



Vigor 2700VoIP

Užívateľská príručka

(verzia 2.0, dátum 11.8. 2006)

Obsah

1. Indikácia a konektory	5
1.1 Predný a zadný pohľad na Vigor 2700VoIP	5
1.2 Inštalácia hardvéru	5
2 Základné nastavenia	6
2.1 Zmena hesla	6
2.2 Rýchle nastavenie (Quick start wizard)	8
2.2.1 Nastavenie protokolu/zapúzdrenie	8
2.2.2 PPPoE/PPPoA	9
2.2.3 Bridged IP	11
2.2.4 Routed IP	11
2.3 Online stav	11
2.4 Status bar	12
3 Rozšírené nastavenia webu	12
3.1 Prístup na Internet	13
3.1.1 Základy Internet Protokol (IP) siete	13
3.1.2 PPPoE/PPPoA	13
3.1.3 MPoA	16
3.1.4 MULTI - PVC	18
3.2 LAN	20
3.2.1 Základy LAN	20
3.2.2 Hlavné nastavenie	22
3.2.3 Statické routovanie	24
3.2.4. Virtualne LAN (VLAN)	27
3.2.5 Spojiť IP s MAC	28
3.3 NAT	29
3.3.1 Presmerovanie portov	29
3.3.2 DMZ hostiteľ	31
3.3.3 Otvorenie skupiny portov	32
3.3.4 Zoznam najbežnejších portov	34
3.4 Firewall	34
3.4.1 Základy pre firewall	35
3.4.2 Hlavné nastavenie	37
3.4.3 Nastavenie filtrovania	38
3.4.4 Blokovanie IM	41
3.4.5 P2P blokovanie	41
3.4.6 DoS obrana	42
3.4.7 Obsahové filtrovanie	44
3.5 Riadenie Pasma	46
3.5.1 Limit pre session	46
3.5.2 Limit sirky pasma	47
3.5.3 QoS - Kvalita služby	48
3.6 Aplikácie	53
3.6.1 Dynamické DNS	54
3.6.2 Plánovač	55
3.6.3 Radius	57
3.6.4 UPnP	57
3.6.5. IGMP	59
3.6.6. Wake on LAN	60
3.7 VPN a vzdialený prístup	60
3.7.1 Riadenie vzdialeného prístupu	60
3.7.2 PPP Hlavné nastavenie	61
3.7.3 IPSec hlavné nastavenie	62
3.7.4 IPSec Peer totožnosť	63
3.7.5 Vzdialene prihlásený užívateľ	64
3.7.6 LAN to LAN	67
3.7.7 Sprava spojenia	73
3.8 Správa certifikátov	73
3.8.1 Lokálny certifikát	73
3.8.2 Dôveryhodný CA certifikát	75
3.9 VoIP	76
3.9.1 Programovanie volaní	77
3.9.2 Účty SIP	80
3.9.3 Nastavenia telefónu	82
3.9.4 Stav	86
3.11 Správa systému	87

3.11.1 Stav systému	88
3.11.2 Heslo administrátora	89
3.11.3 Zálohovanie konfigurácie	90
3.11.4 Zaznamenávanie systému	91
3.11.5 Čas a dátum	93
3.11.6 Správa systému	94
3.11.7 Reštartovanie systému	95
3.11.8 Upgrade firmveru	95
3.12. Diagnostické nástroje	96
3.12.1 WAN pripojenie	96
3.12.2 Dial-out spúšťači mechanizmus	97
3.12.3 Routovacia tabuľka	97
3.12.4 ARP Cache tabuľka	98
3.12.5 DHCP tabuľka	98
3.12.6 NAT tabuľka spojení (sessions)	99
3.12.7 Ping Diagnostika	100
3.12.8 Monitor prietoku dát	100
3.12.9 Sledovanie trasy paketu	101

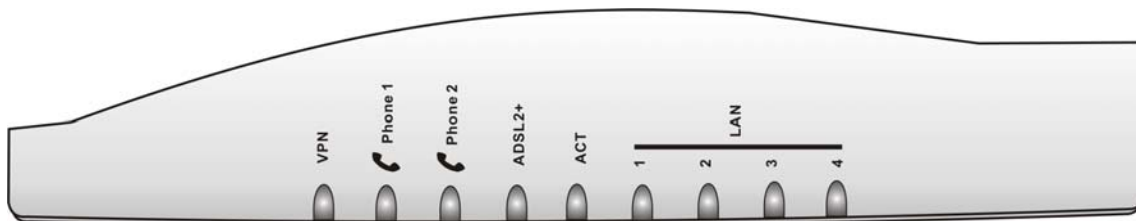
ÚVOD

Vigor2700VoIP je zariadenie ktoré integruje ADSL, ADSL2/2+ prístup pre uspokojenie nárokov bytových i firemných zákazníkov. Pri rýchlosti sťahovania do 12Mbps (ADSL2) alebo 24Mbps (ADSL2+), Vigor2700VoIP poskytuje výnimočnú šírku prístupu na internet.

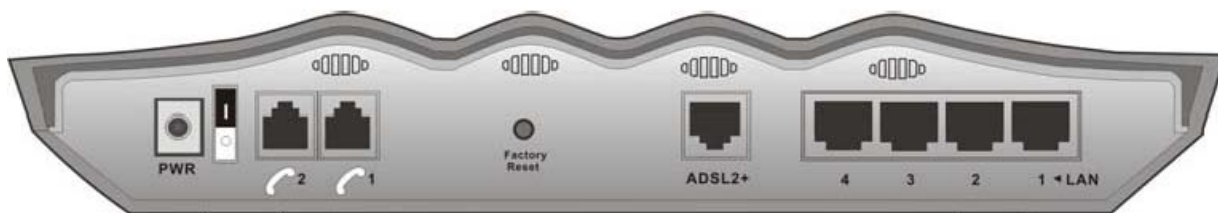
Pre zabezpečenie vášho systému poskytuje Vigor vyspelý firewall s vyspelými prvkami ako napr. Stateful Packet Inspection (stavová inšpekcia paketov - SPI), aby zabezpečil spoľahlivosť siete zisťovaním a zabránením preniknutia paketov s nebezpečným obsahom, alebo útokom na DoS. Ďalej umožňuje rodičovskú kontrolu webu proti zobrazovaniu stránok s nevhodným obsahom.

1. Indikácia a konektory

1.1 Predný a zadný pohľad na Vigor 2700VoIP



LED	Stav	Vysvetlenie
VPN	Svieti	VPN tunel je vytvorený.
Phone 1 & 2 (FXS1, FXS2)	Svieti	Telefón je zodvihnutý.
	Bliká	Prichádza telefónny hovor
ADSL2+	Svieti (Zelená)	ADSL je v móde show time (prijaté k DSLAM).
	Bliká (Zelená)	Zariadenie je v stave synchronizácie s DSLAM (showtime)
	Bliká (Orange)	Prenášajú sa dáta
ACT (Activity)	Svieti	Router je zapnutý.
	Bliká	Router je zapnutý a v prevádzkovom stave.
LAN (1, 2, 3, 4)	Zelená	Je vytvorené spojenie na príslušnom porte.
	Bliká	Prenášajú sa ethernetové pakety.



Rozhranie	Vysvetlenie
PWR	Konektor pre napájací zdroj 12VDC.
0/1	Vypínač zariadenia (0-Vypnuté 1- Zapnuté)
VoIP 1/2	RJ 11 konektor pre analógovú VoIP komunikáciu.
Factory Reset	Obnoví výrobné nastavenie. Použitie I: Zapnite router (ACT LED bliká). Zatlačte a držte stlačené tlačítko na viac ako 5 sekúnd. Keď začne ACT LED blikáť rýchlejšie ako je v bežnom stave, uvoľnite tlačítko. Router sa reštartuje s výrobným nastavením. Použitie II: Vypnite router (ACT nesvieti). Zatlačte a držte tlačítko stlačené, potom router zapnite. Po viac ako 5 sekundách od zánutia routera uvoľnite tlačítko. Router je v dočasném výrobnom nastavení a čaká na upgrade firmvéru, pomocou softvéru na upgradovanie firmvéru spustenom na PC pripojenom iba v drôtovej LAN (nie cez WIFI).
ADSL 2+	Konektor prístup do internetu cez ADSL, ADSL2/2+.
LAN 4 – 1	Konektor pre lokálne sieťové zariadenia.

