

Time Restriction on IP address

To deny Internet access on a certain day and time on a specific IP address. The first thing to do is set the time schedule as follows:

The screenshot displays the configuration interface of a BILLION VoIP/802.11g ADSL2+ Firewall Router. On the left is a navigation menu with options: Status, Quick Start, Configuration, LAN, WAN, System, Firewall, VPN, VoIP, QoS, Virtual Server, Time Schedule, Advanced, Save Config to FLASH, and Language. The 'Time Schedule' option is highlighted with a green arrow and labeled '1. Click on 'Time Schedule''. The main area shows a table titled 'Time Schedule' with columns: ID, Name, Day in a week, Start Time, End Time, Edit, and Clear. The table contains 16 rows, each representing a time slot (TimeSlot1 to TimeSlot16). All slots have 'sMTWTFs' as the day pattern and '08:00' to '18:00' as the time range. A green arrow points to the 'Edit' button of the first row, labeled '2. Click on 'Edit' on a time ID'. At the bottom of the interface are buttons for 'SAVE CONFIG', 'RESTART', and 'LOGOUT'.

ID	Name	Day in a week	Start Time	End Time	Edit	Clear
1	TimeSlot1	sMTWTFs	08:00	18:00	Edit	Clear
2	TimeSlot2	sMTWTFs	08:00	18:00	Edit	Clear
3	TimeSlot3	sMTWTFs	08:00	18:00	Edit	Clear
4	TimeSlot4	sMTWTFs	08:00	18:00	Edit	Clear
5	TimeSlot5	sMTWTFs	08:00	18:00	Edit	Clear
6	TimeSlot6	sMTWTFs	08:00	18:00	Edit	Clear
7	TimeSlot7	sMTWTFs	08:00	18:00	Edit	Clear
8	TimeSlot8	sMTWTFs	08:00	18:00	Edit	Clear
9	TimeSlot9	sMTWTFs	08:00	18:00	Edit	Clear
10	TimeSlot10	sMTWTFs	08:00	18:00	Edit	Clear
11	TimeSlot11	sMTWTFs	08:00	18:00	Edit	Clear
12	TimeSlot12	sMTWTFs	08:00	18:00	Edit	Clear
13	TimeSlot13	sMTWTFs	08:00	18:00	Edit	Clear
14	TimeSlot14	sMTWTFs	08:00	18:00	Edit	Clear
15	TimeSlot15	sMTWTFs	08:00	18:00	Edit	Clear
16	TimeSlot16	sMTWTFs	08:00	18:00	Edit	Clear

- Status
- Quick Start
- Configuration
- LAN
- WAN
- System
- Firewall
- VPN
- VoIP
- GoS
- Virtual Server
- Time Schedule
- Advanced
- Save Config to FLASH
- Language

Time Schedule

Edit Time Slot

ID	1
Name	TimeSlot1
Day	<input type="checkbox"/> Sun. <input checked="" type="checkbox"/> Mon. <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri. <input type="checkbox"/> Sat.
Start Time	09 : 00
End Time	17 : 30
<input type="button" value="Apply"/>	

