ASUS VP100

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

Uživatelská příručka

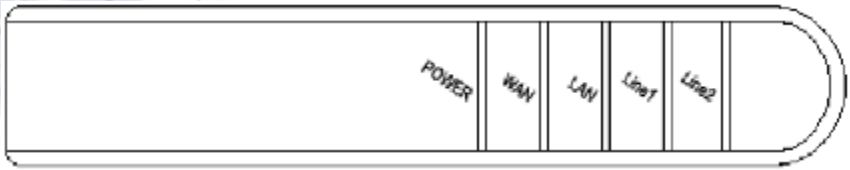
CE

OBSAH

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.

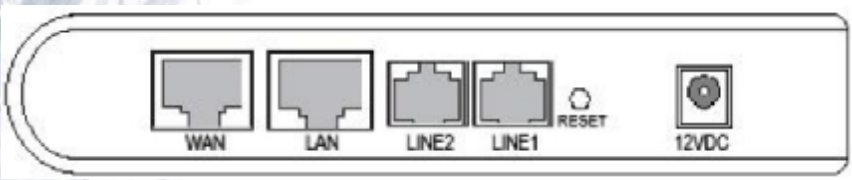
1.1 ČELNÍ PANEL ASUS VP100



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 PANEL 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 ehernetový 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 přepěťovou 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 dvěmi 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 sítě 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.)**

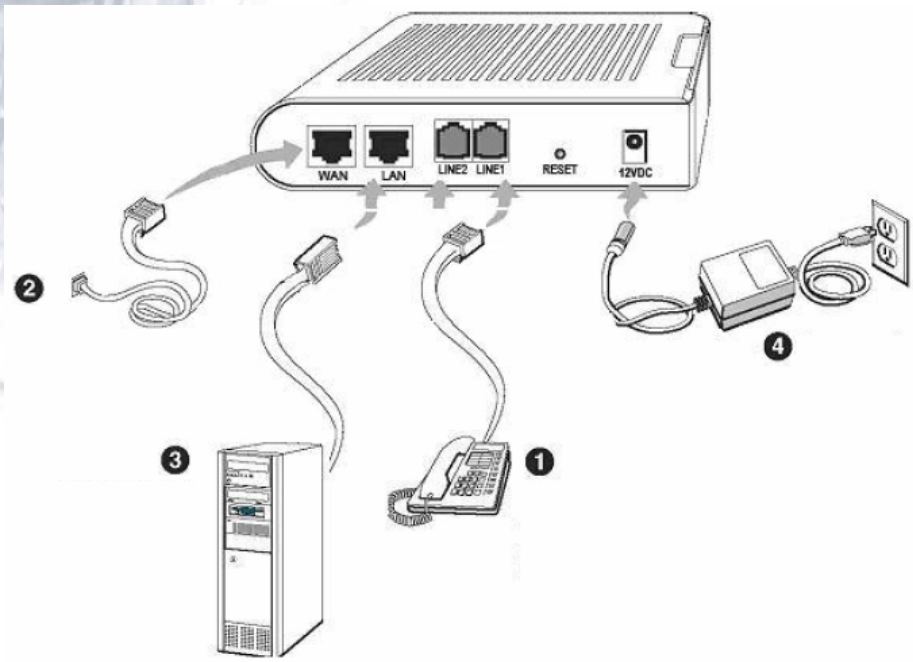
Nakonec připojte k SMTA jeho napájecí zdroj.

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 switche 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 Váše 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**

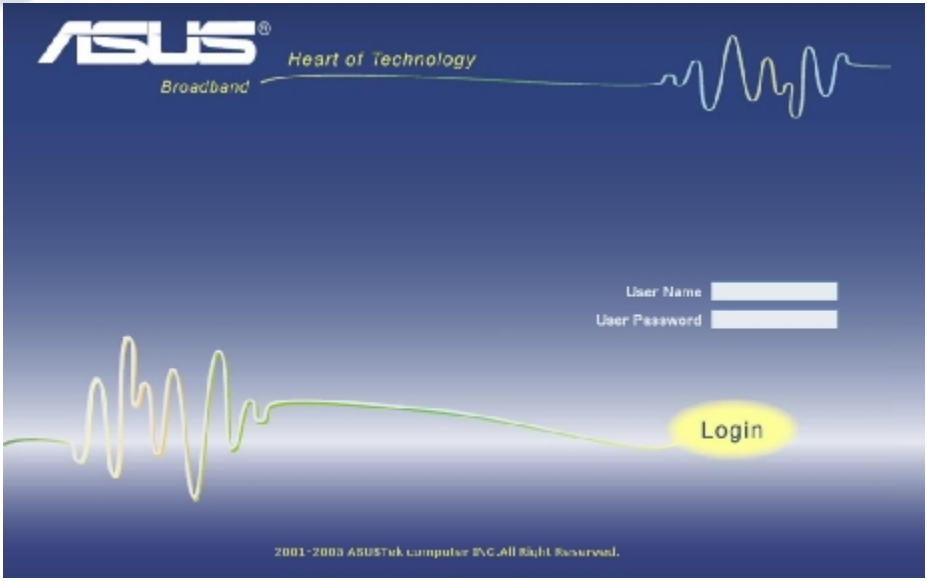
2. **Někteří poskytovatelé MOHOU požadovat následující informace:**
   - **MAC (Media Access Control) adresu připojeného zařízení**
   - **Hostname připojeného počítače**
   - **Název domény, kterou poskytovatel používá**

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:

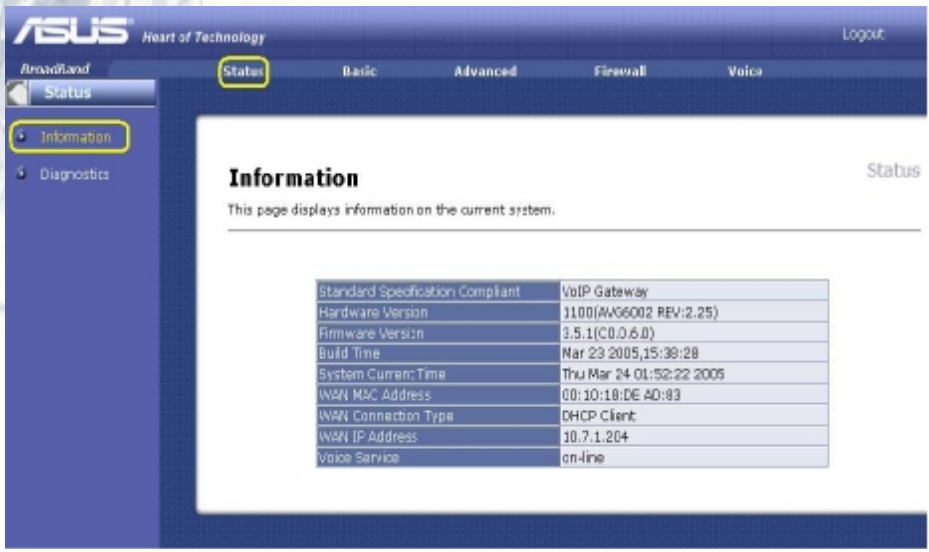
1. **Z vestavěného DHCP serveru získejte IP adresu připojeného počítače, ze kterého budete konfiguraci provádět**
2. **Spusťte web prohlížeč (Internet Explorer nebo Netscape atd.)**
3. **Do adresového řádku zadejte URL adresu http://192.168.15.1**

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.