1.2 Inštalácia hardvéru

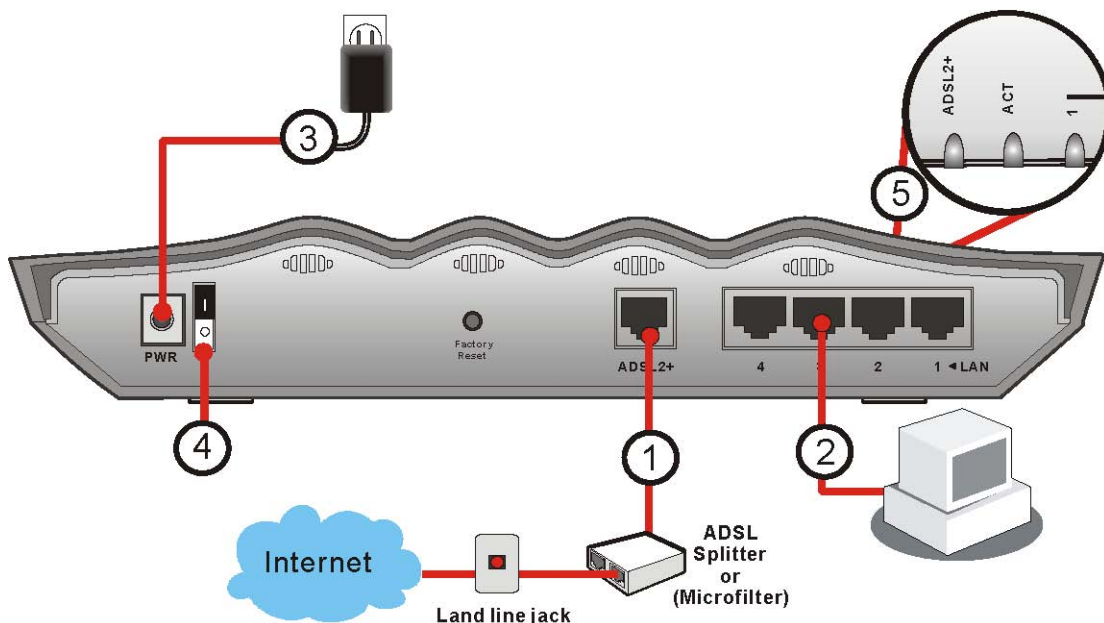
Pred začatím konfigurácie routera, je potrebné korektne pripojiť vaše zariadenie. Pripojte DSL rozhranie k externému ADSL splittru ADSL káblom.

Pripojte jeden zo štyroch portov k vášmu počítaču káblom RJ-45. Toto zariadenie umožňuje prepojiť priamo štyri počítače.

Pripojte jeden koniec elektrického káblu do konektoru zariadenia a druhý do el. zásuvky.

Zapnite router.

Skontrolujte LED diódy ACT a ADSL2+, LAN LEDs aby ste sa uistili že sieť je prepojená. (detailnejšie informácie o LED viď sekcia 1.1.)



2 Základné nastavenia

Pre riadne používanie routeru je dôležité zmeniť heslo konfigurácie webu kvôli bezpečnosti a upraviť základné nastavenia.

Táto kapitola vysvetľuje ako nastaviť administrátorské heslo a ako upraviť základné nastavenia pre úspešne pripojenie k internetu. Uvedomte si, že len administrátor môže meniť nastavenia.

2.1 Zmena hesla

Ak chcete zmeniť heslo zariadenia, musíte najskôr vstúpiť na stránku nastavení prostredníctvom prednastaveného hesla.


Zaistite, aby bol počítač riadne pripojený k routeru.



Poznámka: Môžete jednoducho nastaviť váš počítač aby získal IP adresu dynamicky od routeru alebo nastaviť IP adresu počítača tak, aby bola taká istá ako prednastavená IP adresa siete routeru 192.168.1.1.

Otvorte váš internetový prehliadač a zadajte adresu <http://192.168.1.1>. Otvori sa pop-up okno ktoré bude vyžadovať používateľské meno a heslo. Zadajte prednastavené hodnoty meno používateľa: **admin** a heslo: **admin** a kliknite na OK.

Pripojiť na: 192.168.1.1



Login to the Router Web Configurator

Meno používateľa:

Heslo:

☐ Zapamätať heslo

OK Zrušiť

Teraz sa otvorí hlavné okno.

Vigor2700 Series

ADSL2/2+ Firewall Router

DrayTek
www.draytek.com

Rychle nastavenie
Online stav

Pristup do internetu
LAN
NAT
Firewall
Riadenie pasma
Aplikacie
VPN a vzdialeny pristup
Sprava certifikatov
VoIP
Sprava systemu
Diagnosticke nástroje

Texty su bez diakritiky.

Stav systému

Nazov modelu	: Vigor2700 series
Verzia firmware	: 2.6.2.1_RC3
Datum a čas výroby	: Aug 7 2006 17:22:44

LAN MAC adresa : 00-50-7F-D6-99-A8 1. IP adresa : 192.168.1.1 Maska 1. podsiete : 255.255.255.0 DHCP Server : Ano	WAN Stav linky : Nepripojena MAC adresa : 00-50-7F-D6-99-A9 Spojenie : --- IP adresa : --- Prednastavena brana : --- DNS : 194.109.6.66
--	---

VoIP Port : 1 2 SIP server : sip.voi.t-com.sk as Meno/Cislo uctu : change_me change_me Registracia na SIP : Kodek : Prichadzajuće volania : 0 0 Odchadzajuće volania : 0 0
--

Chodíte na stránku System Maintenance (Správa systému) a zvolíte Administrator Password (Heslo administrátora).

[Sprava systemu >> Nastavenie administratorskeho hesla](#)

Heslo administrátora


Stare heslo	<input type="password"/>
Nove Heslo	<input type="password"/>
Znovuzadanie noveho hesla	<input type="password"/>

OK

Zadajte vstupné heslo (prednastavené je **admin**) v poli Old Password. Zadajte nové do poľa Stare heslo a zadajte ho opakovane do poľa Znovuzadanie noveho hesla. Pokračujte kliknutím na OK.

Vaše heslo bolo zmenené. Pri ďalšom otvorení použite nové heslo na prístup do konfigurátora routera.

Pripojiť na: 192.168.1.1 [?] [X]



Login to the Router Web Configurator

Meno používateľa:

Heslo:

☐ Zapamätať heslo

2.2 Rýchle nastavenie (Quick start wizard)

Ak Váš router môže pracovať v prostredí s vysokorychlostným NAT, táto konfigurácia vám pomôže nastaviť a používať router rýchlo. Prvé okno Quick Start Wizardu je vstupné heslo. Po zadaní hesla kliknite na Next (ďalej).

2.2.1 Nastavenie protokolu/zapúzdrenie

V Quick Start Wizarde, môžete nakonfigurovať prístup routeru na internet pomocou rôznych protokolov ako PPPoE, PPPoA, Bridged IP, alebo Routed IP.

