

ASUS VP100

VoIP Gateway/Router/Firewall, 2xEth., 2xFXS port

Uživatelská příručka



OBSAH

1	ZÁKLADNÍ INFORMACE	3
1.1	ČELNÍ PANEL ASUS VP100.....	3
1.2	ZADNÍ PANEL ASUS VP100.....	4
2	INSTALACE ASUS VP100 (SMTA)	5
2.1	BEZPEČNOSTNÍ INSTRUKCE.....	5
2.2	INSTALACE ASUS VP100 (SMTA).....	5
3	RYCHLÝ START	7
3.1	POTŘEBNÉ INFORMACE.....	7
3.2	PŘÍSTUP K ASUS VP100 (SMTA).....	8
3.3	ZÁKLADNÍ NASTAVENÍ.....	9
3.4	SETUP.....	10
3.4.1	WAN – typ připojení DHCP klient.....	10
3.4.2	WAN – typ připojení Statická IP adresa.....	11
3.4.3	WAN – typ připojení PPPoE.....	12
3.5	KONFIGURACE DHCP SERVERU.....	13
3.6	NASTAVENÍ SYSTÉMOVÝCH HODIN.....	14
3.7	UPGRADE FIRMWARE.....	15
3.8	MANAGEMENT - STRÁNKA SPRÁVCE NASTAVENÍ.....	17
3.9	NASTAVENÍ DDNS.....	18
3.10	NASTAVENÍ ZÁLOHOVÁNÍ.....	19
4	ŘEŠENÍ PROBLÉMŮ	20
4.1	INFORMAČNÍ STRÁNKA.....	20
4.2	DIAGNOSTICKÁ STRÁNKA.....	21
5	ADVANCED – KONFIGURACE PRO POKROČILÉ	23
5.1	VOLITELNÉ MÓDY.....	23
5.2	LAN IP ADRESA, MAC ADRESA A FILTROVÁNÍ PORTŮ.....	25
5.3	PŘESMĚROVÁNÍ PORTŮ.....	28
5.4	TRIGGERY.....	29
5.5	DMZ HOSTING.....	30
6	KONFIGURACE FIREWALLU	31
6.1	WEB FILTR.....	31
6.2	LOCAL EVENT LOG– ZÁZNAM LOKÁLNÍCH UDÁLOSTÍ.....	32
7	NASTAVENÍ HLASOVÝCH SLUŽEB	33
7.1	SETUP - NASTAVENÍ.....	33
7.2	KONFIGURACE.....	35

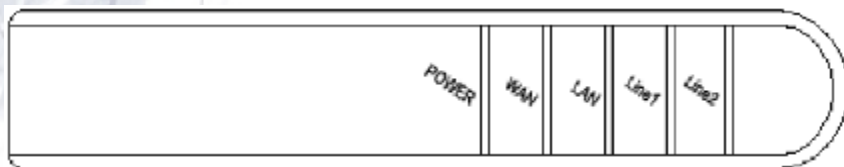
7.3	ADVANCED – KONFIGURACE PRO PORKOČILÉ	36
7.4	AUTO PROVISION – AUTOMATICKÁ KONFIGURACE ..	38
7.5	PHONEBOOK – TELEFONNÍ SEZNAM.....	39
7.6	CALL HISTORY	40
7.7	CALL FEATURES	40

8 PROHLÁŠENÍ O SHODĚ 43

1 ZÁKLADNÍ INFORMACE

ASUS VP100 je samostatný mediální terminálový adaptér (dále jen SMTA) obsahuje VoIP bránu (telefonie přes internet), 10/100Mb Ethernet, Router a Firewall v jednom kompaktním zařízení, pracující na společné firmwarové platformě.

1.1 ČELNÍ PANEL ASUS VP100



LED	Popis
Power	Svítí SMTA je zapnuto Nesvítí SMTA je vypnuto
WAN	Svítí WAN port je připojen k dalšímu zařízení, např. kabelovému modemu Nesvítí Nepřipojeno, připojení nefunguje
LAN	Svítí LAN port je připojen k PC Nesvítí Nepřipojeno, připojení nefunguje Bliká SMTA vysílá/přijímá data přes LAN
Line 1	Svítí Linka 1 - zvednuté sluchátko Nesvítí Linka 1 - zavěšeno
Line 2	Svítí Linka 1 - zvednuté sluchátko Nesvítí Linka 1 - zavěšeno

1.2 ZADNÍ PANEĽ ASUS VP100

ASUS VP100 (SMTA) obsahuje dvě Ethernetová rozhraní (WAN a LAN) a dvě rozhraní telefonní (FXS), ke kterým je možno přímo připojit telefonní přístroje, fax apod.



Port	Popis
WAN	WAN ethernetový port, se konektorem RJ-45 připojí k WAN zařízení jako je kabelový modem nebo ADSL routek atd.
LAN	LAN ethernetový port, se konektorem RJ-45 připojí ethernetovému zařízení, jako jsou např. PC nebo switch atd.
LINE1	Telefonní konektor RJ-11 pro připojení telefonního přístroje nebo faxu
LINE2	
RESET	Krátký stisk – resetuje zařízení beze změny konfigurace. Stiskněte tlačítko na 1 sekundu. Dlouhý stisk – resetuje zařízení a nastavuje počáteční tovární konfiguraci. Držte tlačítko stisknuté po dobu min. 6 sekund
POWER	Napájecí konektor pro 12V zdroj (adaptér)

2 INSTALACE ASUS VP100 (SMTA)

2.1 BEZPEČNOSTNÍ INSTRUKCE

!!! Před instalací si pozorně přečtěte následující informace !!!:

- ASUS VP100 (SMTA) postavte na rovnou plochu blízko kabelům, místo musí být dostatečně větrané.
- Nezakrývejte větrací otvory, zabráníte přehřátí přístroje.
- Přístroj připojte ke zdroji chráněnému bleskojistkou nebo jinou přepětovou ochranou, snížíte tím riziko zničení bleskem nebo napěťovými špičkami.
- Neotvírejte kryt přístroje. Otevření má za následek ztrátu záruky.
- Před zahájením čištění přístroje ho nejprve odpojte od zdroje napětí. K čištění můžete použít vlhký hadřík. Nepoužívejte tekuté nebo rozprašovací čističe ani antistatické prostředky.

2.2 INSTALACE ASUS VP100 (SMTA)

Připojte všechny kabely do příslušných zásuvek.

ASUS VP100 (SMTA) disponuje dvěma telefonními linkami. Kabely zapojte následujícím způsobem:

1. Telefon či fax propojte kabelem RJ-11 se zásuvkou označenou LINE1
2. Pokud budete používat druhý telefon nebo fax, připojte ho dalším kabelem s konektory RJ-11 k zásuvce označené LINE2.

ASUS VP100 (SMTA) má dva ethernetové porty 10/100Base-T auto MDI/MDIX pro síť LAN a WAN. Oba porty je možno připojit kabelem z kroucených dvojlinek RJ-45 k PC, switchi nebo hubu. Kabely připojte následujícím způsobem:

1. Připojte WAN port k účastnické zásuvce modemu poskytovatele.
2. Připojte LAN port k ethernetové zásuvce vašeho síťového zařízení (PC, notebook, switch, atd.)

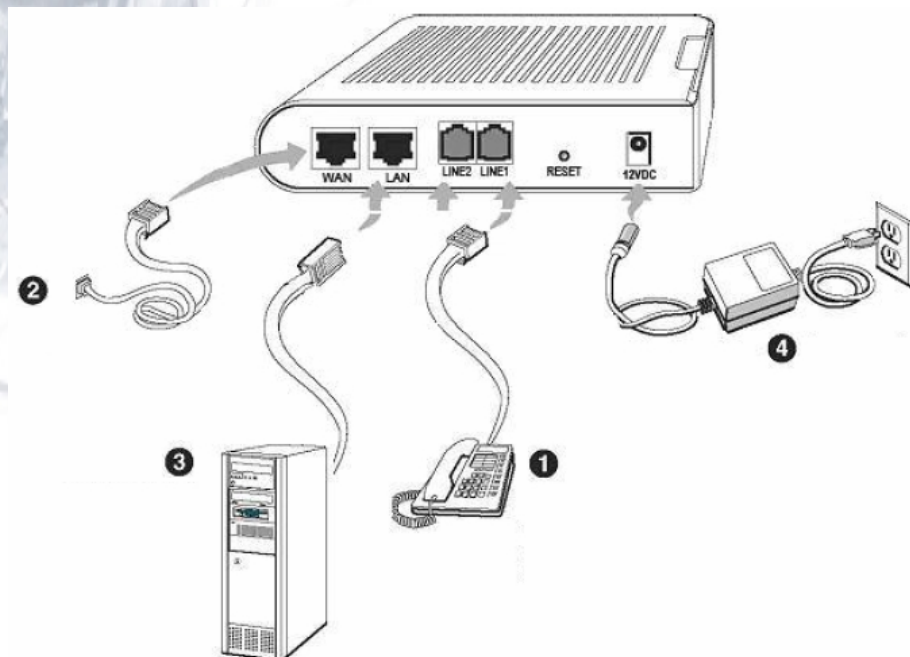
Nakonec připojte k SMTA jeho napájecí zdroj.

1. Zasuňte dutý napájecí konektor AC adaptéru do zásuvky označené 12V DC.

***Poznámka:** Napájecí zdroj (AC adapter) je univerzální pro vstupní napětí elektrické rozvodné sítě v rozsahu od 100 do 240 V (50/60 Hz).*

2. Zapojte AC adapter do elektrické zásuvky.

Následující obrázek zobrazuje zapojení SMTA:



1. Porty LINE1 a LINE2 připojte k telefonním přístrojům nebo faxu pomocí kabelu RJ-11
2. WAN port propojte ethernetovým kabelem RJ-45 s modemem ADSL nebo kabelovým modemem atd..
3. LAN port spojte s ethernetovou zásuvkou PC, hubu nebo switchu pomocí kabelu RJ-45
4. Do napájecí zásuvky zastrčte dutý konektor AC adaptéru a ten zapojte do elektrické sítě

3 RYCHLÝ START

Tato část obsahuje návod, jak rychle nastavit a uvést do provozu VoIP zařízení ASUS VP100 (SMTA), takže Váš PC získá přístup k veřejnému internetu prostřednictvím Vámi zvoleného internetového poskytovatele (ISP).