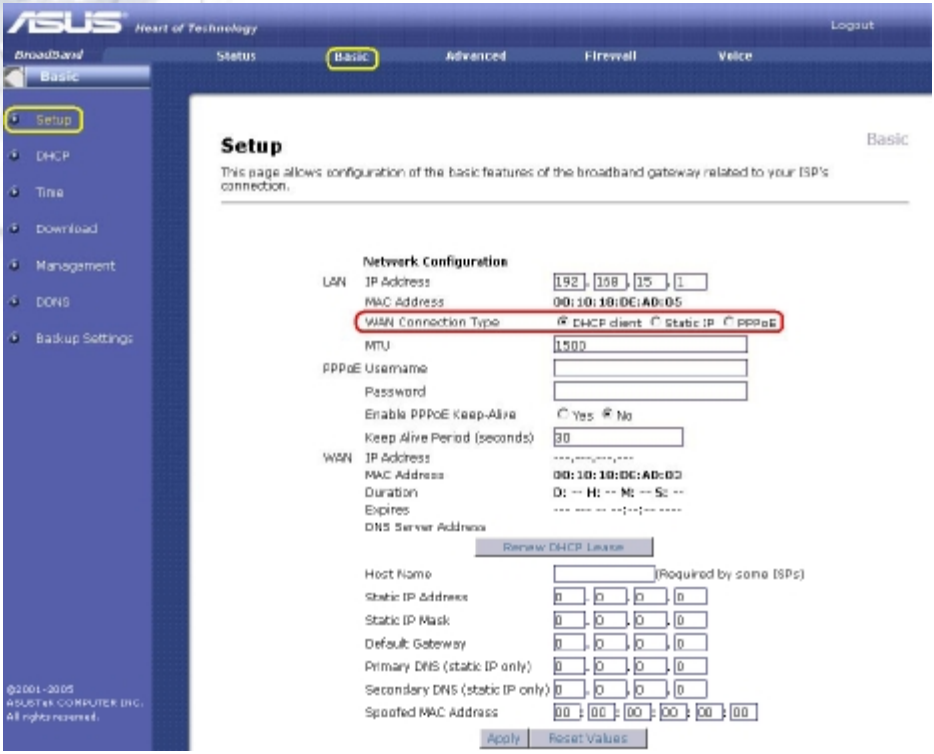
3.3 ZÁKLADNÍ NASTAVENÍ

Po přihlášení se zobrazí stránka aktuálního stavu systému (Status)



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*.



3.4.1 WAN – typ připojení DHCP klient

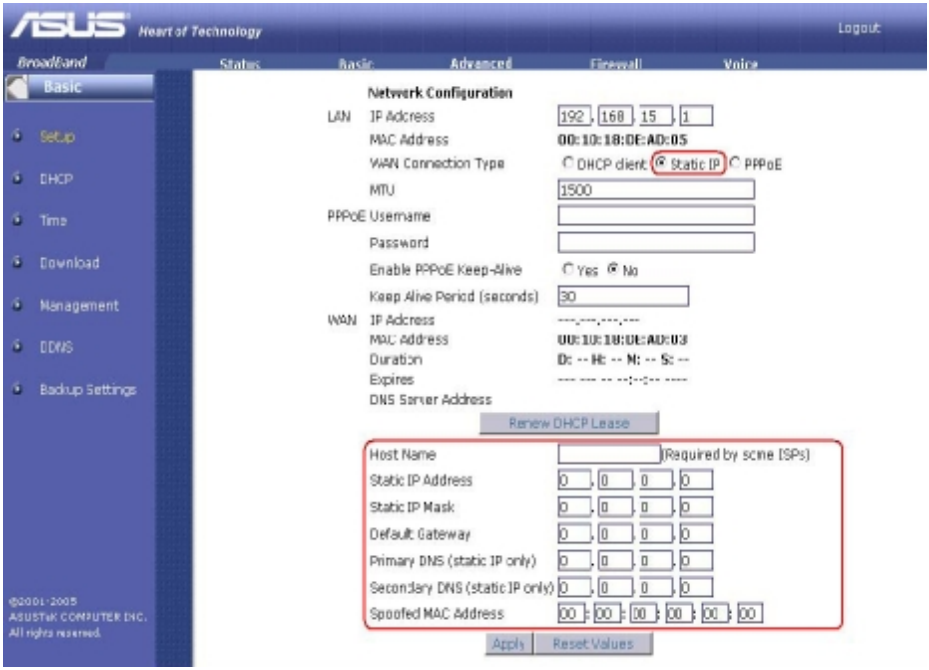
Pokud Váš poskytovatel používá DHCP, klikněte pouze na přepínací tlačítko *DHCP client* a pak na tlačítko Apply. Jestliže jste již dříve nakonfigurovali DHCP připojení a chcete pouze obnovit stávající pronájem adresy, klikněte na *Renew DHCP Lease*.

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.**

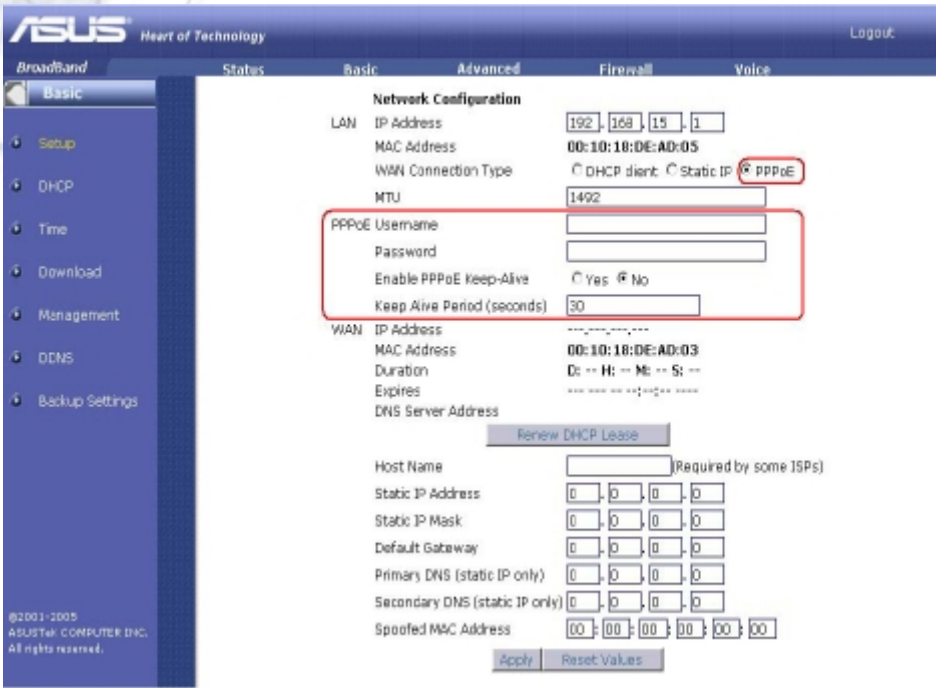
Po vyplnění potřebných políček stiskněte Apply, SMTA bude restartováno do vašeho nastavení.