Rychle nastavenie

2. Pripojenie do internetu

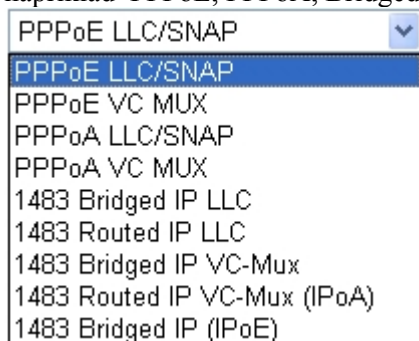
VPI	<input type="text" value="1"/>	<input type="button" value="Auto detekcia"/>
VCI	<input type="text" value="32"/>	
Protokol / Zapuzdrenie	<input type="text" value="PPPoE LLC/SNAP"/>	
Pevna IP	<input type="radio"/> Ano <input checked="" type="radio"/> Nie(Dynamicka IP)	
IP adresa	<input type="text"/>	
Maska podsiete	<input type="text"/>	
Predvolena brana	<input type="text"/>	
Primarny DNS	<input type="text"/>	
Sekundarny DNS	<input type="text"/>	

Teraz nastavte vhodný typ sieťového pripojenia na internet cez router podľa nastavení poskytnutých vašim poskytovateľom internetových služieb.

VPI je skratka pre Virtual Path Identifier (identifikátor virtuálnej cesty). Je to 8-bitová hlavička vnútri každej ATM bunky ktorá indikuje kam má byť bunka smerovaná. ATM je metóda posielania dát v malých paketoch pevnej veľkosti. Používa sa na prenos dát do klientských počítačov.

VCI je skratka Virtual Channel Identifier (identifikátor virtuálneho kanálu). Je to 16-bitová hlavička vnútri každej ATM bunky ktorá indikuje kam má byť bunka smerovaná počas cesty sieťou. Virtuálny kanál je logické prepojenie medzi dvoma koncovými zariadeniami siete.

Protokol/Zapúzdrenie Zvoľte režim IP rozhrania siete. Je dostupných niekoľko režimov prístupu na internet ako napríklad PPPoE, PPPoA, Bridged IP a Routed IP.



Pevná IP kliknite na Yes (áno) na špecifikáciu pevnej IP adresy routera. Inak kliknite na **Nie (Dynamická IP)** aby ste umožnili routeru voľiť si dynamickú IP adresu. Ak zvolíte **Nie**, nasledujúca IP adresa, maska podsiete a zvolená brána sa nezmení.

IP adresa priradiť IP adresu ku zvolenému protokolu.

Maska podsiete priradiť hodnotu masky podsiete ku protokolu Routed IP alebo Bridged IP.

Predvolená brána Priradiť IP adresu brány ku protokolu Routed IP a Bridged IP.

Primárny DNS Priradiť IP adresu primárnej DNS.

Sekundárny DNS Priradiť IP adresu sekundárnej DNS.

2.2.2 PPPoE/PPPoA

PPPoE je skratka pre Point-to-Point Protocol over Ethernet (protokol bod do bodu cez ethernet). Je založený na dvoch široko uznávaných štandardoch – PPP a Ethernet. Spája používateľov cez ethernet a internet pomocou spoločného širokopásmového média, napríklad DSL linka, bezdrátové spojenie alebo káblový modem. Všetci užívatelia ethernetu môžu zdieľať spoločné pripojenie.

PPPoA znamená Point-to-Point Protocol over ATM (PPP cez ATM). PPPoA využíva PPP dial-up protokol s prenosom cez ATM.

PPPoE používa väčšina užívateľov DSL. Všetci miestni užívatelia môžu zdieľať jedno PPPoE alebo PPPoA pripojenie na internet. Váš poskytovateľ internetových služieb vám poskytne užívateľské meno, heslo a autentifikačný režim.

Ak vám váš poskytovateľ IS poskytuje pripojenie PPPoE alebo PPPoA, zvolte PPPoE alebo PPPoA.

3. nastavit PPPoE / PPPoA

Meno poskytovateľa	<input type="text"/>
Užívateľské meno	<input type="text"/>
heslo	<input type="password"/>
Potvrdiť heslo	<input type="password"/>
<input checked="" type="checkbox"/> Vždy zapnuté	
Odpojiť po	<input type="text" value="-1"/> Sekund

Meno poskytovateľa	zadájte špecifické meno podľa požiadaviek poskytovateľa internetových služieb.
Užívateľské meno	zadájte platné užívateľské meno poskytnuté poskytovateľom internetových služieb.
Heslo	zadájte platné heslo poskytnuté poskytovateľom internetových služieb.
Potvrdiť heslo	zadájte heslo ešte raz.
Vždy zapnuté	odškrtnite toto pole pre trvalé pripojenie k internetu
Odpojiť po	zadájte hodnotu v sekundách, po akej bude prerušené pripojenie k internetu pri nečinnosti.

Kliknite na Dalej pre kontrolu a potvrdenie zvolených nastavení.

Sprievodca rychlím startom

4. Prosím potvrďte vaše nastavenia:

VPI	: 1
VCI	: 32
Protokol / Zapuzdrenie	: PPPoE / LLC
Pevná IP	: Nie
Primárny DNS	:
Sekundárny DNS	:
Vždy zapnutý	: Áno

Kliknite na Ukončit. Zobrazí sa online status protokolu vid' okno nižšie.

Online stav

Systemový stav				Čas od spustenia systému: 0:1:5		
LAN stav		Primárny DNS: 195.12.128.1		Sekundárny DNS: 195.72.0.3		
IP adresa		TX Pakety	RX pakety			
192.168.1.1		1	0			
WAN stav		IP adresa brány: 195.72.7.1		<button>Rozpojit PPPoE</button>		
Mod	IP adresa	TX Pakety	TX rychl.	RX pakety	RX rychl.	Čas od spustenia systému
PPPoE	62.65.169.134	43	35	40	16	0:00:32
ADSL informácie		(Verzia ADSL firmware: 1311302_B)				
ATM statistiky	TX bloky	RX bloky	Upravené bloky		Neupravené bloky	
	55	44	0		1	
ADSL stav	Mod	Stav	Rychlost odosielania	Rychlost prijimania	Odstup signal-sum	Trvanie linky
	G.DMT	SHOWTIME	352000	3072000	9	48

2.2.3 Bridged IP

Kliknite na 1483 Bridged IP ako protokol. Zadáajte všetky informácie obdržané od poskytovateľa internetových služieb.

Po zadání všetkých informácií na tejto stránke, kliknite na Next (Dalej) pre pokračovanie na Ďalšiu stránku. Tu kliknite na Finish (uončiť). Zobrazí sa Online stav protokolu.

2.2.4 Routed IP

Kliknite na protokol 1483 Routed IP. Zadáajte všetky informácie obdržané od poskytovateľa internetových služieb.

Po zadání všetkých informácií na tejto stránke, kliknite na Next (Dalej) pre pokračovanie na Ďalšiu stránku. Tu kliknite na Finish (uončiť). Zobrazí sa Online stav protokolu.