3.1 POTŘEBNÉ INFORMACE

Ke konfiguraci ASUS VP100 (SMTA) potřebujete znát následující údaje; obvykle je dodá poskytovatel služby:

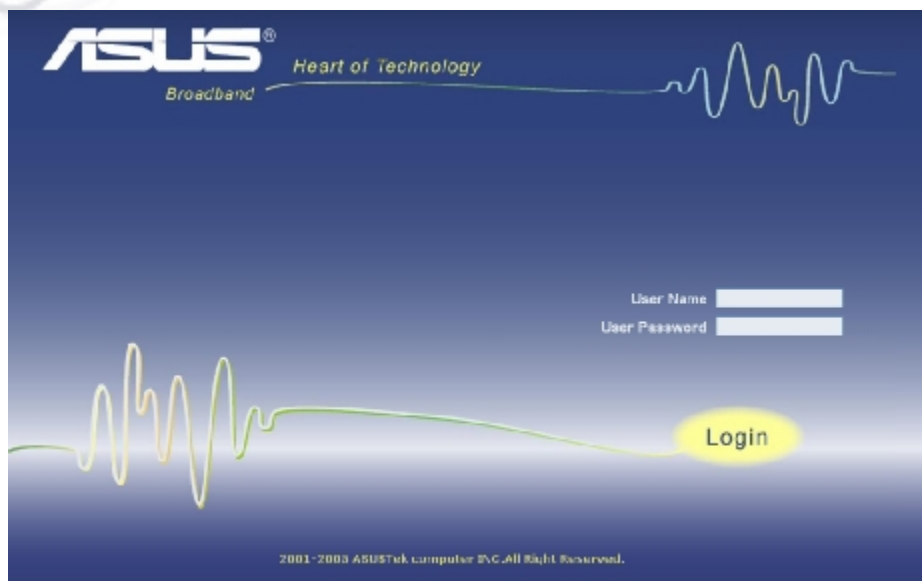
1. Jestliže Váš poskytovatel **NEPOUŽÍVÁ** DHCP (dynamické přidělování IP adresy), budete potřebovat následující:
 - Statickou IP adresu nebo PPPoE účet přidělený Vašemu počítači
 - Masku podsítě, kterou používá Váš ISP
 - IP adresu výchozí brány (gateway)
 - IP adresy primárního a sekundárního DNS serveru
2. Někteří poskytovatelé **MOHOU** požadovat následující informace:
 - MAC (Media Access Control) adresu připojeného zařízení
 - Hostname připojeného počítače
 - Název domény, kterou poskytovatel používá

3.2 PŘÍSTUP K ASUS VP100 (SMTA)

Nastavená IP adresa SMTA je 192.168.15.1 z LAN strany. Nastavení parametrů SMTA probíhá prostřednictvím web stránek:


1. Z vestavěného DHCP serveru získajte IP adresu připojeného počítače, ze kterého budete konfiguraci provádět
2. Spusťte web prohlížeč (Internet Explorer nebo Netscape atd.)
3. Do adresového řádku zadejte URL adresu <http://192.168.15.1>

Po navázání spojení se zobrazí přihlašovací okno, podobné tomu na obrázku. Heslo je shodné s uživatelským jménem: pro obojí můžete použít buď „admin“ nebo „user“. Po zadání jména a hesla klikněte na tlačítko Login. Použitím jména (a hesla) „admin“ získáte některá další práva, která pod jménem „user“ nejsou přístupná.



3.3 ZÁKLADNÍ NASTAVENÍ

Po přihlášení se zobrazí stránka aktuálního stavu systému (Status)



ASUS[®] Heart of Technology Logout

[Broadband](#) **Status** [Basic](#) [Advanced](#) [Firewall](#) [Voice](#)

[Status](#)

- Information**
- Diagnostics

Information Status

This page displays information on the current system.

Standard Specification Compliant	VoIP Gateway
Hardware Version	1100(AW66002 REV:2.25)
Firmware Version	3.5.1(C0.0.6.0)
Build Time	Mar 23 2005,15:38:28
System Current Time	Thu Mar 24 01:52:22 2005
WAN MAC Address	00:10:18:DE AD:83
WAN Connection Type	DHCP Client
WAN IP Address	10.7.1.204
Voice Service	on-line

3.4 SETUP

Stránka Setup umožňuje konfigurovat nastavení WAN (pouze řádek *LAN IP Address* obsahuje údaj týkající se LAN). Podle typu připojení, které používá Váš poskytovatel je třeba zvolit *WAN connection type*. Označte jednu z možností: *DHCP client*, *static IP* nebo *PPPoE*.

ASUS Heart of Technology Logout

Broadband Status **Basic** Advanced Firewall Voice

Basic

Setup

- Setup
- DHCP
- Time
- Download
- Management
- DHCP
- Backup Settings

Setup Basic

This page allows configuration of the basic features of the broadband gateway related to your ISP's connection.

Network Configuration

LAN IP Address: 192 | 168 | 15 | 1

MAC Address: 00:10:10:0E:AD:05

WAN Connection Type: DHCP client Static IP PPPoE

MTU: 1500

PPPoE Username:

Password:

Enable PPPoE Keep-Alive: Yes No

Keep Alive Period (seconds): 30

WAN IP Address::.....

MAC Address: 00:10:10:0E:AD:00

Duration: D: -- H: -- M: -- S: --

Expires::.....

DNS Server Address:

Host Name: (Required by some ISPs)

Static IP Address: | | |

Static IP Mask: | | |

Default Gateway: | | |

Primary DNS (static IP only): | | |

Secondary DNS (static IP only): | | |

Spotted MAC Address: | | | | |

©2001-2005
ASUSTEK COMPUTER INC.
All rights reserved.

3.4.1 WAN – typ připojení DHCP klient

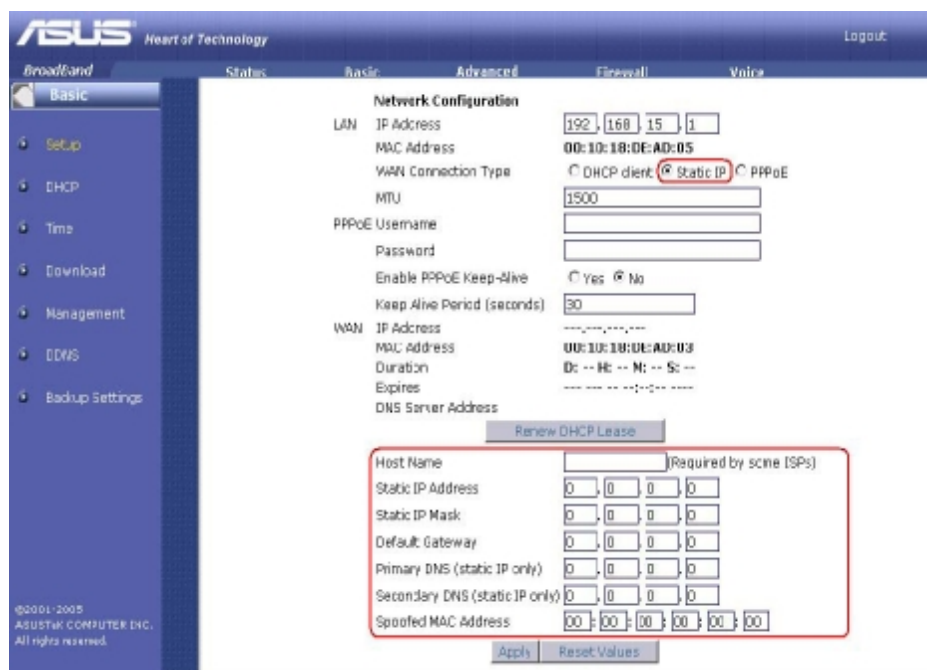
Pokud Váš poskytovatel používá DHCP, klikněte pouze na přepínací tlačítko *DHCP client* a pak na tlačítko **Apply**. Jestliže jste již dříve nakonfigurovali DHCP připojení a chcete pouze obnovit stávající pronájem adresy, klikněte na *Renew DHCP Lease*.

3.4.2 WAN – typ připojení *Statická IP adresa*

Pokud Vám poskytovatel přidělil statickou IP adresu, potom je třeba aktualizovat následující políčka:

- Host Name – nepovinné, vyžadováno některými poskytovateli
- Static IP Address
- Static IP Mask (Maska podsítě)
- Default Gateway (Výchozí brána)
- Primary DNS
- Secondary DNS
- Spoofed MAC Address – jedinečná MAC adresa. Váš poskytovatel může požadovat, abyste zde zadali MAC adresu Vašeho počítače. Pokud ne, můžete stranu WAN opatřit MAC adresou routeru jakožto koncového zařízení; v tomto případě zadejte samé nuly.

Po vyplnění potřebných políček stiskněte **Apply**, SMTA bude restartováno do vašeho nastavení.



ASUS Heart of Technology Logout

BroadBand Status Basic Advanced Firewall Voice

Basic

- Setup
- DHCP
- Time
- Download
- Management
- DDNS
- Backup Settings

Network Configuration

LAN IP Address: 192, 168, 15, 1
 MAC Address: 00:10:18:0E:AD:05
 WAN Connection Type: DHCP client Static IP PPPoE
 MTU: 1500
 PPPoE Username:
 Password:
 Enable PPPoE Keep-Alive: Yes No
 Keep Alive Period (seconds): 30

WAN IP Address:
 MAC Address: 00:10:18:0E:AD:03
 Duration: D: -- H: -- M: -- S: --
 Expires: -----
 DNS Server Address:

Host Name: (Required by some ISPs)

Static IP Address:

Static IP Mask:

Default Gateway:

Primary DNS (static IP only):

Secondary DNS (static IP only):

Spoofed MAC Address:

©2001-2005 ASUS® COMPUTER INC. All rights reserved.

3.4.3 WAN – typ připojení PPPoE

Pokud Váš poskytovatel používá připojení PPPoE (Point-to-Point Protocol over Ethernet), stačí vyplnit následující políčka:

1. Vložte PPPoE uživatelské jméno (username) a heslo (password)
2. Zvolte „yes“, jelikož chcete zapnout funkci KeepAlive (udržovat spojení)
3. V případě „yes“ zadejte periodu obnovování v sekundách
4. Po ukončení zadání klikněte na **Apply** ve spodní části obrazovky.

The screenshot shows the ASUS router's web interface. The 'Basic' tab is selected under 'Network Configuration'. The 'WAN Connection Type' is set to 'PPPoE'. The 'PPPoE Username' and 'Password' fields are highlighted with a red box. The 'Enable PPPoE Keep-Alive' option is selected with a radio button, and the 'Keep Alive Period (seconds)' is set to 30. The 'WAN IP Address' is set to 192.168.15.1. The 'Host Name' field is empty, and the 'Static IP Address' and 'Static IP Mask' fields are also empty. The 'Apply' button is visible at the bottom.

Nyní je SMTA nakonfigurováno pro využívání základních funkcí. Pro získání přístupu k Internetu je třeba následující:

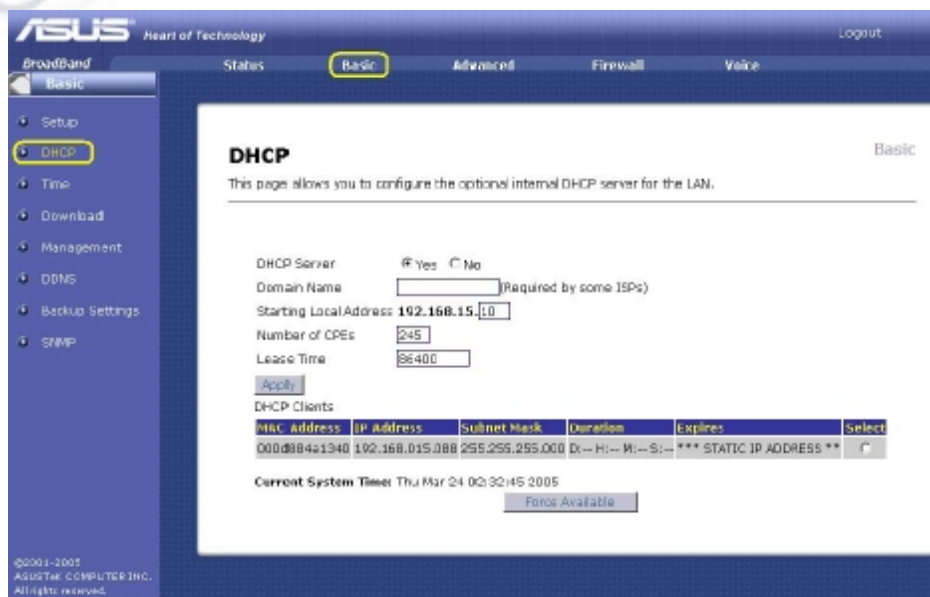
1. Zapněte SMTA a počkejte, až se zaregistruje u poskytovatele a obdrží použitelnou IP adresu.