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“, jetliže 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.**



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

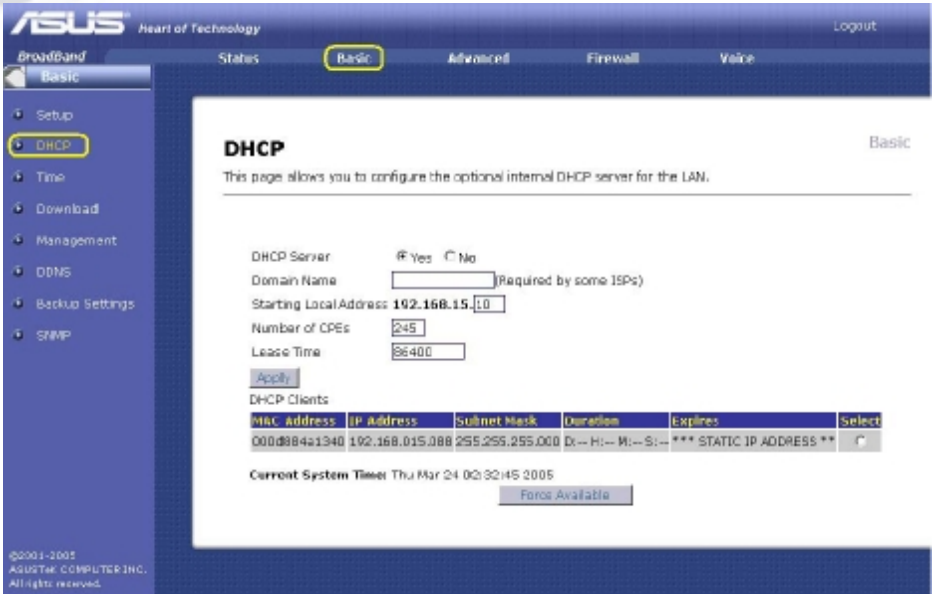
1. **Zapněte SMTA a počkejte, až se zaregistruje u poskytovatele a obdrží použitelnou IP adresu.**

2. **Pro každé PC připojené k LAN portu získejte 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.

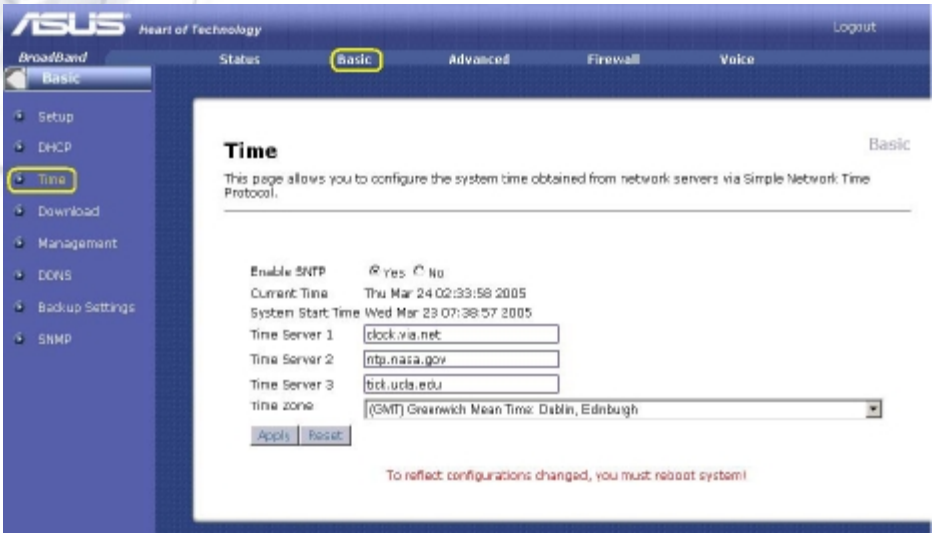


Pokud používáte na straně LAN vlastní DHCP server, můžete vnitřní DHCP server vypnout zvolením „no“. Pokud tak učiníte, zkontrolujte, zda LAN IP adresa SMTA spadá do stejné masky podsítě jako externí DHCP server (maska podsítě je vždy 255.255.255.0), jinak SMTA bude za strany LAN nedostupný. IP adresa 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 řádku Time Server 1-3 jsou již adresy přednastaveny, můžete je podle potřeby změnit.*

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

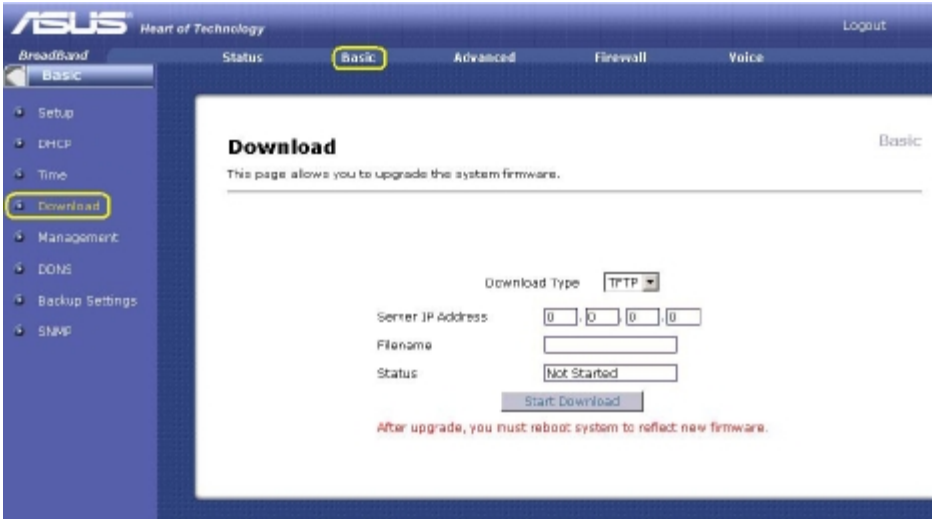
3.7 UPGRADE FIRMWARE

Pro upgrade firmwaru SMTA je potřeba nejdříve stáhnout příslušný firmware z internetu (www.joyce.cz). Po stažení souboru je firmware možno upgradovat dvěmi 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 upgradu firmwaru**
4. **Klikněte na tlačítko Start Download.**

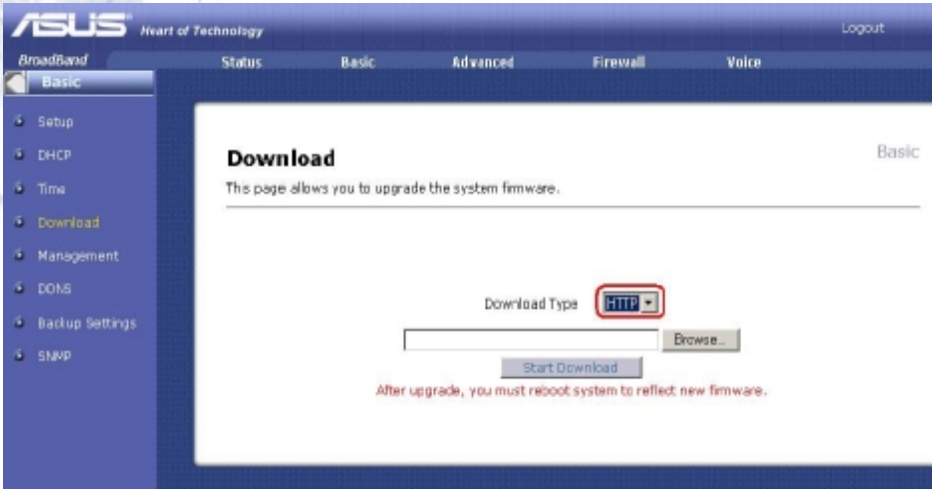
Poznámka: *Po úspěšném stažení souboru se objeví výzva k restartování přístroje*