2.3 Online stav

Online staa zobrazuje stav systému, WAN siete, informácie o ADSL a stave súčastí routera na jednej stránke. Ak zvolíte PPPoE alebo PPPoA ako protokol, nájdete na stránke Online Status tlačítko **Vytocit PPPoE** alebo **Vytocit PPPoA**

Systemový stav				Čas od spustenia systému: 0:1:5		
LAN stav		Primárny DNS: 195.12.128.1		Sekundárny DNS: 195.72.0.3		
IP adresa		TX Pakety		RX pakety		
192.168.1.1		1		0		
WAN stav		IP adresa brany: 195.72.7.1		Rozpojit PPPoE		
Mod	IP adresa	TX Pakety	TX rychl.	RX pakety	RX rychl.	Čas od spustenia systému
PPPoE	62.65.169.134	43	35	40	16	0:00:32
ADSL informácie (Verzia ADSL firmware: 1311302_B)						
ATM statistiky	TX bloky	RX bloky	Upravené bloky		Neupravené bloky	
	55	44	0		1	
ADSL stav	Mod	Stav	Rychlost odosielania	Rychlost prijimania	Odstup signal-sum	Trmenie linky
	G.DMT	SHOWTIME	352000	3072000	9	48

Primárny DNS	Zobrazuje pridelenú IP adresu pre primárnu DNS
Sekundárny DNS	Zobrazuje pridelenú IP adresu pre sekundárnu DNS.
IP adresa (v LAN)	Zobrazuje IP adresu v miestnej sieti.
TX Pakety	Zobrazuje celkový počet paketov vyslaných cez rozhranie miestnej siete.
RX Pakety	Zobrazuje celkový počet paketov prijatých cez rozhranie miestnej siete.
IP adresa brany:	Zobrazuje IP adresu pridelenú zvolenej bráne.
IP adresa (vo WAN)	Zobrazuje IP adresu rozhrania WAN siete.
TX Rychl.	Zobrazuje rýchlosť odosielania paketov cez rozhranie WAN siete.
RX Rychl	Zobrazuje rýchlosť prijímania paketov cez rozhranie WAN siete.
Čas od spustenia systému	Zobrazuje celkovú dobu prevádzky rozhrania.
TX bloky	Zobrazuje celkový počet odoslaných ATM Blokov.
RX bloky	Zobrazuje celkový počet prijatých ATM Blokov.
Upravené bloky	Zobrazuje celkový počet prijatých ATM blokov ktoré boli poškodené a opravené.
Uncorrected Blocks	Zobrazuje celkový počet prijatých ATM blokov ktoré boli poškodené, ale neopravené.
Mod	Zobrazuje používaný režim modulácie: G.DMT, G.Lite, alebo T1.413.
Stav	Zobrazuje stav DSL linky.
Rychlost odosielania	Zobrazuje rýchlosť odosielania dát (bit/sekunda).
Rychlost prijimania	Zobrazuje rýchlosť prijímania dát (bit/sekunda).
Odstup signal-sum	Zobrazuje hodnotu Signal Noise Ratio Margin (dB). Čím vyššia hodnota, tým lepšia kvalita signálu
Trmenie linky	Zobrazuje hodnotu

2.4 Status bar

Pri každom kliknutí na OK na stránke pri uložení nastavenia, môžete nájsť odkazy, ktoré vám ukazujú interakciu systému s vami.

Stav: Pripravený

Pripravený ukazuje že systém je pripravený aby ste zadávali nastavenia.

Settings Saved (Nastavenia uložené) znamená že vaše nastavenia budú uložené ak kliknete na Finish (dokončiť) alebo OK.

3 Rozšírené nastavenia webu

Po ukončení základných nastavení routera sa ľahko pripojíte na Internet. Tým, ktorí chcu upraviť viac nastavení, aby si ich prispôbili svojim požiadavkám, je určená táto kapitola.

3.1 Prístup na Internet

Pristup do internetu

- PPPoE / PPPoA
- MPoA (RFC1483/2684)
- Multi-PVC

3.1.1 Základy Internet Protokol (IP) siete

IP znamená Internet Protokol. Každé zariadenie pracujúce v sieti založenej na IP vrátane routerov, tlačových serverov a hostiteľských PC potrebuje IP adresu, aby bol identifikovateľný v sieti. IP adresy sú verejne publikované v Network Information Centre (Centrum sieťových informácií - NIC), aby sa predišlo konfliktom IP adries. Mať jedinečnú IP adresu je povinné pre zariadenia vo verejných sieťach, pre súkromné a miestne siete však nie, ani nie je povinné pre hostiteľské PC v správe routera pokiaľ nie sú určené na verejný prístup. Preto má NIC rezervované určité adresy verejnosti na registráciu neprístupné. Ostatné sú známe ako súkromné IP adresy a ich zoznam je nasledovný:

od 10.0.0.0 do 10.255.255.255

od 172.16.0.0 do 172.31.255.255

od 192.168.0.0 do 192.168.255.255

Čo sú verejné a súkromné IP adresy

Pri svojej úlohe routera riadiť a ochraňovať miestnu sieť, spája skupinu hostiteľských PC. Každý z nich má súkromnú IP adresu pridelenú vo Vigor routeri zabudovaným DHCP severom. Router použije prednastavenú osobnú IP adresu: 192.168.1.1 pre komunikáciu s miestnymi hostiteľmi. Medzitým bude komunikovať s inými zariadeniami za použitia verejnej IP adresy. Po prechode dát router pretransformuje verejnú adresu na súkromnú a dáta prídu na určený hostiteľský počítač. Týmto spôsobom môže viac PC zdieľať jedno pripojenie na Internet.

Získajte svoju verejnú IP adresu od poskytovateľa IS

Pre získanie verejnej IP adresy pre Vigor router od vášho poskytovateľa IS existujú tri protokoly: Point to Point Protocol over Ethernet (PPPoE), PPPoA and MPoA. Multi-PVC ponúka pokročilejšie nastavenia.

Pri rozložení ADSL je na premostenie zariadení umiestnených v objekte zákazníka (customer premises equipment (CPE)) potrebné overenie a autorizácia PPP. Point to Point Protocol over Ethernet (PPPoE) spája sieť hostiteľských PC prostredníctvom prístupového zariadenia s koncentrátoru vzialeného prístupu alebo agregáčného koncentrátora. Táto implementácia uľahčuje užívateľovi používanie zariadenia. Poskytuje kontrolu prístupu, účtovanie, typ služby na základe požiadaviek používateľa.

Keď sa router začne pripájať k poskytovateľovi IS, spustí sa proces požadovania spojenia. Následne sa vytvorí komunikácia. Vaše používateľské ID a heslo je overené prostredníctvom PAP alebo CHAP autentifikačným systémom RADIUS. Poskytovateľom IS vám bude pridelená IP adresa, DNS server a iné požadované informácie.

3.1.2 PPPoE/PPPoA

PPPoA, zahrnutý v RFC1483, môže pracovať v Logical Link Control-Subnetwork Access Protocol alebo režime VC-Mux . ako zariadenie CPE, Vigor router slúži na transport na základe PPP session cez ADSL loop a Digital Subscriber Line Access Multiplexer (SDLAM) vášho poskytovateľa IS.

Aby ste zvolili PPPoE or PPPoA ako prístupový protokol na Internet, zvolte PPPoE/PPPoA z Prístup do internetu.

Zobrazí sa nasledujúca stránka:

PPPoE / PPPoA klientsky mod

PPPoE/PPPoA klient <input checked="" type="radio"/> Zapnut <input type="radio"/> Vypnut	
Nastavenie DSL modemu	
Multi-PVC kanal	Channel 1
VPI	1
VCI	32
Typ zapuzdrenia	LLC/SNAP
Protokol	PPPoE
Modulacia	G.DMT
PPPoE prechod	
<input type="checkbox"/> Pre drotovú LAN <input type="checkbox"/> Pre bezdrotovú LAN	
Nastavenie poskytovateľa (ISP)	
Meno poskytovateľa	
Užívateľské meno	
Heslo	
PPP overovanie	PAP alebo CHAP
<input checked="" type="checkbox"/> Vždy zapnutý	
Odpojiť po	-1 sec.(s)
IP adresa od poskytovateľa WAN IP Alias	
Pevná IP	<input type="radio"/> Áno <input checked="" type="radio"/> Nie (Dynamická IP)
Pevná IP adresa	
* : Vyzadovane niektorými ISP poskytovateľmi <input checked="" type="radio"/> Standardná MAC adresa <input type="radio"/> Specifikovať MAC adresu MAC adresa : 00 . 50 . 7F : D8 . ED . F1	
Index(1-15) v Planovaci Nastavene: , , , ,	

OK

PPPoE/PPPoA klient Kliknite na Enable (umožniť) aby ste aktivovali túto funkciu. Ak kliknete na Disable (znemožniť), táto funkcia sa uzavrie a všetky nastavenia ktoré ste upravili budú neplatné.