1. You can use the default name or change it to one of choice.

2. Tick in the box on the day(s) you wish to apply the rule .

3. Set the starting time and the end time.

4. Click on the 'Apply' button.

SAVE CONFIG

RESTART

LOGOUT

Next you need to enable the firewall

The screenshot shows the configuration interface of a BILLION VoIP/802.11g ADSL2+ Firewall Router. The left sidebar contains a menu with the following items: Status, Quick Start, Configuration, LAN, WAN, System, Firewall, General Settings, Packet Filter, Intrusion Detection, URL Filter, IM/P2P Blocking, Firewall Log, VPN, VoIP, QoS, Virtual Server, Time Schedule, and Advanced. The 'Firewall' item is highlighted, and a green arrow points to it with the text '1. Click on 'Firewall''. The main content area is titled 'General Settings' and 'Firewall Security'. It contains the following options: 'Security' with radio buttons for 'Enable' (selected) and 'Disable'; 'All blocked/User-defined'; 'High security level'; 'Medium security level' (selected); and 'Low security level'. A green arrow points to the 'Enable' radio button with the text '2. Click on the 'Enable' radio button.' Below these options is a warning message: '(! If some applications cannot work after enabling Firewall, please check the Packet Filter especially Port Filter rules. For example, adding (TCP:443,outbound allowed) will let HTTPS data go through Firewall.)'. Then, 'Block WAN Request' with radio buttons for 'Enable' and 'Disable' (selected). Another warning message follows: '(! Enable for preventing any ping test from Internet, such as hacker attack.)'. At the bottom of the settings area is an 'Apply' button, which is highlighted with a green arrow and the text '3. Click on the 'Apply' button.' The bottom of the page features three buttons: 'SAVE CONFIG', 'RESTART', and 'LOGOUT'.

BILLION™ VoIP/802.11g ADSL2+ Firewall Router

Powering communications with Security

General Settings

Firewall Security

Security ☒ Enable ☐ Disable

☐ All blocked/User-defined

☐ High security level

☒ Medium security level

☐ Low security level

(! If some applications cannot work after enabling Firewall, please check the Packet Filter especially Port Filter rules. For example, adding (TCP:443,outbound allowed) will let HTTPS data go through Firewall.)

Block WAN Request ☐ Enable ☒ Disable

(! Enable for preventing any ping test from Internet, such as hacker attack.)

Apply

SAVE CONFIG RESTART LOGOUT

- Status
- Quick Start
- Configuration
- LAN
- WAN
- System
- Firewall
 - General Settings
 - Packet Filter
 - Intrusion Detection
 - URL Filter
 - IM/P2P Blocking
 - Firewall Log
- VPN
- VoIP
- QoS
- Virtual Server
- Time Schedule
- Advanced

Packet Filter

[Add TCP/UDP Filter](#)

[Add Raw IP Filter](#)

Packet Filter Rules

Name	Time Schedule	Source IP / Netmask Destination IP / Netmask	Protocol	Source port(s) Destination port(s)	Inbound Outbound		
mei_http	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	80 ~ 80	Block Allow	Edit	Delete
mei_dns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 53 ~ 53	Block Allow	Edit	Delete
mei_tdns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 53 ~ 53	Block Allow	Edit	Delete
mei_ftp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 21 ~ 21	Block Allow	Edit	Delete
mei_tnet	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 23 ~ 23	Block Allow	Edit	Delete
mei_smtp	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit	Delete

SAVE CONFIG






RESTART

LOGOUT


BILLION™ VoIP/802.11g ADSL2+ Firewall Router Powering communications with Security

Packet Filter 6. Enter a name for the rule.

Add TCP/UDP Filter

Rule Name	Helper 			7. Choose the name of the time rule from the drop down list.
Time Schedule	TimeSlot1 			
Source IP Address(es)	0.0.0.0	Netmask	0.0.0.0	8. '0.0.0.0' means any IP.
Destination IP Address(es)	192.168.1.12	Netmask	255.255.255.0	9. The IP address of the machine you wish to apply the time rule.
Type	TCP/UDP 			10. Select the protocol type.
Source Port	0	-	65535	11. Public Ports
Destination Port	0	-	65535	12. Internal ports
Inbound	Block 			13. 'Allow' or 'Block' inbound traffics.
Outbound	Block 			14. 'Allow' or 'Block' outbound traffics.

15. Click on the 'Apply' button.

Apply  Return

SAVE CONFIG RESTART LOGOUT

After the settings are applied you must save the setting permanently.

Status

Quick Start

Configuration

Save Config to FLASH

Language

Save Config to FLASH**Please confirm that you wish to save the configuration.***There will be a delay while saving as configuration information is written to FLASH chips.***b. Click on the 'Apply' button.****a. Click on 'SAVE CONFIG'.**

SAVE CONFIG

RESTART

LOGOUT

Status
Quick Start
Configuration
Save Config to FLASH
Language



c. Click the 'OK' button to complete the process.

SAVE CONFIG

RESTART

LOGOUT