Nahrání pomocí HTTP –

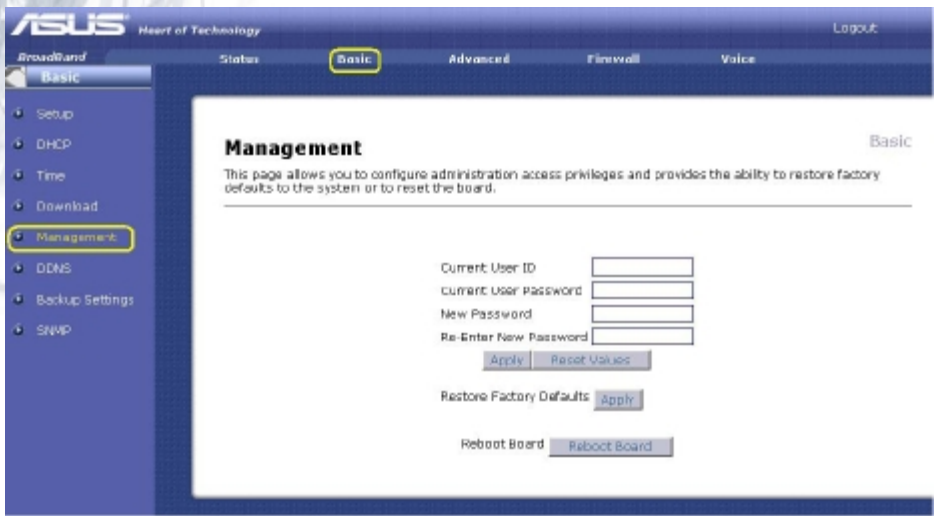
1. V roletě zvolte HTTP
2. Klikněte na Browse (Procházet) a najděte upgrade soubor na Vašem PC.
3. Klikněte na tlačítko Start Download.

Následující obrázek zobrazuje stránku pro stažení protokolem HTTP.



3.8 MANAGEMENT - STRÁNKA SPRÁVCE NASTAVENÍ

Někdy je zapotřebí obnovit původní nastavení parametrů. Toto je možné provézt 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 přihlášeni 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 –

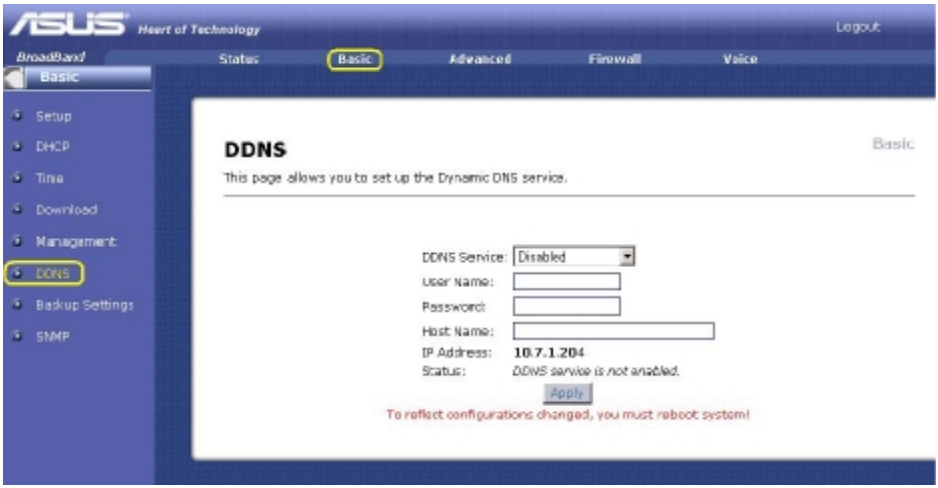
Toto je stejná funkce jako stisknutí resetovacího tlačítka na zadním panelu SMTA. Před restartováním budou uloženy všechny změny nastavení.

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.

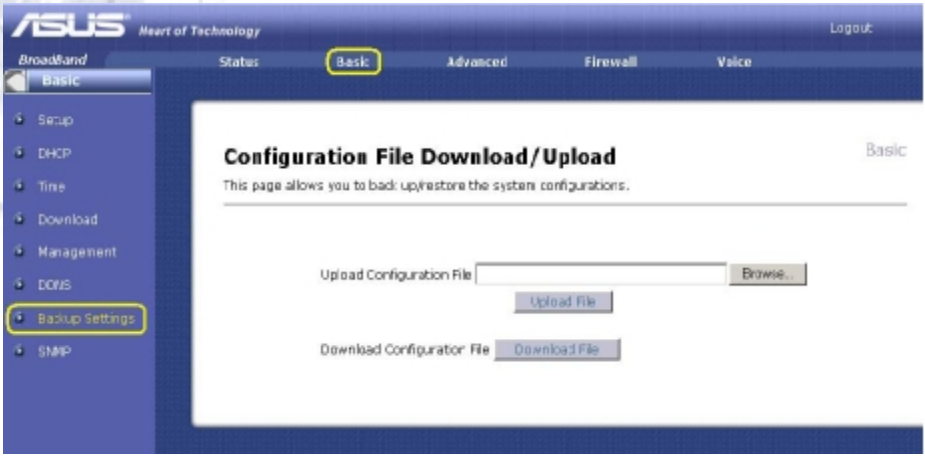
- **DDNS Service: Vyberte přednastaveného poskytovatele DDNS: www.DynDNS.org**
- **UserName: Zadejte uživatelské jméno přidělené poskytovatelem**
- **Password: Zadejte heslo přidělené poskytovatelem.**
- **HostName: Hostname, které je registrované na webové stránce DDNS poskytovatele.**
- **IP Address: 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.



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.

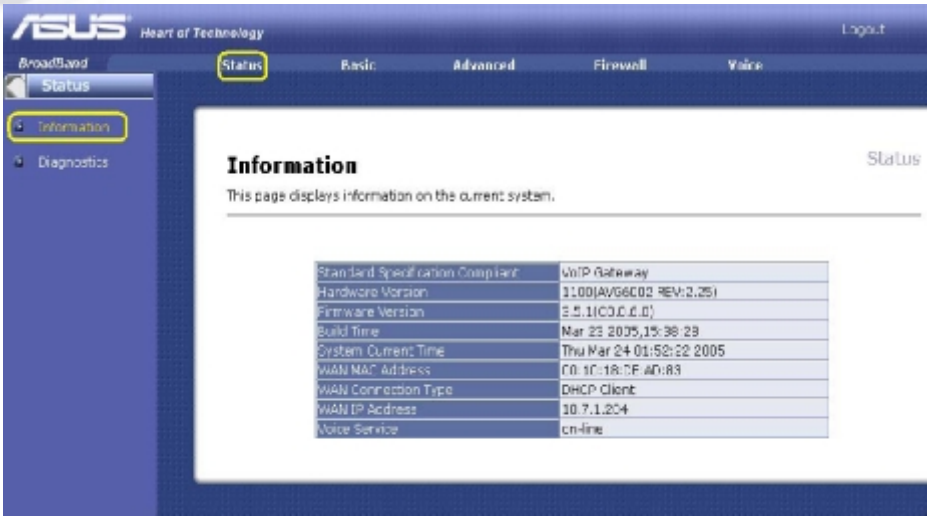


4 ŘEŠENÍ PROBLÉMŮ

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 aktualizování stisknutím tlačítka Refresh.