Nastavenie DSL modemu Nastavte parametre DSL požadované vaším poskytovateľom IS. Sú nevyhnutné na spustenie pripojenia DSL s vaším poskytovateľom IS.

Multi-PVC kanal tu zobrazené voľby sú určené stránkou Internet Access – Multi PVCs (prístup na Internet – Multi PVC's). Ak zvolíte M-PVCs Channel, znamená to že žiadne možnosti nebudú zvolené.

VPI Zadať hodnoty poskytnuté poskytovateľom IS.

VCI Zadať hodnoty poskytnuté poskytovateľom IS.

Typ zapuzdrenia Otvorte zoznam a zvolte typ určený poskytovateľom IS.

Protokol Otvorte zoznam a zvolte typ určený poskytovateľom IS. Ak ste už nastavili protokol v Quick Start Wizarde, nie je nutné meniť nastavenia v tejto skupine.

Modulacia Otvorte zoznam a zvolte typ určený poskytovateľom IS

PPPoE Prechod Router ponúka pripojenie PPPoE dial-up. Navyše môžete zriadiť spojenie PPPoE priamo od miestnych klientov s poskytovateľom IS prostredníctvom routeru Vigor.

Pre drotovú LAN Ak zaštrnete toto pole, PC v tej istej sieti môže použiť ďalšie PPPoE session (iné ako hostiteľské PC), aby sa pripojilo na Internet.

Pre bezdrotovú LAN Ak zaštrnete toto pole, PC v tej istej sieti môže použiť bezdrátové PPPoE session (iné ako hostiteľské PC), aby sa pripojilo na Internet.

Nastavenie poskytovateľa zadajte vaše užívateľské meno, heslo a autentifikačné parametre na základe informácií od poskytovateľa IS. Ak chcete byť pripojení k internetu trvale, zaškrtnite možnosť Vždy zapnutý.

Meno poskytovateľa Zadajte ISP Name určené poskytovateľom ISP.

Užívateľské meno Zadajte užívateľské meno poskytnuté poskytovateľom IS.

Heslo Zadajte heslo poskytnuté poskytovateľom IS.

PPP overovanie Zvoľte iba PAP alebo PAP alebo CHAP pre PPP.

Vždy zapnutý Zaškrtnite ak chcete aby bol router pripojený trvale k Internetu.

Odpojit po Zvoľte interval v sekundách, po ktorom sa odpojí router od Internetu ak je spojenie nečinné.

IP adresa poskytovateľa Poskytovateľ IS zvyčajne určuje IP adresu dynamicky pri každom pripojení. V niektorých prípadoch môže poskytovateľ IS určiť vždy rovnakú IP adresu, ak to požadujete. V tomto prípade môžete zadať IP adresu do pol'a Pevna IP adresa. Ak chcete využívať túto funkciu, kontaktujte svojho poskytovateľa IS.

Pevna IP adresa Kliknite na Ano ak chcete využívať funkciu Pevna IP.

WAN IP Alias ak máte hromadnú verejnú IP adresu a radi by ste ju využili na rozhraní WAN siete, použite WAN IP alias. Môžete nastaviť rozličných 8 IP adries.

http://192.168.1.1 - WAN IP Alias - Microsoft Internet Expl...

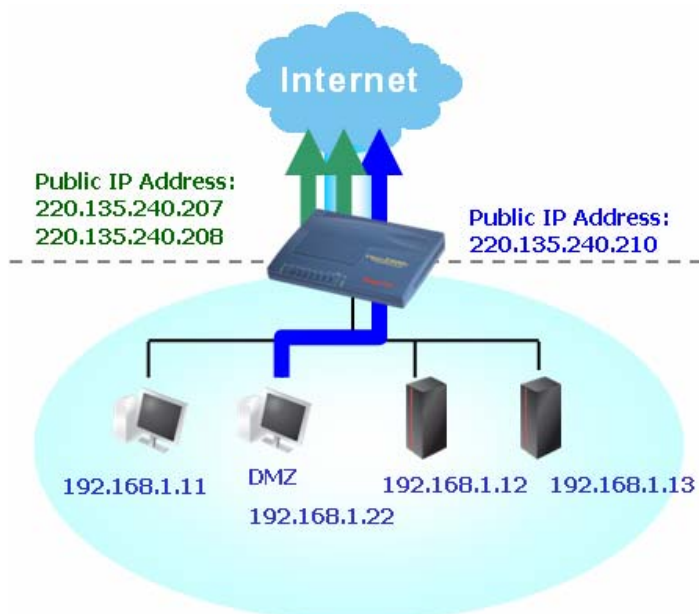
WAN IP Alias (Multi-NAT)

Index	Zapnut	Pridana WAN IP	Pripojiť IP k NAT
1.	<input checked="" type="checkbox"/>	62.65.169.134	<input checked="" type="checkbox"/>
2.	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="checkbox"/>
3.	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="checkbox"/>
4.	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="checkbox"/>
5.	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="checkbox"/>
6.	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="checkbox"/>
7.	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="checkbox"/>
8.	<input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="checkbox"/>

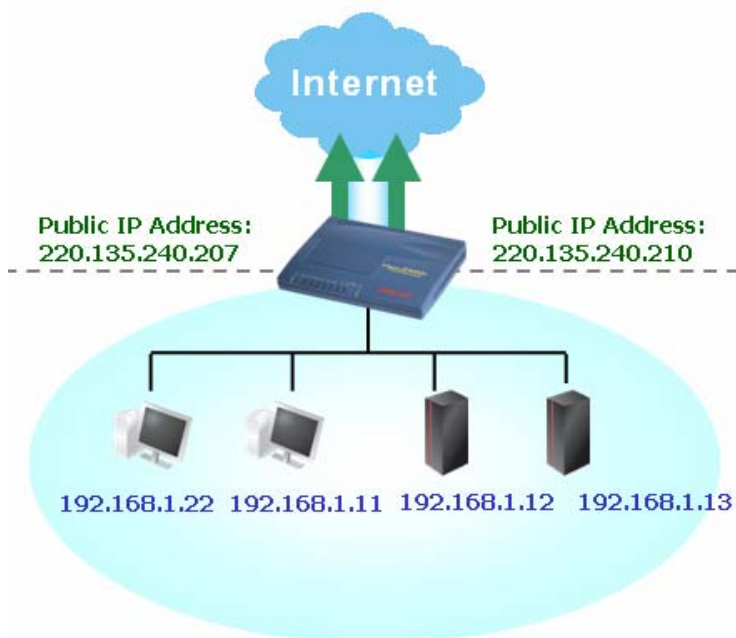
OK Vymazať Zavrieť

Hotovo Internet

Zaškrtnutím políčka Pripojiť IP k NAT, dáta z NAT hostiteľov budú preposlané na báze session.



Ak políčko **Pripojiť IP k NAT** nezaškrtnete, stále môžete tieto verejné IP adresy použiť na iné účely ako napr. DMZ host alebo Open Ports.



Standardná MAC adresa Zadajte MAC adresu pre router. Môžete použiť Prednastavenú MAC adresu, alebo upresniť inú MAC adresu ak potrebujete.

MAC adresa – Zadajte MAC adresu manuálne.

Index (1-15) v Planovací Nastavenie: môžete zadať štyri časové údaje podľa potreby. Všetky nastavenia musia byť nastavené predtým na stránke Aplikácie – Planovac.

Po dokončení všetkých nastavení, kliknite prosím na OK, aby ste ich aktivovali.

3.1.3 MPoA

MPoA je špecifikácia, ktorá umožňuje službám ATM, aby boli integrované do existujúcej miestnej siete, ktorá využíva ethernet, token-ring alebo TCP/IP protokol. Cieľom je umožniť miestnym sieťam na rozličných základoch posilať pakety prostredníctvom ATM.