- Pro každé PC připojené k LAN portu získáte pronájem IP adresy z vnitřního DHCP serveru.

***Poznámka:** Komunikace na straně LAN probíhá nezávisle na funkčnosti WAN připojení. Přístup k internetu však bude fungovat až po připojení WAN a nastavení jeho IP adresy.*

3.5 KONFIGURACE DHCP SERVERU

Nastavení DHCP serveru lze rovněž měnit a to prostřednictvím stránky DHCP v základním menu zobrazeném níže.



ASUS Heart of Technology Logout

English
States
Basic
Advanced
Firewall
Voice

Basic
Setup
DHCP
Time
Download
Management
DDNS
Backup Settings
SNMP

DHCP Basic

This page allows you to configure the optional internal DHCP server for the LAN.

DHCP Server Yes No
 Domain Name (Required by some ISPs)
 Starting Local Address:
 Number of CPEs:
 Lease Time:

DHCP Clients

MAC address	IP address	Subnet Mask	Duration	Expires	Select
000d884a1340	192.168.015.088	255.255.255.000	Di--H:--W:--S:--	*** STATIC IP ADDRESS **	<input type="button" value=""/>

Current System Time: Thu Mar 24 02:32:45 2005

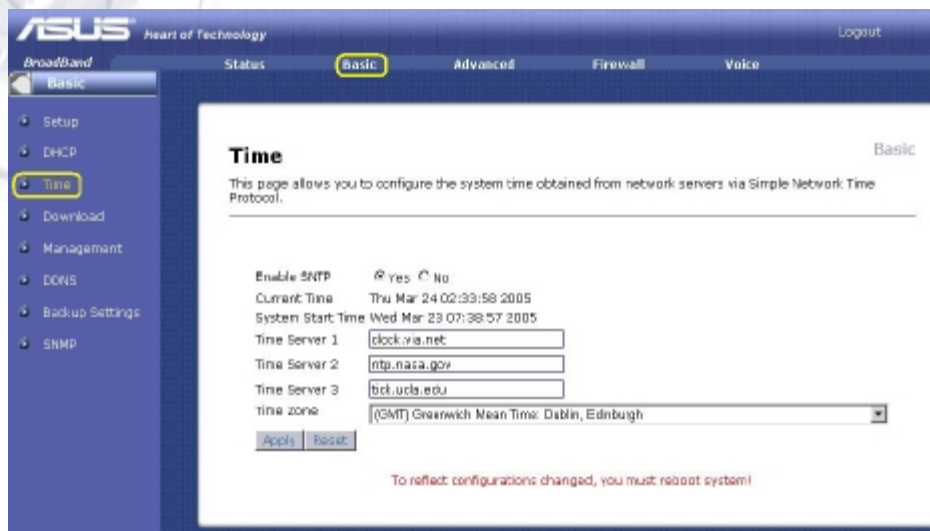
©2005-2005 ASUS® COMPUTER INC. All rights reserved.

Pokud používáte na straně LAN vlastní DHCP server, můžete vnitřní DHCP server vypnout zvolením „no“. Pokud tak učiníte, zkontrolujte, zda LAN IP adresa SMTA spadá do stejné masky podsítě jako externí DHCP server (maska podsítě je vždy 255.255.255.0), jinak SMTA bude za strany LAN nedostupný. IP adresa SMTA se nastavuje na stránce Basic Setup.

Také můžete nastavit počáteční IP adresu pronajímaných IP adres na straně LAN a upravit tak maximální počet počítačů, které mohou být k LAN připojeny.

3.6 NASTAVENÍ SYSTÉMOVÝCH HODIN

SMTA používá SNTP (protokol pro synchronizaci systémového času se zdrojem přesného času v internetu). Na stránce je zobrazen okamžitý a startovní systémový čas. V případě změny konfigurace je třeba SMTA restartovat, aby se změna projevila.



- **Enable SNTP** – zvolte „yes“ pro zapnutí funkce automatické synchronizace času.
- **Current Time** – okamžitý čas systému.
- **System Start Time** – počáteční čas běhu systému.
- **Time Server[1-3]** – adresy časových serverů, se kterými se má systém synchronizovat. Nejdříve se pokusí spojit s Time Server 1. Jestliže spojení selže, pokusí se spojit s druhým atd.

***Poznámka:** V řádce Time Server 1-3 jsou již adresy přednastaveny, můžete je podle potřeby změnit.*

- Time Zone – časové pásmo; vyberte ho podle své geografické polohy.

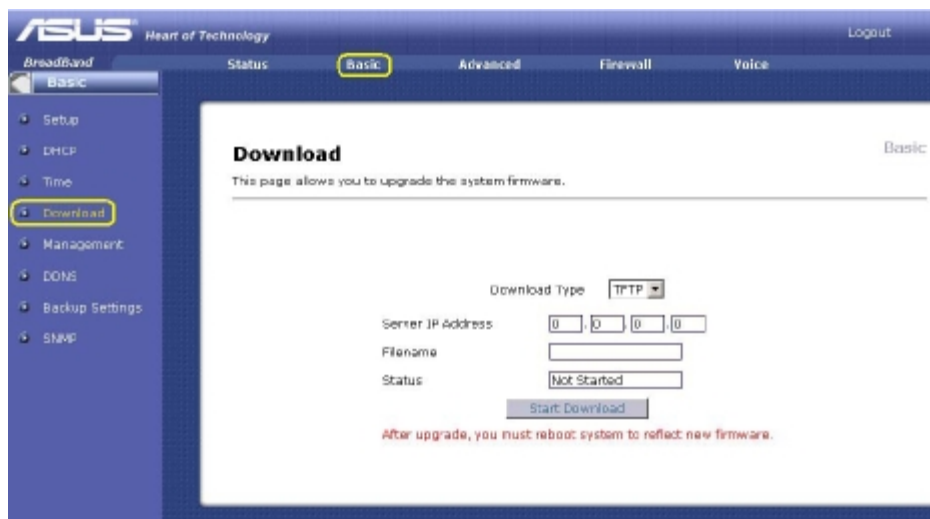
3.7 UPGRADE FIRMWARE

Pro upgrade firmwaru SMTA je potřeba nejdříve stáhnout příslušný firmware z internetu (www.joyce.cz). Po stažení souboru je firmware možno upgradovat dvěma metodami – TFTP (Trivial File Transfer Protocol) nebo HTTP (HyperText Transfer Protocol).

Nahrání pomocí TFTP –

1. V roletě zvolte TFTP
2. Zadejte IP adresu TFTP serveru, na kterém máte stažený soubor.
3. Zadejte jméno souboru, který obsahuje upgrade firmwaru
4. Klikněte na tlačítko Start Download.

***Poznámka:** Po úspěšném stažení souboru se objeví výzva k restartování přístroje*



ASUS® Heart of Technology Logout

Broadband Status **Basic** Advanced Firewall Voice

Basic

- Setup
- DHCP
- Time
- Download**
- Management
- DNS
- Backup Settings
- SNMP

Download

Basic

This page allows you to upgrade the system firmware.

Download Type

Server IP Address

Filename

Status

After upgrade, you must reboot system to reflect new firmware.

Nahrání pomocí HTTP –

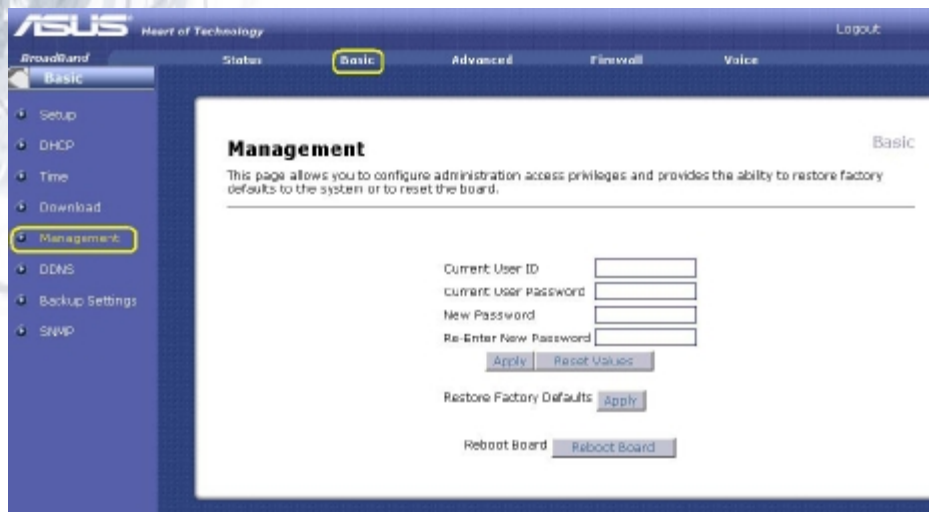
1. V roletě zvolte HTTP
2. Klikněte na **Browse** (Procházet) a najděte upgrade soubor na Vašem PC.
3. Klikněte na tlačítko **Start Download**.

Následující obrázek zobrazuje stránku pro stažení protokolem HTTP.



3.8 MANAGEMENT - STRÁNKA SPRÁVCE NASTAVENÍ

Někdy je zapotřebí obnovit původní nastavení parametrů. Toto je možné provést ze stránky Management Page, která je přístupná z Basic Menu, jak je zobrazeno níže:



Změna hesla –

***Poznámka:** Nelze změnit uživatelská jména na jiná než „admin“ a „user“. Pouze hesla je možno měnit.*

1. Zadejte současné uživatelské jméno (ID), pod kterým jste právě přihlášení a příslušné heslo.
2. Vložte nové heslo.
3. Znovu zadejte nové heslo pro vyloučení možnosti překlepu.
4. Klikněte na **Apply** pro aplikaci zadaných změn.
5. Jestliže chcete začít znovu a vymazat všechna zadávací pole, klikněte na **Reset Values**.

Obnovit tovární nastavení –

Pro obnovení původního nastavení klikněte na druhé tlačítko **Apply** (Restore Factory Defaults). Přístroj se resetuje na původní nastavení z výroby.