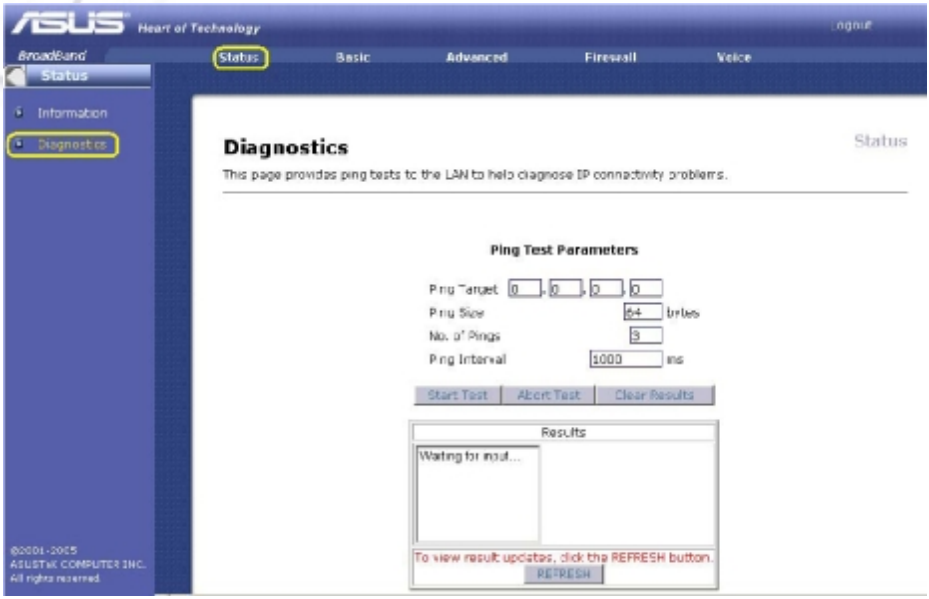


- **Standard Specification Compliant – název zařízení**
- **Hardwaru Version – verze a typové číslo přístroje**
- **Firmware Version – aktuální verze firmwaru**
- **Build Time - datum vytvoření firmwaru**
- **System Current Time – aktuální systémový čas**
- **WAN MAC Addres – MAC (Media Access Control) 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“.



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 pingy v milisekundách (1000 ms = sec)**

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

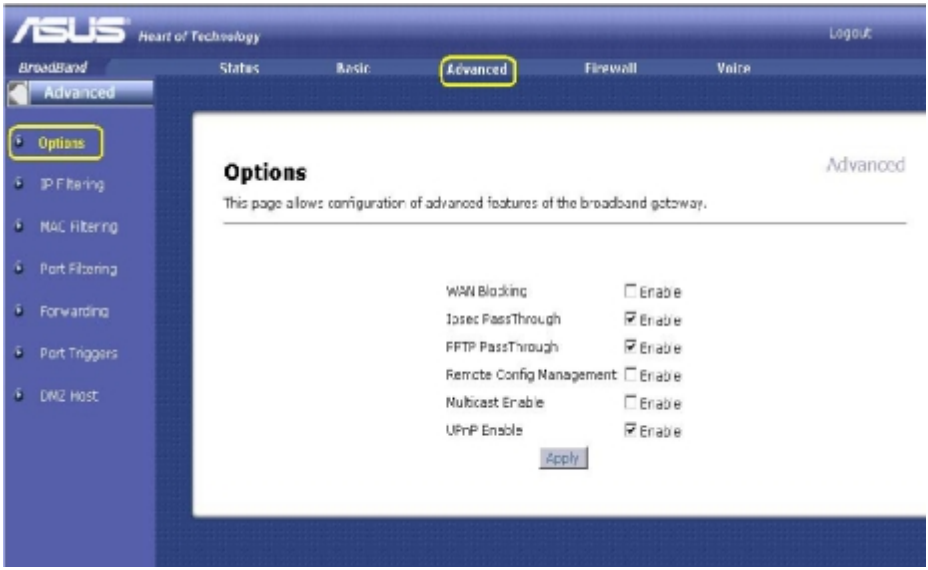
5 ADVANCED – KONFIGURACE PRO POKROČILÉ

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 triggery (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.

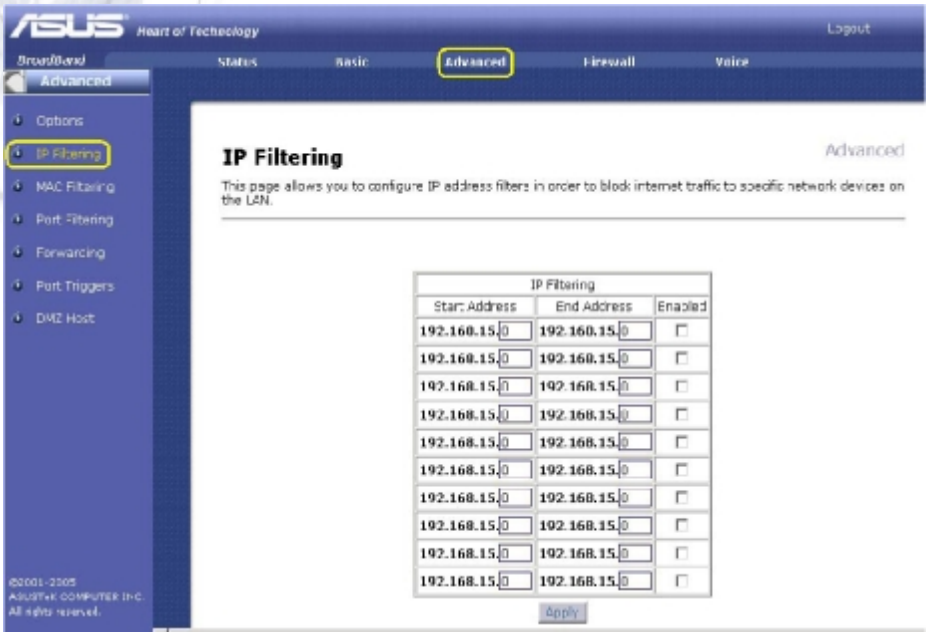


Pro aktivaci požadované funkce zaškrtněte příslušný čtvereček. Změnu nastavení odešlete tlačítkem Apply. Tyto funkce lze aktivovat bez resetování systému.

- **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 Privat 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).

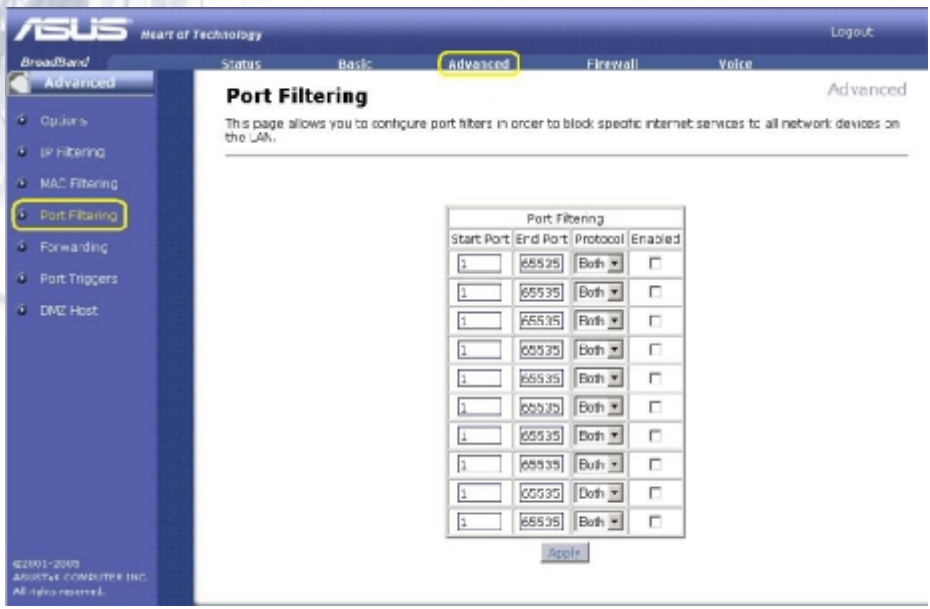


Zadáním počáteční a konečné hodnoty rozsahu filtrovaných IP adres můžete určit, kterým místním počítačům bude odepřen přístup k WAN. Všimněte si, že postačí zadat pouze LSB (nejnižší byte) IP adresy. Vyšší byty jsou automaticky převzaty z IP adresy SMTA. Pro celkovou aktivaci funkce filtrování je ještě 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 zasílání odchozího provozu do WAN , můžete také specifikovat prostřednictvím MAC adresy. Toto se nastavuje na stránce MAC Filtering Page, viz obrázek níže.

