this application, either TCP, UDP, or All (all protocols supported by the Router).
- **Status** - The status of this entry. "Enabled" means the virtual server entry is enabled.
- **Common Service Port** - Some common services already exist in the pull-down list.
- **Modify** - To modify or delete an existing entry.

**To setup a virtual server entry:**

1. Click the **Add New...** button.
2. Select the service you want to use from the **Common Service Port** list if the **Common Service Port** menu does not list the