Rebootování desky –

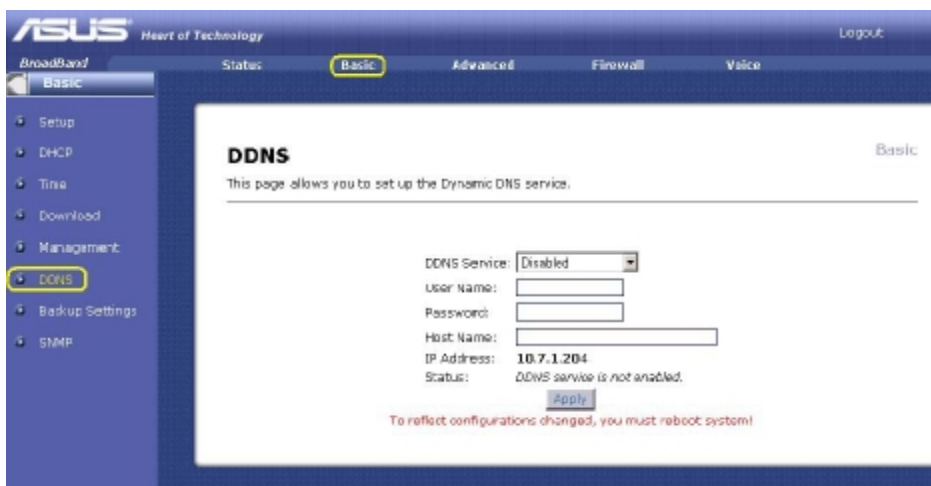
Toto je stejná funkce jako stisknutí resetovacího tlačítka na zadním panelu SMTA. Před restartováním budou uloženy všechny změny nastavení.

3.9 NASTAVENÍ DDNS

Používáte-li DDNS (Dynamic Domain Name System – dynamická služba doménových jmen), službu k monitorování IP adresy svého webového nebo FTP serveru, zde můžete zadat údaje, které Vám poskytl Váš DDNS poskytovatel. Přednastavený poskytovatel DDNS je www.DynDNS.org.

- **DDNS Service:** Vyberte přednastaveného poskytovatele DDNS: www.DynDNS.org
- **UserName:** Zadejte uživatelské jméno přidělené poskytovatelem
- **Password:** Zadejte heslo přidělené poskytovatelem.
- **HostName:** Hostname, které je registrované na webové stránce DDNS poskytovatele.
- **IP Address:** Zadejte IP adresu WAN portu (stejná jako je na Information page)
- **Status:** Zobrazení okamžitého stavu služby DDNS.

Po zadání všech údajů klikněte na tlačítko **Apply**.



ASUS Heart of Technology Logout

Broadband Status **Basic** Advanced Firewall Voice

Basic

- Setup
- DHCP
- Tina
- Download
- Management
- DDNS**
- Backup Settings
- SNMP

DDNS

Basic

This page allows you to set up the Dynamic DNS service.

DDNS Service:

User Name:

Password:

Host Name:

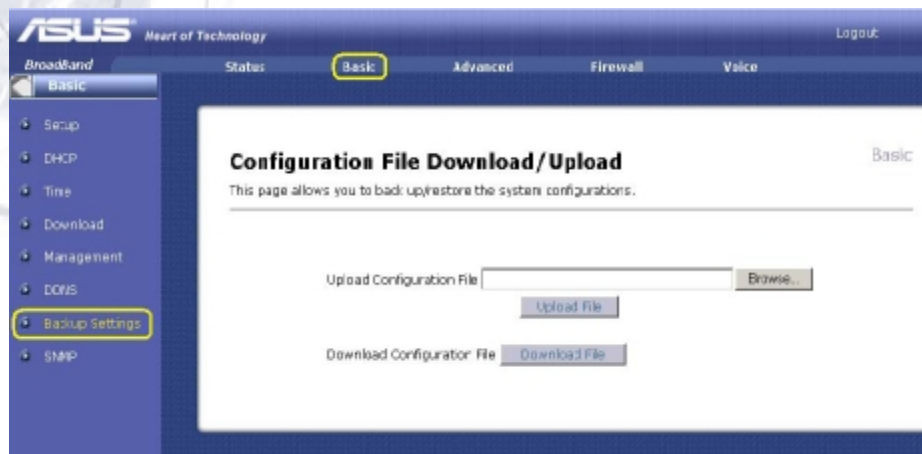
IP Address: 10.7.1.204

Status: DDNS service is not enabled.

To reflect configurations changed, you must reboot system!

3.10 NASTAVENÍ ZÁLOHOVÁNÍ

Na této stránce můžete uložit nebo naopak nahrát svoje nastavení parametrů SMTA do / ze svého PC. Jestliže chcete nahrát konfiguraci, již dříve uloženou v souboru na PC, vyhledejte tento konfigurační soubor (tlačítko Browse) a stiskněte tlačítko Upload File. Pokud chcete uložit současnou konfiguraci systému, klikněte na Download File.




4 ŘEŠENÍ PROBLÉMŮ

Pro pomoc při řešení potíží, které mohou vzniknout s SMTA, je zde několik stránek. Základní informace se nacházejí na stránce Information Page. K vlastnímu řešení je stránka Diagnostics Page.

4.1 INFORMAČNÍ STRÁNKA

První částí v oddílu Status je informační stránka. Zde se nacházejí informace vztahující se k verzi hardwaru a softwaru, WAN a podobně. Údaje mohou být kdykoliv aktualizováni stisknutím tlačítka Refresh.



The screenshot shows the ASUS router's web interface. The top navigation bar includes 'Broadband', 'Status', 'Basic', 'Advanced', 'Firewall', and 'Voice'. The 'Status' tab is selected, and the 'Information' sub-tab is active. The main content area displays system information in a table format.

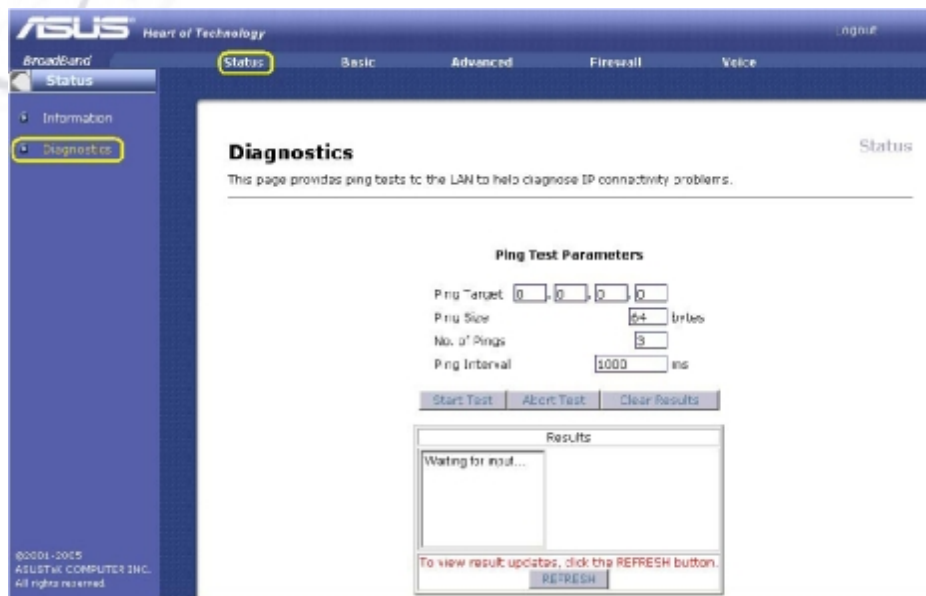
Standard Specification Compliant	VoIP Gateway
Hardware Version	1100(AVG602 REV:2.25)
Firmware Version	5.5.11(CO.C.0.0)
Build Time	Mar 23 2005,15:38:29
System Current Time	Thu Mar 24 01:52:22 2005
WAN MAC Address	00:1C:18:0F:AD:83
WAN Connection Type	DHCP Client
WAN IP Address	10.7.1.204
Voice Service	on-line

- **Standard Specification Compliant** – název zařízení
- **Hardware Version** – verze a typové číslo přístroje
- **Firmware Version** – aktuální verze firmwaru
- **Build Time** - datum vytvoření firmwaru
- **System Current Time** – aktuální systémový čas
- **WAN MAC Address** – MAC (Media Access Control) adresa WAN portu; jedinečné číslo identifikující každé zařízení

- WAN Connection Type – typ protokolu (DHCP klient, statická IP nebo PPPoE) právě používaného pro vnější spojení WAN.
- WAN IP Address - aktuální IP adresa WAN.
- Voice Service – status (online nebo offline) SMTA.

4.2 DIAGNOSTICKÁ STRÁNKA

Diagnostická stránka pomáhá hledat příčiny problémů s IP připojením pomocí testu „ping“.



ASUS Heart of Technology ngnif

BroadBand **Status** Basic Advanced Firewall Voice

Information **Diagnostics**

Diagnositics

This page provides ping tests to the LAN to help diagnose IP connectivity problems.

Ping Test Parameters

Ping Target:

Ping Size: bytes

No. of Pings:

Ping Interval: ms

Results

Waiting for input...

To view result updates, click the REFRESH button.

©2001-2005 ASUSTEK COMPUTER INC. All rights reserved.

V případě, že budete při řešení problému s WAN připojením potřebovat pomoc technického pracovníka, tento test může být pro něj užitečný. K počítačům jak na straně vnější WAN, tak na vnitřní LAN je možno se „dopingat“.

- Ping Target (Ping cíl) – Zadejte IP adresu síťového zařízení, s nímž chcete prověřit spojení.
- Ping Size – velikost jednotlivých paketů použitých pro ping test.

- **No. of Pings** – počet pokusů v každém testu.
- **Ping Interval** – interval mezi jednotlivými pingu v milisekundách (1000 ms = sec)

***Poznámka:** Pro zobrazení všech výsledků testu v okně stiskněte tlačítko Refresh.*

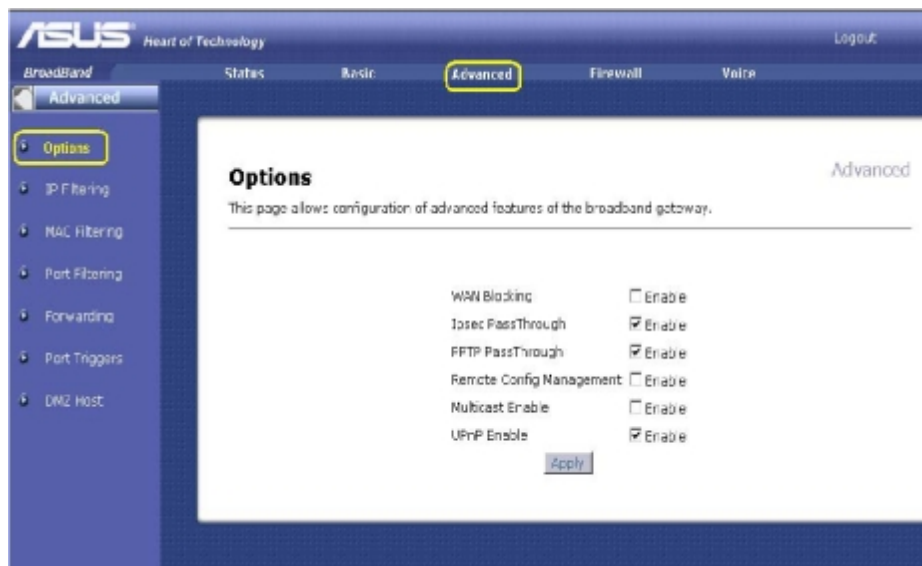
5 ADVANCED – KONFIGURACE PRO POKROČILÉ

Router SMTA podporuje mnoho pokročilých funkcí; jsou dokumentovány v této části a obsahují:

1. Volitelné blokování WAN, průchod IpSec, průchod PPTP, vzdálenou správu, zapnutí módů multicast a UPnP (univerzální plug and play)
2. Filtrování LAN IP adresy, MAC adresy a čísla portu
3. Přesměrování z WAN do LAN portu a triggerů (spouštěče).
4. DMZ hosting

5.1 VOLITELNÉ MÓDY

SMTA je možno provozovat v různých módech, které si liší způsobem směrování IP provozu. Nastavení je přístupné z Advanced Menu na stránce Options.