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

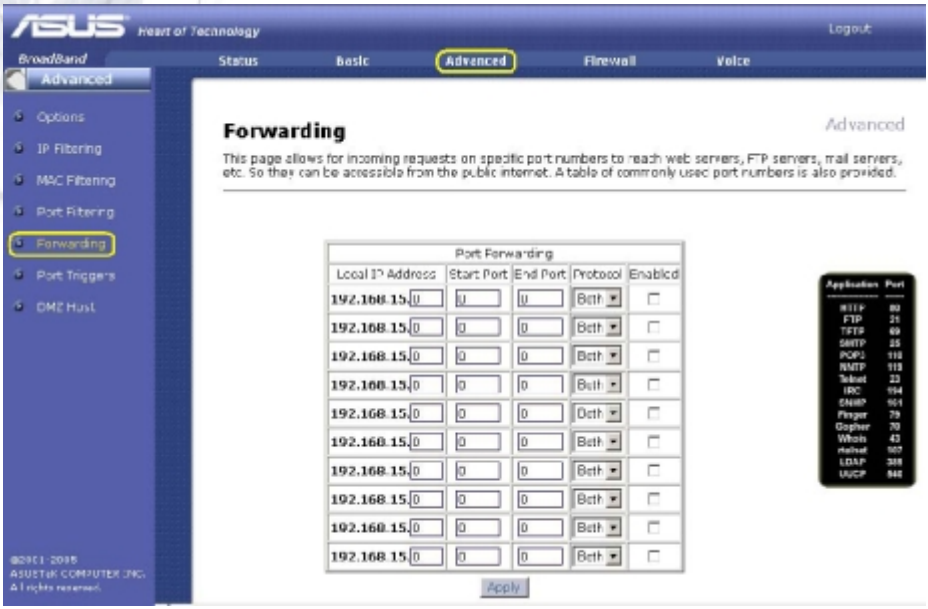
Podobně můžete zabránit odchozímu provozu na určitých portech WAN. Nastavuje se na stránce Port Filtering Page, viz obrázek níže.



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 sítě 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

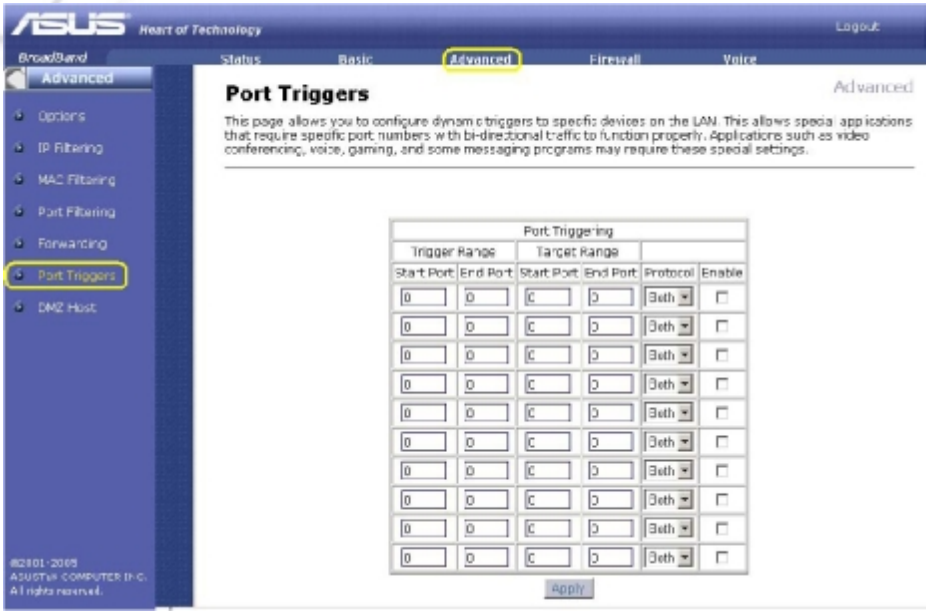
Přesměrování dovoluje provozovat veřejně přístupné servery v síti LAN namapováním TCP/UDP portů na lokální PC. Stránka Forwarding page je zobrazena níže.



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 adresu 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 potencionálním útokům hackerů.



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.

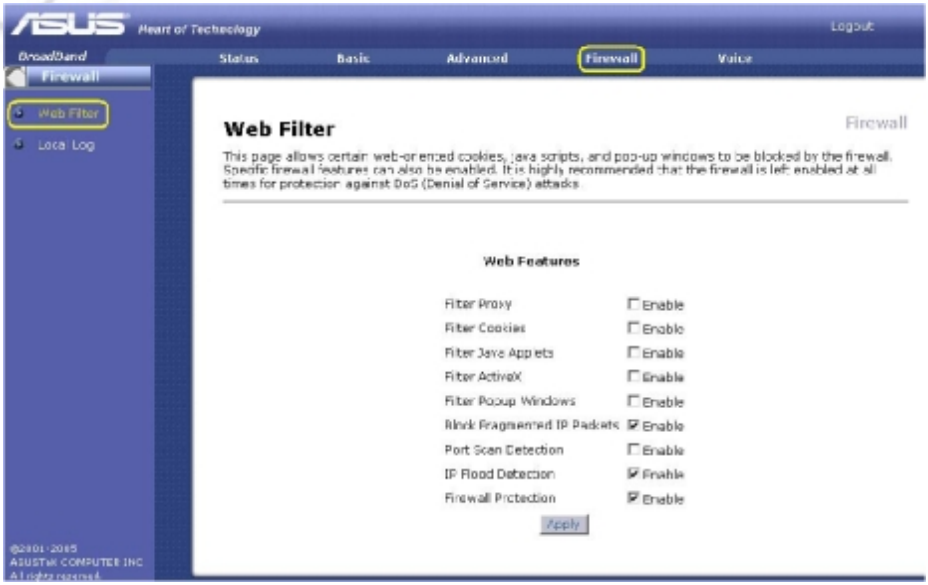
Můžete konfigurovat jedno PC jako DMZ host. To se hodí, jestliže PC používá „problémové“ aplikace, které při komunikaci používají náhodná čísla portů a neumí pracovat s porty-triggery nebo přesměrováním portů, jak bylo zmíněno v předchozí kapitole. Jestliže je některé PC specifikované jako DMZ Host, 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 zaškrtávacího okénka Enable.

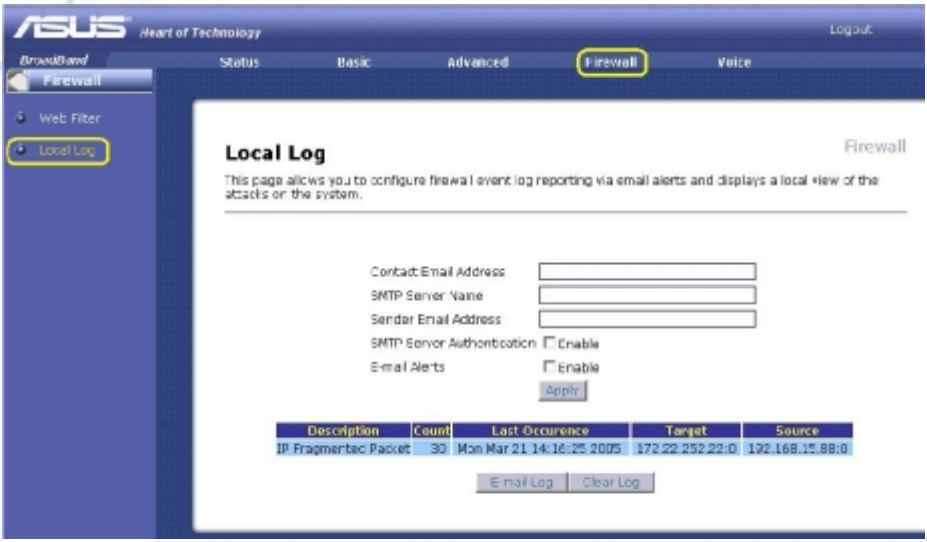


- **Blokování Proxies, Cookies, Java Applets, ActiveX controls a Popup Windows.**
- **Block Fragmentes IP Packets – blokování neúplných IP paketů**
- **Port Scan Detection – detekuje a blokuje pokusy o scanování portů, které mají původ jak z WAN, tak z LAN.**

- **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.