Aby ste zvolili MPoA ako prístupový protokol, zvolte prosím MPoA z menu Prístup do internetu. Zobrazí sa nasledujúca stránka:

MPoA (RFC1483/2684) Mod

MPoA (RFC1483/2684) <input type="radio"/> Zapnut <input checked="" type="radio"/> Vypnut	
Nastavenie DSL modemu Multi-PVC kanal <input type="button" value="Select M-PVCs kanal"/>	
Zapuzdrenie <input type="button" value="1483 Routed IP LLC"/>	
VPI	<input type="text" value="1"/>
VCI	<input type="text" value="32"/>
Modulacia	<input type="button" value="G.DMT"/>
RIP protokol <input type="checkbox"/> Aktivovat RIP	
Bridge Mode <input type="checkbox"/> Aktivovat Bridge Mode	
Nastavenie WAN IP siete <input type="radio"/> Ziskat IP adresu automaticky Meno routra <input type="text"/> * Meno domeny <input type="text"/> * <input checked="" type="radio"/> Specifikovat IP adresu <input type="button" value="WAN IP Alias"/> IP adresa <input type="text" value="0.0.0.0"/> Maska podsiete <input type="text" value="0.0.0.0"/> IP adresa brany <input type="text"/> <hr/> * : Pozadovane niektorými poskytovateľmi <input checked="" type="radio"/> Standardna MAC adresa <input type="radio"/> Specifikovat MAC adresu MAC adresa : <input type="text" value="00"/> . <input type="text" value="50"/> . <input type="text" value="7F"/> : <input type="text" value="D8"/> . <input type="text" value="ED"/> . <input type="text" value="F1"/> <hr/> IP DNS servra Primarna IP adresa <input type="text"/> Sekundarna IP adresa <input type="text"/>	

OK

MPoA (RFC1483/2684)	Kliknite na Zaonut aby ste aktivovali túto funkciu. Ak kliknete na Vypnut, funkcia bude uzavretá a všetky nastavenia neplatné.
Nastavenia DSL modemu	Nastavte DSL parametre požadované poskytovateľom IS. Sú nevyhnutné na vybudovanie DSL pripojenia k vášmu poskytovateľovi IS.
Multi-PVC kanal:	tieto možnosti sú determinované stránkou Pripojenie do internetu – Multi PVC.
Multi PVC kanal	znamená, že ani jedna možnosť nebude zvolená.
Zapuzdrenie	Otvorte zoznam a zvolte typ určený poskytovateľom IS.
VPI	Zadajte hodnoty poskytnuté poskytovateľom IS.
VCI	Zadajte hodnoty poskytnuté poskytovateľom IS.
Modulacia	Zadajte hodnotu poskytnuté poskytovateľom IS.
RIP protokol	Routing Information Protocol(RFC1058) špecifikuje ako si routre vymieňajú informácie. Kliknite na Aktivovat RIP, ak chcete aktivovať túto funkciu.
Bridge Mode	Ak zvolíte protokol Bridged IP, zaškrtnite toto políčko na spustenie tejto funkcie. Router bude pracovať ako bridge modem.
Nastavenie WAN IP siete:	Táto skupina vám umožňuje získať automaticky IP adresu alebo ju zadať manuálne.
Ziskat IP adresu automaticky	Zakliknite toto tlačítko, aby ste získali IP adresu automaticky.
Meno routra	Zadajte meno routera určené poskytovateľom IS.

Meno domeny zadajte názov vašej domény.

WAN IP Alias ak máte hromadne IP adresy a radi by ste ich využili na rozhraní WAN siete, použite prosím WAN IP Alias. Môžete nastaviť 8 rôznych IP adries.

Index	Zapnut	Pridana WAN IP	Pripojiť IP k NAT
1.	v	62.65.169.134	v
2.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
3.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
4.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
5.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
6.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
7.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
8.	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>

OK Vymazať Zavrieť

Hotovo Internet

Standardna MAC adresa Zadajte MAC adresu pre router. Môžete použiť Prednastavenú MAC adresu, alebo upresniť inú MAC adresu ak potrebujete.

MAC adresa Zadajte MAC adresu manuálne.

DNS Server IP Zadajte primárnu IP adresu routera. Ak je to potrebné, zadajte pre prípadnú potrebu v budúcnosti aj sekundárnu IP adresu.

Po dokončení všetkých nastavení, kliknite prosím na OK, aby ste ich aktivovali.

3.1.4 MULTI - PVC

Router Vigor umožňuje vytvorenie multi-PVC na využívanie rôznych prenosov dát. Jednoducho choďte na stránku Prístup do internetu a zvolíte Multi-PVC. Systém umožňuje nastavenie ôsmich kanálov, ktoré možno nastaviť ako prvú PVC linku, ktorá bude slúžiť ako multi-PVC.

Multi-PVC

Hlavne		Bridge				
Kanal	Zapnuty	VPI	VCI	Typ QoS	Protokol	Zapuzdrenie
1.	<input checked="" type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="32"/>	UBR <input type="button" value="v"/>	PPPoE <input type="button" value="v"/>	<input type="text" value="LLC/SNAP"/> <input type="button" value="v"/>
2.	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="33"/>	UBR <input type="button" value="v"/>	MPoA <input type="button" value="v"/>	<input type="text" value="1483 Bridged IP LLC"/> <input type="button" value="v"/>
3.	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="34"/>	UBR <input type="button" value="v"/>	PPPoE <input type="button" value="v"/>	<input type="text" value="LLC/SNAP"/> <input type="button" value="v"/>
4.	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="35"/>	UBR <input type="button" value="v"/>	PPPoE <input type="button" value="v"/>	<input type="text" value="LLC/SNAP"/> <input type="button" value="v"/>
5.	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="36"/>	UBR <input type="button" value="v"/>	PPPoE <input type="button" value="v"/>	<input type="text" value="LLC/SNAP"/> <input type="button" value="v"/>
6.	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="37"/>	UBR <input type="button" value="v"/>	PPPoE <input type="button" value="v"/>	<input type="text" value="LLC/SNAP"/> <input type="button" value="v"/>
7.	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="38"/>	UBR <input type="button" value="v"/>	PPPoE <input type="button" value="v"/>	<input type="text" value="LLC/SNAP"/> <input type="button" value="v"/>
8.	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="39"/>	UBR <input type="button" value="v"/>	PPPoE <input type="button" value="v"/>	<input type="text" value="LLC/SNAP"/> <input type="button" value="v"/>

Poznámka: VPI/VCI musí byť unikátne pre každý kanál!

OK Vymazať Zrušiť

Zapnuty

Zaškrtnite toto políčko aby ste povolili kanál. Kanály, ktoré sú tu povolené, budú zobrazené v menu Multi-PVC na stránke Prístup do internetu. Aj keď tu môžete povoliť osem kanálov, na stránke Prístup do internetu môžete zvoliť len jeden.

VPI

Zadajte hodnoty od poskytovateľa IS.

VCI

Zadajte hodnoty od poskytovateľa IS.

QoS Type

Vyberte si patričný typ QoS.

Typ QoS

UBR

UBR

CBR

ABR

nrtVBR

rtVBR

Protokol

vyberte si patričný protokol pre daný kanál.

Zapuzdrenie

vyberte si patričný typ pre daný kanál. Na základe nastavení protokolu budú typy rozličné.

Protokol

PPPoE

PPPoA

PPPoE

MPoA

Zapuzdrenie

LLC/SNAP

VC MUX

LLC/SNAP

Zapuzdrenie

1483 Bridged IP LLC

1483 Bridged IP LLC

1483 Route IP LLC

1483 Bridged IP VC-Mux

1483 Routed IP VC-Mux(IPoA)

1483 Bridged IP(IPoE)

Všeobecná stránka vám umožní nastaviť prvý PVC. Pre nastavenie druhého PVC, kliknite na Bridge. Otvorí sa stránka konfigurácie Bridge.