The screenshot shows the ASUS SMTA web interface. At the top, the ASUS logo and 'Heart of Technology' are visible. The navigation bar includes 'Broadband', 'Status', 'Basic', 'Advanced' (highlighted with a yellow box), 'Firewall', and 'Voice'. A 'Logout' link is in the top right. The left sidebar shows 'Advanced' selected, with 'Options' highlighted. The main content area is titled 'Options' and contains the following configuration options:

WAN Blocking	<input type="checkbox"/> Enable
Ipsec PassThrough	<input checked="" type="checkbox"/> Enable
PPTP PassThrough	<input checked="" type="checkbox"/> Enable
Remote Config Management	<input type="checkbox"/> Enable
Multicast Enable	<input type="checkbox"/> Enable
UPnP Enable	<input checked="" type="checkbox"/> Enable

An 'Apply' button is located at the bottom of the configuration options.

Pro aktivaci požadované funkce zaškrtněte příslušný čtvereček. Změnu nastavení odešlete tlačítkem **Apply**. Tyto funkce lze aktivovat bez resetování systému.

- **WAN Blocking** (blokování WAN) způsobuje, že SMTA ani počítače za ním nejsou ze strany WAN viditelné. Například ping testy na WAN IP adresu SMTA nebo na adresu počítačů na straně LAN zůstanou bez odezvy. Pro hackery je těžší objevit Vaši WAN IP adresu a napadnout LAN.
- **IPsec/PPTP (Point-to-Point Tunneling Protocol) Pass Through** mód umožňuje těmto protokolům procházet přímo přes SMTA, takže zařízení nebo software VPN (Virtual Private Network) může komunikovat přímo s WAN.
- **Remote Configuration Management (Vzdálená správa)** dovoluje, aby SMTA byl spravován (nastavován) přes WAN z libovolného místa na internetu.
- **Multicast Enable (Umožnit skupinové vysílání)** dovoluje multicast provozu (označenému speciální multicast specifickou adresou) procházet z/do počítačů privátní sítě za SMTA.
- **UPnP Enable (Universal Plug-and-Play)** umožňuje počítačům za SMTA ovládat SMTA jako NAT –Traversal zařízení.

5.2 LAN IP ADRESA, MAC ADRESA A FILTROVÁNÍ PORTŮ

SMTA může být konfigurován tak, aby určitým počítačům nedovolil v místní síti přístup k WAN určením IP adres, které mají být filtrovány. Ty mohou být nastaveny na stránce IP Filtering Page v Advanced Menu (viz obrázek níže).

ASUS Heart of Technology Logout

Broadband Status Basic **Advanced** Firewall Voice

Advanced

- Options
- IP Filtering**
- MAC Filtering
- Port Filtering
- Forwarding
- Port Triggers
- DMZ Host

IP Filtering Advanced

This page allows you to configure IP address filters in order to block internet traffic to specific network devices on the LAN.

IP Filtering		
Start Address	End Address	Enabled
192.168.15.0	192.168.15.0	<input type="checkbox"/>
192.168.15.0	192.168.15.0	<input type="checkbox"/>
192.168.15.0	192.168.15.0	<input type="checkbox"/>
192.168.15.0	192.168.15.0	<input type="checkbox"/>
192.168.15.0	192.168.15.0	<input type="checkbox"/>
192.168.15.0	192.168.15.0	<input type="checkbox"/>
192.168.15.0	192.168.15.0	<input type="checkbox"/>
192.168.15.0	192.168.15.0	<input type="checkbox"/>
192.168.15.0	192.168.15.0	<input type="checkbox"/>
192.168.15.0	192.168.15.0	<input type="checkbox"/>

©2001-2005
ASUSTeK COMPUTER INC.
All rights reserved.

Zadáním počáteční a konečné hodnoty rozsahu filtrovaných IP adres můžete určit, kterým místním počítačům bude odepřen přístup k WAN. Všimněte si, že stačí zadat pouze LSB (nejnižší byte) IP adresy. Vyšší byty jsou automaticky převzaty z IP adresy SMTA. Pro celkovou aktivaci funkce filtrování je ještě třeba zaškrtnout okénko „enable“ a kliknout na tlačítko Apply. Zrušením položky Enable funkci filtrování vypnete, nastavení rozsahu adres však bude zachováno.

Počítače lokální sítě, kterým chcete zabránit v zasilání odchozího provozu do WAN , můžete také specifikovat prostřednictvím MAC adresy. Toto se nastavuje na stránce MAC Filtering Page, viz obrázek níže.

ASUS Heart of Technology Logout

Broadband Status Basic **Advanced** Firewall Voice

Advanced

- Options
- IP Filtering
- MAC Filtering**
- Port Filtering
- Forwarding
- Port Triggers
- DWZ Host

MAC Filtering Advanced

This page allows you to configure MAC address filters in order to block internet traffic to specific network devices on the LAN.

MAC Address Filters												
MAC 01	00	00	00	00	00	00	MAC 02	00	00	00	00	00
MAC 03	00	00	00	00	00	00	MAC 04	00	00	00	00	00
MAC 05	00	00	00	00	00	00	MAC 05	00	00	00	00	00
MAC 07	00	00	00	00	00	00	MAC 08	00	00	00	00	00
MAC 09	00	00	00	00	00	00	MAC 10	00	00	00	00	00
MAC 11	00	00	00	00	00	00	MAC 12	00	00	00	00	00
MAC 13	00	00	00	00	00	00	MAC 14	00	00	00	00	00
MAC 15	00	00	00	00	00	00	MAC 15	00	00	00	00	00
MAC 17	00	00	00	00	00	00	MAC 18	00	00	00	00	00
MAC 19	00	00	00	00	00	00	MAC 20	00	00	00	00	00

Apply

©2001-2005
ASUSTeK COMPUTER INC.
All rights reserved.

To je výhodné proto, že MAC adresu konkrétní síťové karty počítače není možno měnit, zatímco IP adresa může být přestavena, nebo přidělena DHCP serverem pokudé jinak.

Podobně můžete zabránit odchozímu provozu na určitých portech WAN. Nastavuje se na stránce Port Filtering Page, viz obrázek níže.

ASUS Heart of Technology Logout

BroadBand Status Basic Advanced Firewall Voice

Advanced

- CPU Fans
- IP Filtering
- MAC Filtering
- Port Filtering
- Forwarding
- Port Triggers
- DMZ Host

Port Filtering Advanced

This page allows you to configure port filters in order to block specific internet services to all network devices on the LAN.

Port Filtering			
Start Port	End Port	Protocol	Enabled
<input type="text" value="1"/>	<input type="text" value="85535"/>	Both	<input type="checkbox"/>
<input type="text" value="1"/>	<input type="text" value="85535"/>	Both	<input type="checkbox"/>
<input type="text" value="1"/>	<input type="text" value="85535"/>	Both	<input type="checkbox"/>
<input type="text" value="1"/>	<input type="text" value="85535"/>	Both	<input type="checkbox"/>
<input type="text" value="1"/>	<input type="text" value="85535"/>	Both	<input type="checkbox"/>
<input type="text" value="1"/>	<input type="text" value="85535"/>	Both	<input type="checkbox"/>
<input type="text" value="1"/>	<input type="text" value="85535"/>	Both	<input type="checkbox"/>
<input type="text" value="1"/>	<input type="text" value="85535"/>	Both	<input type="checkbox"/>
<input type="text" value="1"/>	<input type="text" value="85535"/>	Both	<input type="checkbox"/>
<input type="text" value="1"/>	<input type="text" value="85535"/>	Both	<input type="checkbox"/>

©2001-2002
ASUSTek COMPUTER INC.
All rights reserved.

Zadáním počáteční a konečné adresy portu určíte rozsah portů, které budou blokovány. Tyto porty budou zablokovány pro VŠECHNY počítače nezávisle na jejich IP nebo MAC adrese. Například chcete-li všem počítačům síť LAN zakázat přístup k HTTP stránkám (tj. zabránit surfování na internetu), zadejte počáteční adresu (Start Port) 80, konečnou adresu (End Port) také 80, v položce Protokol vyberte TCP, zaškrtněte Enabled a odešlete tlačítkem **Apply**.

5.3 PŘESMĚROVÁNÍ PORTŮ

Přesměrování dovoluje provozovat veřejně přístupné servery v síti LAN namapováním TCP/UDP portů na lokální PC. Stránka Forwarding page je zobrazena níže.

Forwarding Advanced

This page allows for incoming requests on specific port numbers to reach web servers, FTP servers, mail servers, etc. So they can be accessible from the public internet. A table of commonly used port numbers is also provided.

Port Forwarding				
Local IP Address	Start Port	End Port	Protocol	Enabled
192.168.15.0	0	0	Beth	<input type="checkbox"/>
192.168.15.0	0	0	Beth	<input type="checkbox"/>
192.168.15.0	0	0	Beth	<input type="checkbox"/>
192.168.15.0	0	0	Beth	<input type="checkbox"/>
192.168.15.0	0	0	Oct	<input type="checkbox"/>
192.168.15.0	0	0	Beth	<input type="checkbox"/>
192.168.15.0	0	0	Beth	<input type="checkbox"/>
192.168.15.0	0	0	Beth	<input type="checkbox"/>
192.168.15.0	0	0	Beth	<input type="checkbox"/>
192.168.15.0	0	0	Beth	<input type="checkbox"/>

Application	Port
HTTP	80
FTP	21
TFTP	69
SMTP	25
POP2	110
SMTP	110
telnet	23
IRC	194
SNMP	161
Fringer	70
Gopher	70
Whois	43
Remote	100
LDAP	389
UUCP	540

©2011 2015
ASUSTeK COMPUTER INC.
All rights reserved.

Pro správné namapování je třeba zadat rozsah čísel portů, které mají být lokálně přesměrovány, a IP adresu, na niž má být provoz přicházející na tyto porty přesměrován. Pokud je třeba pouze jedna adresa portu, zadejte počáteční (start) i konečnou (end) adresu stejnou. Pro rychlou orientaci se na stránce nachází také tabulka obecně používaných adres portů.