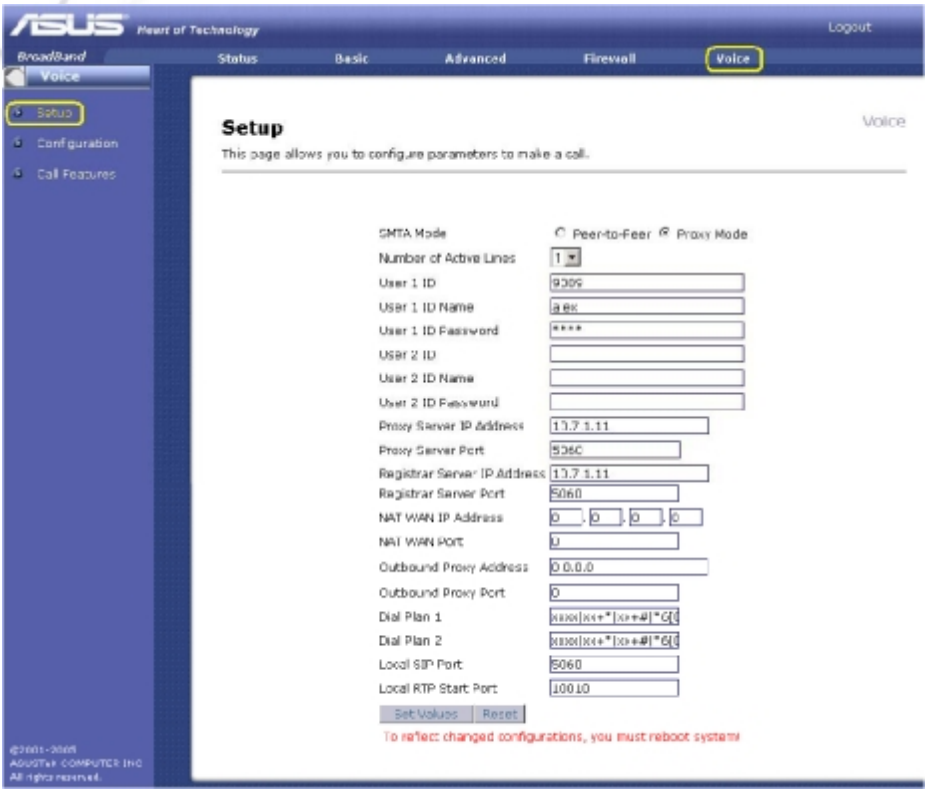
Pro zapnutí automatického varování emailem zadejte svou emailovou adresu, dále adresu emailového serveru, který tento účet spravuje (provozovaný Vaším poskytovatelem), zaškrtněte políčko „enable“ a klikněte na tlačítko Apply. Nyní bude po každém zaregistrovaném pokusu o útok zaslána samostatná zpráva. 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.

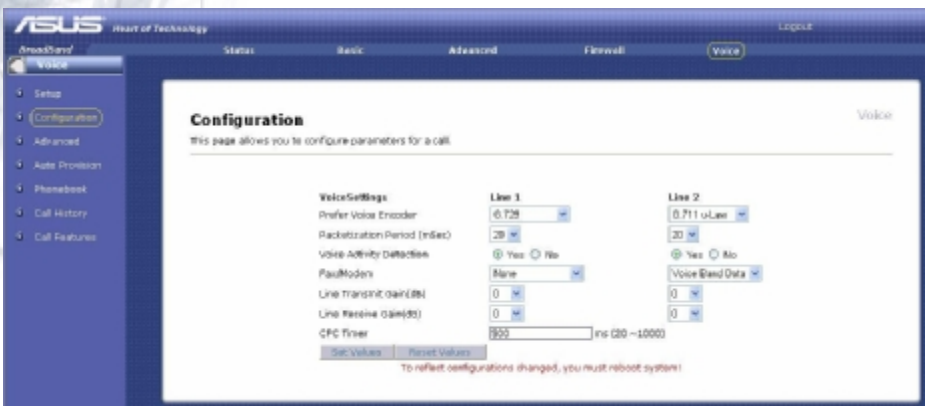


- **SMTA Mode: Peer-to-Peer: Mód Peer-to-Peer (rovný s rovným) nevyžaduje žádné další nastavování. Pouze klikněte na tlačítko.**
- **Proxy Mode: Při použití proxy módu je třeba nastavit následující parametry:**
    1. **Number of Active Lines – počet používaných linek nebo portů.**
    2. **User 1 ID – 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 vytáčecích 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

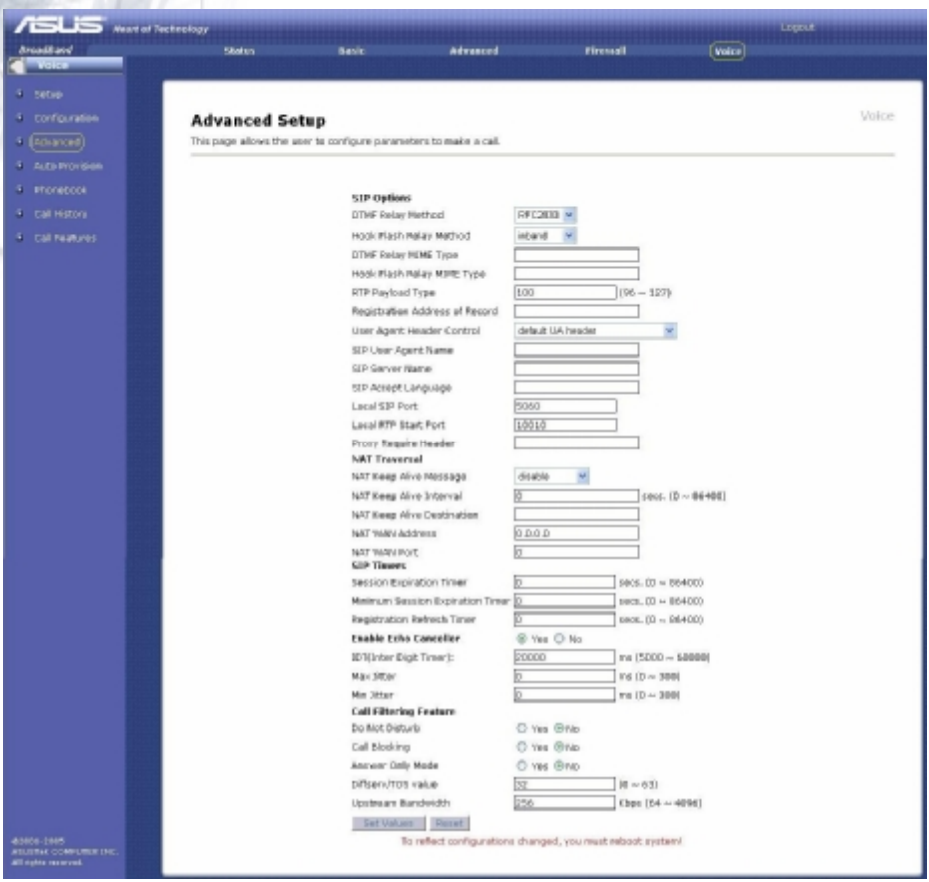
Na této stránce je možno nastavovat způsob odesílání a příjmu hlasové aktivity.