Multi-PVC

Hlavne	Bridge					
Kanal	Zapnuty	P1	P2	P3	P4	
1.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
7.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
8.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Poznámka: 1. Kanal 1 az 4 su rezervovane pre pouzitie Nat/Route.

2. P1 je rezervovany pre pouzitie Nat/Route.

OK Vymazat Zrusit

Zapnuty

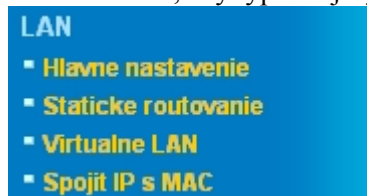
Zaškrtnite toto políčko aby ste povolili tento kanál. Môžu byť povolené len kanály 5-8, pretože kanály 1-4 sú rezervované pre používanie NAT.

P1 až P4

sú porty miestnej siete. Zaškrtnite políčko, aby ste vyhradili port pre kanál 5-8. Ak kliknete na Vymazat, vymažete všetky nastavenia na stránke. Keď dokončíte konfiguráciu kliknite na OK, aby ste uložili nastavenia a opustili stránku alebo Zrusit, aby ste prerušili konfiguráciu a opustili stránku.

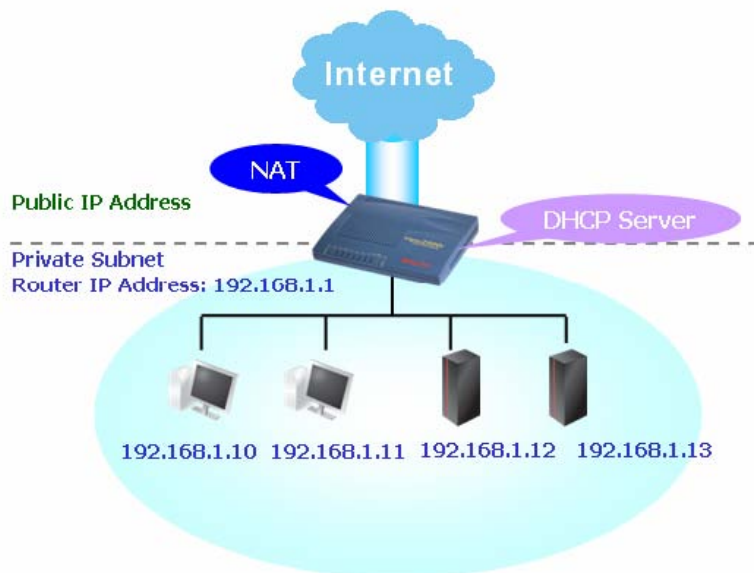
3.2 LAN

Local Area Network (miestna sieť - LAN) je skupina podsietí riadená a regulovaná routerom. Určenie štruktúry siete závisí od toho, aký typ verejnej IP adresy vám poskytuje poskytovateľ IS.

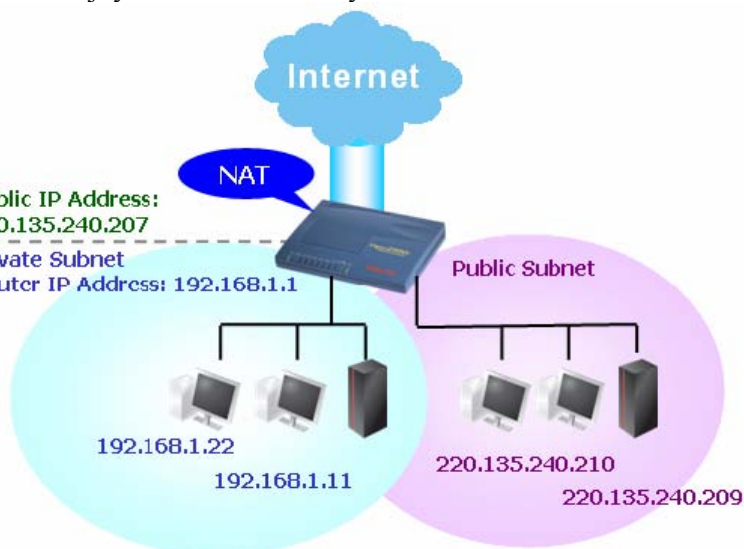


3.2.1 Základy LAN

Najbežnejšia funkcia routera Vigor je NAT. Vytvára vašu súkromnú sieť. Router komunikuje s verejnými hosťami pomocou verejnej IP adresy a miestnymi hosťami prostredníctvom súkromnej IP adresy. Prekladá a preposiela pakety hosťovi a od hosťa. Pritom má i zabudovaný DHCP server, ktorý priradzuje súkromnú IP adresu každému miestnemu hosťovi, viď diagram.



Vo výnimočných prípadoch môžete mať verejnú IP sieť od poskytovateľa IS ako napríklad 220.135.240.0/24. To znamená, že si môžete nastaviť verejnú podsieť, príp. druhú podsieť, v ktorej má každý hostiteľ svoju verejnú IP adresu. V tomto prípade slúži router Vigor na routovanie IP adries, aby pomáhal hostiteľom v tejto sieti komunikovať s inými verejnými hostiteľmi. Za tým účelom bude slúžiť ako brána pre verejných hostiteľov.



Čo je Routing Information Protokol (RIP)

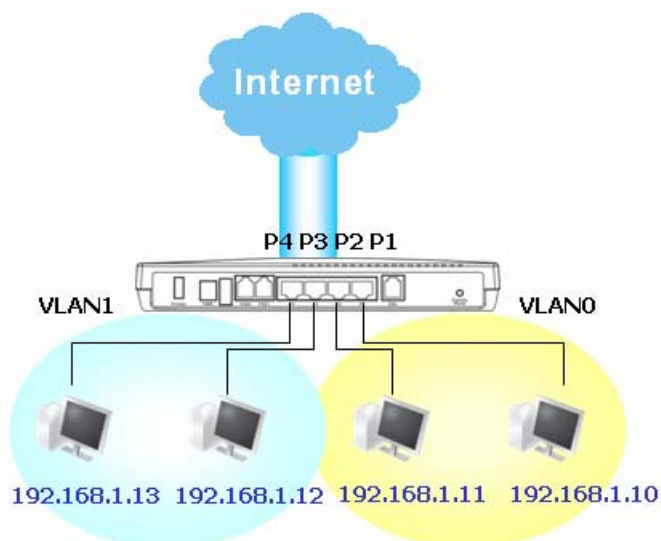
Router Vigor používa RIP na routovanie IP výmenou routovacích informácií so susediacimi routrami. Toto umožňuje užívateľom zmeniť napr. IP adresu a route sa informujú o zmene navzájom.

Čo je Staticke routovanie

Ak máte niekoľko podsietí vo vašej LAN, môže byť efektívnejšie a rýchlejšie spojiť ich prostredníctvom Staticke routovanie. Jednoducho nastavíte pravidlo preposielania dát z určitej podsiete do druhej bez prítomnosti RIP.

Čo sú Virtualne LAN

Môžete vytvoriť skupinu miestnych hostiteľov prostredníctvom fyzických portov a vytvoriť až štyri virtuálne LAN. Aby ste riadili komunikáciu medzi skupinami, nastavíte pravidlo vo funkcii Virtual LAN (VLAN) a ich rýchlosť.



3.2.2 Hlavne nastavenie

Táto stránka poskytuje všeobecné nastavenia LAN. Kliknite na LAN aby ste otvorili stránku pre nastavenia LAN a zvolte Hlavne nastavenie.