5.4 TRIGGERY

Funkce portů-triggerů je podobná funkci přesměrování portů až na to, že to nejsou statické porty nepřetržitě otevřené. Jestliže SMTA zjistí odchozí data směřující na konkrétní port, jehož číslo a IP jsou nastaveny v „Trigger Range“, port nastavený v „Target Range“ je otevřen pro příchozí provoz. Jestliže se příchozí data do 10 minut neobjeví, tento cílový port definovaný v „Target Range“ se uzavře. Tato metoda otevírání určitých portů pro speciální aplikace (například videokonference, síťové hry, přenos souborů v chatovacích programech atd.) je bezpečnější, protože otevírání je dynamicky spouštěno (triggered) a porty nezůstávají nepřetržitě nebo chybně otevřeny a vystaveny tak potenciálním útokům hackerů.

ASUS Heart of Technology Logout

Broadband Status Basic **Advanced** Firewall Voice

Advanced

- Options
- IP Filtering
- MAC Filtering
- Port Filtering
- Forwarding
- Port Triggers**
- DMZ Host

Port Triggers Advanced

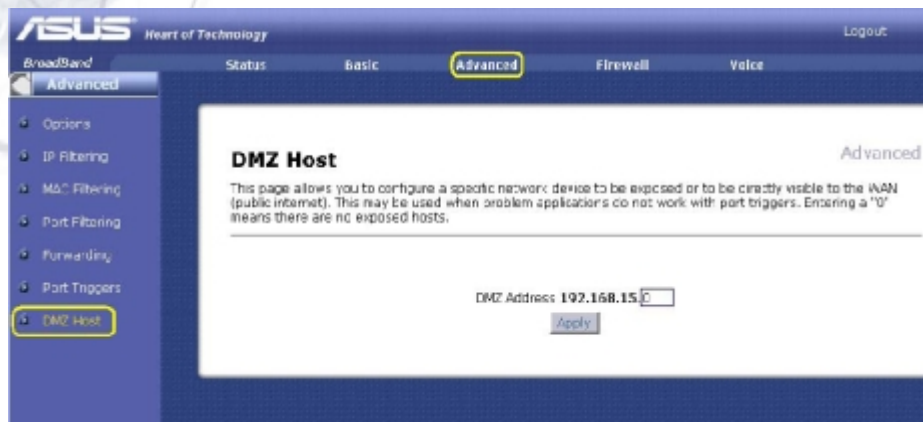
This page allows you to configure dynamic triggers to specific devices on the LAN. This allows special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging programs may require these special settings.

Port Triggering					
Trigger Range		Target Range		Protocol	Enable
Start Port	End Port	Start Port	End Port		
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Beth	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Beth	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Beth	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Beth	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Beth	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Beth	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Beth	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Beth	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Beth	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Beth	<input type="checkbox"/>
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	Beth	<input type="checkbox"/>

©2001-2005
ASUSTeK COMPUTER INC.
All rights reserved.

5.5 DMZ HOSTING

DMZ (De-militarized Zone) hosting (obvykle také nazýváno „Exposed Host“ – odkrytý host) je implicitní (default) příjemce toho příchozího WAN provozu, který NAT nedokáže přeložit na známé místní PC. DMZ může být také popsána jako počítač nebo malá podsíť, která se nachází mezi důvěryhodnou privátní LAN sítí a nedůvěryhodným veřejným internetem. Stránka DMZ Host page je zobrazena níže.



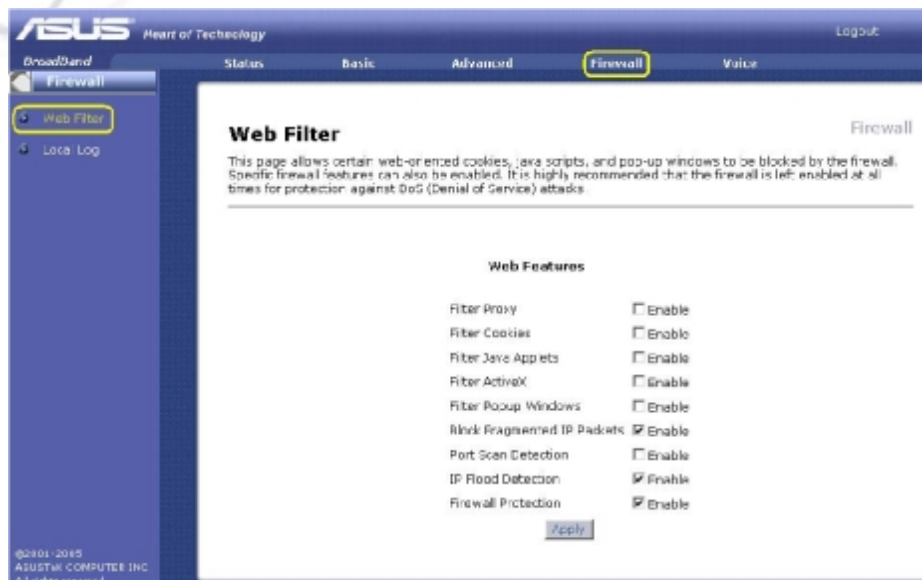
Můžete konfigurovat jedno PC jako DMZ host. To se hodí, jestliže PC používá „problémové“ aplikace, které při komunikaci používají náhodná čísla portů a neumí pracovat s porty-triggery nebo přesměrováním portů, jak bylo zmíněno v předchozí kapitole. Jestliže je některé PC specifikované jako DMZ Host, nezapomeňte po ukončení práce s příslušnou aplikací nastavit podadresu DMZ zpět na nulu, jinak by PC zůstalo zcela odkryto veřejnému internetu, i když stále chráněno firewallem proti útokům DoS (Denial of Service).

6 KONFIGURACE FIREWALLU

SMTA obsahuje vloženou aplikaci firewallu k ochraně soukromé LAN sítě před zlomyslnými útoky (DoS apod.) ze strany WAN interface.

6.1 WEB FILTR

Stránka Web filtru obsahuje různá nastavení týkající se blokování nebo výjimečného povolení průchodu dat z WAN do LAN. Firewall je možno vypnout nebo zapnout prostřednictvím zaškrťovacího okénka Enable.



- **Blokování Proxies, Cookies, Java Applets, ActiveX controls a Popup Windows.**
- **Block Fragmentes IP Packets** – blokování neúplných IP paketů
- **Port Scan Detection** – detekuje a blokuje pokusy o scanování portů, které mají původ jak z WAN, tak z LAN.

- **IP Flood Detection** – detekuje a blokuje záplavů packetů pocházející jak z LAN, tak z WAN. Pro aktivaci vybraných položek je třeba kliknout na tlačítko Apply. Všechna tato nastavení mohou být rychle aktivována bez rebootování SMTA.
- **Firewall Protection** - zapne funkce SPI (Stateful Packet Inspection – kontrola jednotlivých TCP/IP packetů).

6.2 LOCAL EVENT LOG– ZÁZNAM LOKÁLNÍCH UDÁLOSTÍ

Stránka Local Log zasílá zprávy o útocích na firewall dvěma způsoby. Jednak může po každém útoku zaslat samostatný email, a také zůstávají uloženy záznamy události (local log) v modemu a jsou zobrazeny na stránce Local Log ve formě tabulky.

The screenshot shows the ASUS Firewall configuration interface. The 'Local Log' section is active, displaying configuration options for email alerts and a table of local log events.

Local Log Configuration:

- Contact Email Address:
- SMTP Server Name:
- Sender Email Address:
- SMTP Server Authentication: Enable
- Email Alerts: Enable
- Apply:

Local Log Table:

Description	Count	Last Occurrence	Target	Source
IP Fragmented Packet	30	Mon Mar 21 14:16:25 2005	172.22.252.22:0	192.168.15.88:0

Buttons:

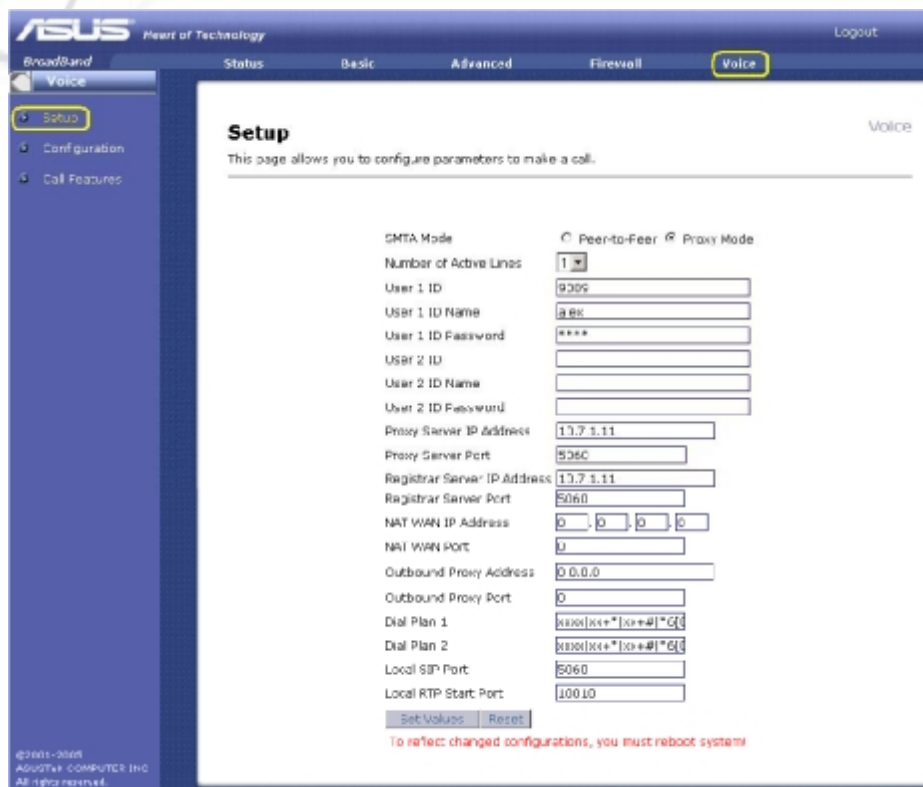
Pro zapnutí automatického varování emailem zadejte svou emailovou adresu, dále adresu emailového serveru, který tento účet spravuje (provozovaný Vaším poskytovatelem), zaškrtněte políčko „enable“ a klikněte na tlačítko **Apply**. Nyní bude po každém zaregistrovaném pokusu o útok zaslána samostatná zpráva. Každý útok je také zaznamenán do tabulky na stránce Event Log. V případě potřeby může být kliknutím na tlačítko Email Log zaslán celý obsah tabulky Event Log Table najednou. Obsah tabulky vymažete tlačítkem Clear Log.

7 NASTAVENÍ HLASOVÝCH SLUŽEB

ASUS VP100 (SMTA) obsahuje aplikaci VoIP, která pracuje na SIP protokolu (telefonie přes internet). Tato část pokrývá SIP účet uživatele, proxy server, registrační server a nastavení DSP (digitální zpracování signálu)

7.1 SETUP - NASTAVENÍ

Následuje stránka hlasového nastavení.



ASUS Heart of Technology Logout

BroadBand **Voice** Status Basic Advanced Firewall

Setup Configuration Call Features

Setup

This page allows you to configure parameters to make a call.

SMTA Mode Peer-to-Peer Proxy Mode

Number of Active Lines

User 1 ID

User 1 ID Name

User 1 ID Password

User 2 ID

User 2 ID Name

User 2 ID Password

Proxy Server IP Address

Proxy Server Port

Registrar Server IP Address

Registrar Server Port

NAT WAN IP Address

NAT WAN PORT

Outbound Proxy Address

Outbound Proxy Port

Dial Plan 1

Dial Plan 2

Local SIP Port

Local RTP Start Port

To reflect changed configurations, you must reboot system!