- **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.



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

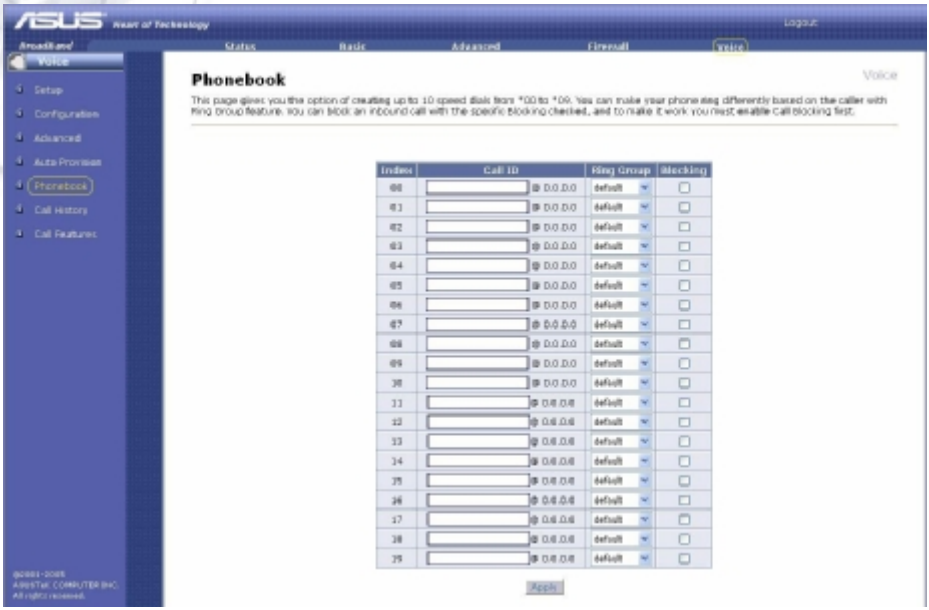
- **Minimum Session Expiration Timer – nejkratší dovolená délka trvání spojení.**
- **Registration Refresh Timer (v mikrosekundách) – časový interval, po jehož uplynutí bude požadováno obnovení registrace.**
- **Enable Echo Canceller – zapnutím se zruší efekt echa v hovoru.**
- **IDT (Inter Digit Timer) – 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 příchozí 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 užitného 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 příchozí hovory. Volající uslyší obsazovací tón.**
- **Call Blocking – blokuje příchozí hovory z čísel uvedených v seznamu blokovaných 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 nezvolíte Auto Provision musíte nastavit ASUS VP100 (SMTA) manuálně. Tuto službu misí podporovat ISP.

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 vyzvánění. Dále můžete zablokovat některé příchozí hovory.

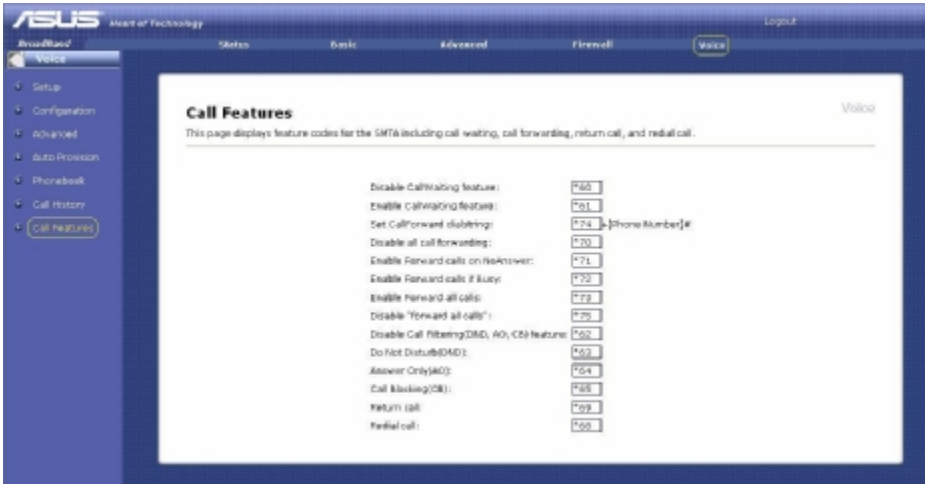


7.6 CALL HISTORY

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, přesměrování, 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 přesměrování	Umožňuje vložit číslo, na které budou přesměrovány příchozí hovory	Vytočte à 74 a telefonní číslo, na které mají být hovory přesměrovány; toto je pouze vložení čísla, nikoliv zapnutí funkce Zrušit VŠECHNA přesměrování – vytočte à 70
Přesměrovat, jestliže není odpověď	Přesměruje příchozí hovory, které nebudou zvednuty, na zvolené číslo	Pro zapnutí navolte à 71
Přesměrovat, pokud je obsazeno	Přesměruje příchozí hovory na zvolené číslo, pokud bude právě obsazeno	Pro zapnutí navolte à 72
Přesměrovat všechny hovory	Přesměruje 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.

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 specification under which conformity is declared)
in accordance with 89/336 EEC-EMC Directive and 1999/5 EC-R & TTE Directive

☐ EN 300328	Electromagnetic compatibility and Radio spectrum Matters (ERM); wideband transmission equipment operating in the 2.4GHz ISN 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	☒ EN 55022	Limits and methods of measurement of radio disturbance characteristics of information technology equipment
		☒ EN 55024	Information Technology equipment-Immunity characteristics-Limits and methods of measurement
☒ EN 300386	Electromagnetic compatibility and Radio spectrum Matters (ERM);Telecommunication equipment; ElectroMagnetic Compatibility (EMC) requirements	☐ EN 50360/ EN 50361	the limitation of exposure of the general public to electromagnetic network fields (0 Hz to 300 GHz) International Commission on Non-Ionizing Radiation Protection (1998), Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields
☐ EN 301489	Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic compatibility(EMC) standard for radio equipment and services; Part 17: Specific conditions for wideband data and HIPERLAN equipment	☐ EN 61000-3-2*	Disturbances in supply systems caused
		☐ EN 61000-3-3*	Disturbances in supply systems caused
☐ 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 (99/5/EC) Directive	☐ EN 55013	Limits and methods of measurement of radio disturbance characteristics of broadcast receivers and associated equipment
		☐ EN 55020	Immunity from radio interference of broadcast receivers and associated equipment
☐ EN 301839	Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive	☐ EN 50081-2	Generic emission standard Part 2 Industrial environment
		☐ EN 50082-2	Generic immunity standard Part 2: Industrial environment

☒ CE marking — CE (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

☐ EN 60065	Safety requirements for mains operated electronic and related apparatus for household and similar general use	☒ EN 60950-1	Safety for information technology equipment including electrical business equipment
☐ EN 60335	Safety of household and similar electrical appliances	☐ EN 50091-1	General and Safety requirements for uninterruptible power systems (UPS)

Manufacturer/Importer

Signature : _____

(Stamp) Date: MAR. 10, 2005

Name : Jonathan Tseng