©2005-2008 ASUSOTEK COMPUTER INC. All rights reserved.

- **SMTA Mode: Peer-to-Peer: Mód Peer-to-Peer (rovný s rovným)** nevyžaduje žádné další nastavování. Pouze klikněte na tlačítko.
- **Proxy Mode:** Při použití proxy módu je třeba nastavit následující parametry:
 1. **Number of Active Lines** – počet používaných linek nebo portů.
 2. **User 1 ID** – číslo telefonu
 3. **User 1 ID Name** – jméno, které se při odchozím hovoru objeví na straně volaného.
 4. **User 1 Password** – heslo pro uživatele 1
 5. **User 2 ID / Name / Password** – vyplňte pouze pokud používáte druhou telefonní linku.
 6. **Proxy Server IP Address** – zadejte adresu proxy serveru, kterou máte od svého VoIP poskytovatele; jestliže proxy server není požadován, zadejte 0.0.0.0.
 7. **Proxy Server Port** – nepovinný údaj; pokud jste číslo portu obdrželi od svého poskytovatele, zadejte ho zde.
 8. **Registrar Server IP Address** – pokud není registrář požadován, zadejte 0.0.0.0. Registrováním umožníte ostatním, aby viděli vaše informace.
 9. **Registrar Server Port** – nepovinný údaj.
 10. **Outbound Proxy Address / Port** – adresu a port odchozího proxy serveru dostanete od svého poskytovatele.
 11. **Dial Plan 1 / 2** – volba ze dvou vytáčekých plánů
 12. **Local SIP Port** – obvyklé číslo SIP portu je 5060, záleží však na Vašem poskytovateli.
 13. **Local RTP Start Port** – počáteční hodnota portu, obvykle číslo v rozsahu deseti tisíc.
 14. Po ukončení nastavení klikněte na **Set Values**.

Poznámka: Aby odeslané změny vstoupily v platnost, je třeba rebootovat zařízení.

7.2 KONFIGURACE

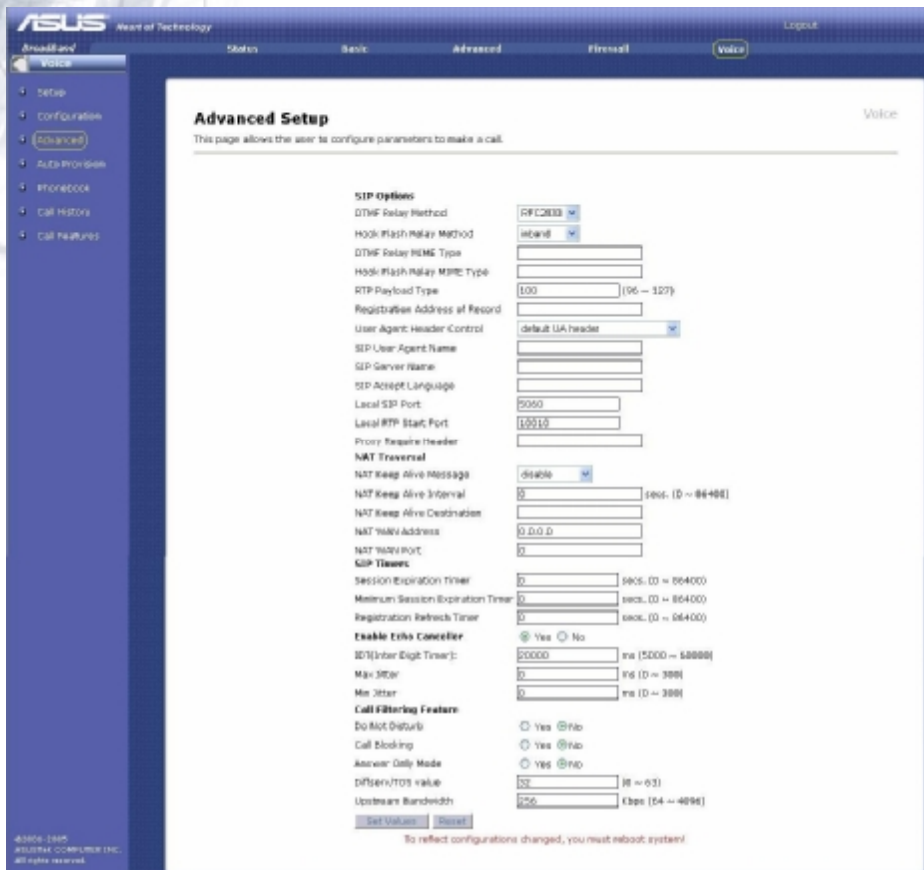
Na této stránce je možno nastavovat způsob odesílání a příjmu hlasové aktivity.



- **Prefer Voice Encoder** – vyberte hlasový kodek, kterému dáváte přednost. Neznamená to, že bude skutečně použit, při výběru typu kódování hlasu však bude brán v potaz. Kodeky se od sebe liší zejména stupněm komprimace hlasu.
- **Packetization Period** – jak často by měly být pakety odesílány (údaj je v mikrosekundách). Může tak snížit nebo zvýšit časový interval mezi jednotlivými odesílanými pakety.
- **Voice Activity Detection** – zvolením můžete snížit objem přenášených dat – když nehovoříte, žádná data nebudou odesílána.
- **Fax / Modem** – volba *None* (žádný) znamená, že kodek nebude nastavován automaticky, což může způsobit, že nepůjde odesílat faxové zprávy. *Voice Band Data* znamená, že kodek se nastaví tak, aby faxy byly správně přenášeny. Volba *T.38* znamená, že odesílané faxy nebudou ovlivněny nastaveným hlasovým kodekem; *T.38* je speciální kodek pro posílání faxů. Při používání faxů se většinou volí *Voice Band Data*.
- **Line Transmit Gain (db)** – zesílení odesílaného hlasu v decibelech (zeslabení je jako záporné číslo, 0 = beze změny)
- **Line Receive Gain (db)** – zesílení přijímaného hlasu v decibelech (zeslabení je jako záporné číslo, 0 = beze změny)

7.3 ADVANCED – KONFIGURACE PRO PORKOČILÉ

Tato stránka umožňuje uživateli nakonfigurovat parametry k uskutečnění hovorů.



The screenshot shows the 'Advanced Setup' page for a device, specifically the 'VOICE' section. The page title is 'Advanced Setup' and it includes a sub-header 'Voice'. Below the title, there is a description: 'This page allows the user to configure parameters to make a call.' The configuration is organized into several sections:

- SIP Options:**
 - DTMF Relay Method: DFC233
 - Hook Flash Relay Method: instant
 - DTMF Relay MIME Type: [empty]
 - Hook Flash Relay MIME Type: [empty]
 - RTP Payload Type: 100 (106 – 127)
 - Registration Address of Record: [empty]
 - User Agent Header Control: default UA header
 - SIP User Agent Name: [empty]
 - SIP Server Name: [empty]
 - SIP Accept Language: [empty]
 - Local SIP Port: 5050
 - Local RTP Start Port: 10010
 - Proxy Require Header: [empty]
- NAT Traversal:**
 - NAT Keep Alive Message: disable
 - NAT Keep Alive Interval: 0 secs. (0 ~ 64000)
 - NAT Keep Alive Destination: [empty]
 - NAT NATV Address: 0.0.0.0
 - NAT NATV Port: 0
- Session Expiration Timer:**
 - Session Expiration Timer: 0 secs. (0 ~ 64000)
 - Minimum Session Expiration Timer: 0 secs. (0 ~ 64000)
 - Registration Refresh Timer: 0 secs. (0 ~ 64000)
- Enable Echo Canceller:**
 - Enable Echo Canceller: Yes (selected) / No
 - IS[Inter-Digit Timer]: 20000 ms (5000 ~ 60000)
 - Max SREAR: 0 % (0 ~ 300)
 - Min Jitter: 0 ms (0 ~ 300)
- Call Filtering Feature:**
 - Do Not Disturb: Yes (selected) / No
 - Call Blocking: Yes (selected) / No
 - Answer Delay Mode: Yes (selected) / No
 - DIFSRV/TOS Value: 52 % (0 ~ 63)
 - Upstream Bandwidth: 256 kbps (64 ~ 4096)

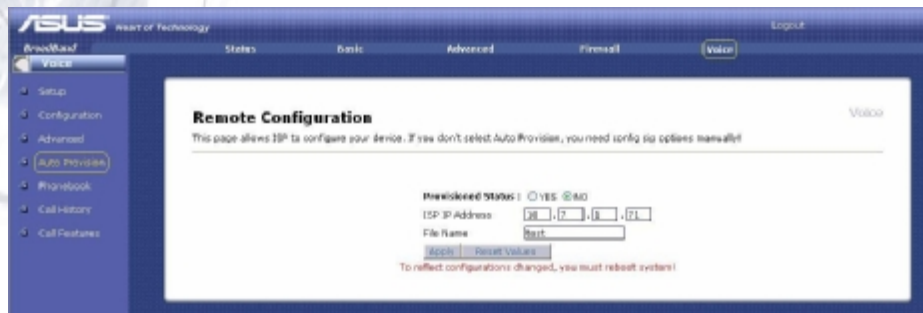
At the bottom of the configuration area, there are buttons for 'Set Values' and 'Reset'. A note at the bottom states: 'To reflect configurations changed, you must reboot system!'.

- **SIP Timers** – časovače lhůty vypršení platnosti registrace a interval re-registrace.
- **Session Expiration Timer** (v mikrosekundách) – max. délka trvání spojení

- **Minimum Session Expiration Timer** – nejkratší dovolená délka trvání spojení.
- **Registration Refresh Timer** (v mikrosekundách) – časový interval, po jehož uplynutí bude požadováno obnovení registrace.
- **Enable Echo Cancellor** – zapnutím se zruší efekt echa v hovoru.
- **IDT (Inter Digit Timer)** – maximální povolená doba mezi jednotlivými vytáčenými číslicemi; pokud se další číslice opozdí, zadaná posloupnost bude zrušena a ozve se obsazovací tón.
- **Max / Min Jitter** – maximální / minimální doba, po kterou je přichodící paket držen ve vyrovnávací paměti (bufferu), než je převeden na zvuk. Pokud je zadána nula, systém použije svoji výchozí hodnotu.
- **Enable RTP DTMF Relay** – zapnutím DTMF a určením typu užitečného zatížení (payload) je možno DTMF tóny posílat ve speciálním protokolu RTP (real-time transport protocol).
- **RTP Payload Type** – pracuje s RTP DTMF Relay.
- **Do Not Disturb (Nerušit)** – blokuje přichodící hovory. Volající uslyší obsazovací tón.
- **Call Blocking** – blokuje přichodící hovory z čísel uvedených v seznamu blokovanych čísel.
- **Answer Only Mode (Pouze odpovědět)** – tento mód je užitečný v případě Vaší dlouhodobé nepřítomnosti, kdy nechcete, aby se Vám na záznamníku hromadily zprávy. Volající uslyší předem nahrané oznámení a spojení bude přerušeno. Volající nemůže zanechat zprávu.
- **Diffserv/ToS Value** – hodnota přiřazená k hlasovým datům, vyjadřující jejich naléhavost, takže routovací síť může s nimi zacházet jinak, než s ostatními daty. Čím je tato hodnota větší, tím větší důležitost budou hlasová data při průchodu sítí mít.
- **Upstream Bandwidth** – šířka pásma v kbps (kilobitech za sekundu) odchozích aktivit, jako jsou odchozí hovory nebo zasílání dat. Zadejte maximální šířku pásma. V okamžicích, kdy neprobíhá žádný hovor, je celé pásmo k dispozici pro internet.

7.4 AUTO PROVISION – AUTOMATICKÁ KONFIGURACE

Tato stránka umožňuje poskytovateli VoIP služeb (ISP) nakonfigurovat Vaše zařízení. Pokud si ne zvolíte Auto Provision musíte nastavit ASUS VP100 (SMTA) manuálně. Tuto službu musí podporovat ISP.



The screenshot shows the ASUS VP100 web interface. The top navigation bar includes 'ASUS' and 'VoIP'. The left sidebar lists menu items: 'Setup', 'Configuration', 'Advanced', 'Auto Provision', 'Handbook', 'Call History', and 'Call Features'. The 'Auto Provision' item is highlighted. The main content area is titled 'Remote Configuration' and contains the following text and form elements:

Remote Configuration VoIP

This page allows ISP to configure your device. If you don't select Auto Provision, you need config sip options manually!

Provisioned Status: YES NO

ISP IP Address:

File Name:

To reflect configurations changed, you must reboot system!

7.5 PHONEBOOK – TELEFONNÍ SEZNAM

Tato stránka Vám nabízí možnosti vytvoření až 10 rychlých vytáčení (speed dials) od *00 do *09.

U telefonní čísel uložených v telefonním seznamu si můžete nastavit podle volajícího volání. Dále můžete zablokovat některé příchozí hovory.

ASUS Wear of Technology Logout

Advanced **Phonebook** Status Basic Advanced Overall **Extra**

Phonebook Voice

This page gives you the option of creating up to 10 speed dial from *00 to *09. You can make your phone ring differently based on the caller with Ring Group feature. You can block an inbound call with the specific blocking checked, and to make it work you must enable Call Blocking first.

Index	Call ID	Ring Group	Blocking
00	<input type="text"/>	default	<input type="checkbox"/>
01	<input type="text"/>	default	<input type="checkbox"/>
02	<input type="text"/>	default	<input type="checkbox"/>
03	<input type="text"/>	default	<input type="checkbox"/>
04	<input type="text"/>	default	<input type="checkbox"/>
05	<input type="text"/>	default	<input type="checkbox"/>
06	<input type="text"/>	default	<input type="checkbox"/>
07	<input type="text"/>	default	<input type="checkbox"/>
08	<input type="text"/>	default	<input type="checkbox"/>
09	<input type="text"/>	default	<input type="checkbox"/>
10	<input type="text"/>	default	<input type="checkbox"/>
11	<input type="text"/>	default	<input type="checkbox"/>
12	<input type="text"/>	default	<input type="checkbox"/>
13	<input type="text"/>	default	<input type="checkbox"/>
14	<input type="text"/>	default	<input type="checkbox"/>
15	<input type="text"/>	default	<input type="checkbox"/>
16	<input type="text"/>	default	<input type="checkbox"/>
17	<input type="text"/>	default	<input type="checkbox"/>
18	<input type="text"/>	default	<input type="checkbox"/>
19	<input type="text"/>	default	<input type="checkbox"/>

©2001-2008
ASUSTEK COMPUTER INC.
All rights reserved.

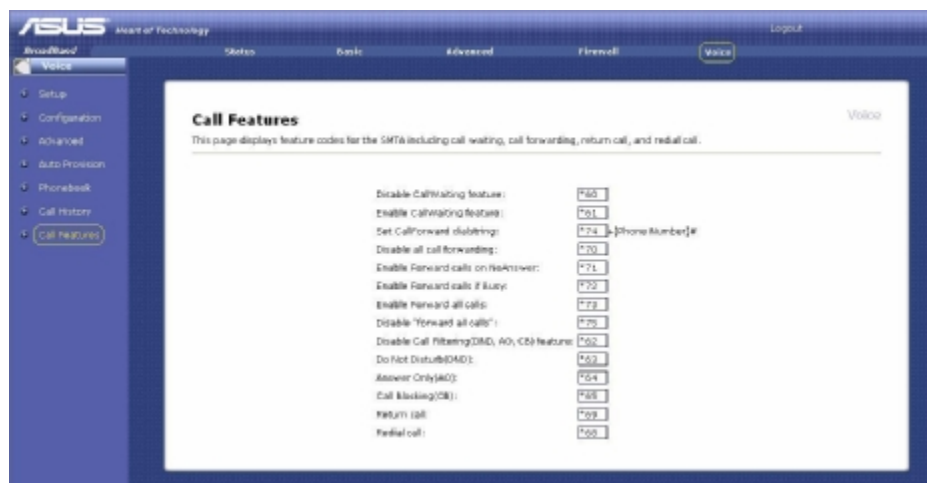
7.6 CALL HISTORY

Tato stránka zobrazuje posledních 20 příchozích a odchozích hovorů.



7.7 CALL FEATURES

Na této stránce je seznam kódů pro jednotlivé funkce jako je čekající hovor, přeměrování, opakované vytáčení apod.



Funkce	Popis	Kód z klávesnice telefonu
Čekající hovor (Call Waiting)	Máte-li právě probíhající hovor a někdo další se Vám snaží dovolat, budete na tento druhý příchozí hovor upozorněni pípnutím; potom můžete první hovor podržet a druhý vyřídit	Vypnutí – vytočte à 60 Zapnutí – vytočte à 61
Nastavit číslo pro přeměrování	Umožňuje vložit číslo, na které budou přeměrovány příchozí hovory	Vytočte à 74 a telefonní číslo, na které mají být hovory přeměrovány; toto je pouze vložení čísla, nikoliv zapnutí funkce Zrušit VŠECHNA přeměrování – vytočte à 70
Přeměrovat, jestliže není odpověď	Přeměruje příchozí hovory, které nebudou zvednuty, na zvolené číslo	Pro zapnutí navolte à 71
Přeměrovat, pokud je obsazeno	Přeměruje příchozí hovory na zvolené číslo, pokud bude právě obsazeno	Pro zapnutí navolte à 72
Přeměrovat všechny hovory	Přeměruje VŠECHNY příchozí hovory (pokud nejsou zvednuty nebo je obsazeno) na zvolené číslo	Zapnutí – vytočte à 73 Vypnutí – vytočte à 75
Zpětné volání (Call Back)	Poslech čísla posledního příchozího hovoru	Pro poslech čísla navolte à 69
Poslední volané číslo (Redial)	Volání na posledně vytočené číslo	Pro vytočení posledního čísla navolte à 68

Výhradní dovozce VoIP zařízení ASUS a WELL pro ČR a SR:

JOYCE ČR, s.r.o., Venhudova 6, 614 00 Brno

www.joyce.cz; e-mail: support@joyce.cz

**U PŘÍPADNÝCH DOTAZŮ NA TECHNICKOU PODPORU VŽDY UVÁDĚJTE:
TYP ZAŘÍZENÍ, SÉRIOVÉ ČÍSLO (S/N) A NÁZEV FIRMY, KDE JSTE ZAŘÍZENÍ
ZAKOUPILI.**

Žádná část této příručky nesmí být publikována, reprodukována, přenesena nebo upravena bez předchozího vědomí a písemného souhlasu firmy JOYCE ČR, s.r.o.

8 PROHLÁŠENÍ O SHODĚ

Declaration of Conformity

We, Manufacturer/Importer
(Full address)

ASUS COMPUTER GmbH
HARKORT STR. 25
40880 RATINGEN, BRD. GERMANY

declare that the product
(description of the apparatus, system, installation to which it refers)

ASUS
VP 100 series

is in conformity with

(reference to the specifications under which conformity is declared)
in accordance with 89/336 EEC-EMC Directive and 1999/5 EC-R & TTE Directive

- | | | | |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> EN 300328 | Electromagnetic compatibility and Radio spectrum Matters (ERM); wideband transmission equipment operating in the 2.4GHz ISM band and using spread spectrum modulation techniques; Part 1: technical characteristics and test conditions Part2: Harmonized EN covering essential requirements under article 3.2 of the R&TTE | <input checked="" type="checkbox"/> EN 55022 | Limits and methods of measurement of radio disturbance characteristics of information technology equipment |
| <input checked="" type="checkbox"/> EN 300386 | Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication equipment; ElectroMagnetic Compatibility (EMC) requirements | <input checked="" type="checkbox"/> EN 55024 | Information Technology equipment-Immunity characteristics-Limits and methods of measurement |
| <input type="checkbox"/> EN 301489 | Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 47: Specific conditions for wireless data and HPERLAN equipment | <input type="checkbox"/> EN 50360/EN 50361 | the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz) International Commission on Non-Ionizing Radiation Protection (1998), Guidelines for limiting exposure in time-varying electric, magnetic, and electromagnetic fields |
| <input type="checkbox"/> EN 301 511 | Global System for Mobile communications (GSM)-Harmonized EN for mobile stations in the GSM 900 and GSM 1800 bands covering essential requirements under article 3.2 of the R&TTE directive (2005/87/EC) Directive | <input type="checkbox"/> EN 61000-3-2* | Disturbances in supply systems caused |
| <input type="checkbox"/> EN 301639 | Broadband Radio Access Networks (BRAN); 5 GHz high performance WLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive | <input type="checkbox"/> EN 61000-3-3* | Disturbances in supply systems caused |
| <input checked="" type="checkbox"/> CE marking | | <input type="checkbox"/> EN 55013 | Limits and methods of measurement of radio disturbance characteristics of broadcast receivers and associated equipment |
| <input type="checkbox"/> EN 60065 | Safety requirements for mains operated electronic and related apparatus for household and similar general use | <input type="checkbox"/> EN 55020 | Immunity from radio interference of broadcast receivers and associated equipment |
| <input type="checkbox"/> EN 60335 | Safety of household and similar electrical appliances | <input type="checkbox"/> EN 50081-2 | Generic emission standard Part 2 Industrial environment |
| | | <input type="checkbox"/> EN 50082-2 | Generic immunity standard Part 2: Industrial environment |



(EC conformity marking)

The manufacturer also declares the conformity of above mentioned product with the actual required safety standards in accordance with LVD 73/23 EEC

- | | | | |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------|------------------------------------------------|-------------------------------------------------------------------------------------|
| <input type="checkbox"/> EN 60065 | Safety requirements for mains operated electronic and related apparatus for household and similar general use | <input checked="" type="checkbox"/> EN 60950-1 | Safety for information technology equipment including electrical business equipment |
| <input type="checkbox"/> EN 60335 | Safety of household and similar electrical appliances | <input type="checkbox"/> EN 50091-1 | General and Safety requirements for uninterruptible power systems (UPS) |

Manufacturer/Importer

(Date)

Date: MAR. 10, 2005

Signature :

Name : Jonathan Tseng