[LAN >> Hlavne nastavenie](#)

Ethernet TCP / IP a DHCP nastavenie

Konfiguracia LAN IP siete	Konfiguracia DHCP servra
Pre NAT pouzitie	<input checked="" type="radio"/> Aktivovat server <input type="radio"/> Deaktivovat server
1st IP Adresa <input type="text" value="192.168.1.1"/>	Relay Agent: <input type="radio"/> 1. podsiet <input type="radio"/> 2. podsiet
1st Maska podsiete <input type="text" value="255.255.255.0"/>	Start IP adresa <input type="text" value="192.168.1.10"/>
Pre pouzitie IP routovania <input type="radio"/> Zapnut <input checked="" type="radio"/> Vypnut	Pocet pridelenych IP <input type="text" value="50"/>
2. IP adresa <input type="text" value="192.168.2.1"/>	IP adresa brany <input type="text" value="192.168.1.1"/>
Maska 2. posiete <input type="text" value="255.255.255.0"/>	IP DHCP servra pre Relay Agent <input type="text"/>
<input type="button" value="DHCP Server 2.podsiete"/>	
Riadenie RIP protokolu <input type="text" value="Vypnut"/>	IP pre DNS server
	Primarna IP adresa <input type="text"/>
	Sekundarna IP adresa <input type="text"/>

1st IP adresa	Zadajte súkromnú IP adresu aby ste sa pripojili k miestnej sieti (predvolená je 192.168.1.1).
1st Maska podsiete	Zadajte kód adresy, ktorý určuje veľkosť siete (predvolený je 255.255.255.0/ 24)
Pre pouzitie IP routovania	Kliknite na Zapnut aby ste spustili túto funkciu. Predvolená je možnosť Vypnut.
2 IP adresa	Zadajte sekundárnu IP adresu pre pripojenie do podsiete (predvolená je 192.168.2.1/ 24)
Maska 2. podsiete	Zadajte kód adresy, ktorý určuje veľkosť siete (predvolený je 255.255.255.0/ 24)
DHCP server 2. podsiete	Môžete nakonfigurovať router aby slúžil ako DHCP server pre druhú podsieť.

Sekundarný DHCP server

Pociatocna IP adresa	<input type="text"/>
Pocet pridelenych IP	<input type="text" value="0"/> (max. 10)

Index	Zhodne MAC adresy	Pridelena IP adresa

MAC adresa : : : : : :

Pociatocna IP adresa: Zadaťte IP adresu do poľa, aby DHCP server začal pridelať IP adresy. Ak je druhá IP adresa routera 220.135.240.1, počiatočná IP adresa musí byť 220.135.240.2 a vyššie, ale menej ako 220.135.240.254.

Pocet pridelenych IP: Zadaťte počet pridelených IP adries. Maximum je 10. Príklad: ak zadáte 3 a druhá IP adresa routera je 220.135.240.1, rozsah IP adries bude od 220.135.240.2 do 220.135.240.4.

MAC adresa: Zadaťte MAC adresu hostiteľa a kliknite na Pridat aby ste vytvorili zoznam hostiteľov, ktorých IP adresa má byť pridelená, zmenená alebo vymazaná. Nastavte zoznam MAC adries. Druhý DHCP server pomôže routeru priradiť správne IP adresy správnym podsietiam a správnym hostiteľom, takže hostelia v druhej podsieti nedostanú pridelené adresy náležiacie hostiteľom v prvej podsieti.

Riadenie RIP protokolu Vypnut deaktivuje RIP protokol. To vedie k zastaveniu výmeny routovacích informácií medzi routermi.

Vypnut

Vypnut

1. podsiet

2. podsiet

1. podsiet router bude vymieňať informácie medzi prvou podsietou a susednými routermi.
 2. podsiet router bude vymieňať informácie medzi druhou podsietou a susednými routermi.

Konfigurácia DHCP servra

DHCP je skratka pre Dynamic Host Configuration Protocol. Pri firemných nastaveniach routera router slúži ako DHCP server. Automaticky oznamuje súvisiace IP nastavenia každému miestnemu užívateľovi, ktorý je nastavený ako DHCP klient. Ak nemáte v sieti DHCP server, je doporučené povoliť routeru slúžiť ako DHCP server. Ak máte iný DHCP server v sieti, môžete umožniť funkcii Relay Agent pomôcť presmerovať požiadavky DHCP do určených umiestnení:

Aktivovat server	Umožní routeru pridelit IP adresu každému hostiteli v LAN
Deaktivovat server	Umožní vám priradiť IP adresy manuálne.
Relay Agent	(1. podsiet/2. podsiet) určite ktorej podsieti budú zasielané DHCP požiadavky.

Start IP adresa Počiatočná IP adresa -.zadajte hodnotu prvej adresy z rozsahu IP adries, ktoré bude DHCP server. Ak je prvá IP adresa 192.168.1.1, počiatočná musí byť 192.168.1.2 a vyššie ale menej ako 192.168.1.254.

Pocet pridelených IP zadajte maximum počtu priradovaných IP adries. Predvolených je 50 a maximum je 253.

IP adresa brany Zadajte IP adresu brány. Je rovnaká ako IP adresa routra, čo znamená že router je predvolená brána.

IP DHCP servra pre Relay Agent – Nastavte IP adresu DHCP servera, ktorú použijete, takže Relay Agent vám pomôže preposielať požiadavky serveru.

IP pre DNS server (konfigurácia DNS servera)

DNS znamená Domain Name System. Každý Internetový hositeľ musí mať jedinečnú IP adresu a tá musí mať človeku čitateľné a zapamätateľné meno ako napr. www.yahoo.com. DNS server konvertuje užívateľské meno na ekvivalentnú IP adresu.

Primarna IP adresa Musíte špecifikovať IP adresu DNS serveru, pretože poskytovateľ IS by vám mal poskytnúť viac než jeden DNS server. Ak ich poskytovateľ neposkytne, router automaticky použije predvolenú IP adresu DNS servra 194.109.6.66.

Sekundarna IP adresa Môžete špecifikovať IP adresu DNS serveru, pretože poskytovateľ IS by vám mal poskytnúť viac než jeden DNS server. Ak ich poskytovateľ neposkytne, router automaticky použije predvolenú IP adresu DNS servra 194.98.0.1.

Predvolená IP adresa DNS servera môže byť nájdená prostredníctvom Online stavu: ak pole aj pre primárnu aj sekundárnu IP adresu je prázdne, router priradí svoju vlastnú IP adresu miestnym užívateľom akko DNS proxy server a použije DNS cache.

Systemový stav

Čas od spustenia systému: 0:3:3

LAN stav		Primárny DNS: 195.12.128.1	Sekundárny DNS: 195.72.0.3
IP adresa	TX Pakety	RX pakety	
192.168.1.1	51	0	

Ak IP adresa domény už je v DNS cache, router okamžite rozlíši názov domény. V opačnom prípade prepošle router DNS paket externému DNS serveru pripojením sa na WAN.

3.2.3 Statické routovanie

Chodíte na LAN aby ste otvorili stránku nastavení a zvolíte Staticke routovanie

[LAN >> Nastavenie statickeho routovania](#)

Staticke routovanie

[Zobrazit routovaci tabulku](#)

Index	Cielova adresa	Stav	Index	Cielova adresa	Stav
1.	???	?	6.	???	?
2.	???	?	7.	???	?
3.	???	?	8.	???	?
4.	???	?	9.	???	?
5.	???	?	10.	???	?

Stav: v --- Aktivne, x --- Neaktivne, ? --- Prazdne

Index Čísla 1-10 v stĺpci Index umožňujú otvoriť stránku nastavenia statickej cesty.

Cielova adresa Zobrazuje adresu destinácie statickej cesty.

Stav Zobrazuje stav statického routovania.

Index cis. 1

Stav/Akcia	Aktivne/Pridat
Cielova IP adresa	192.168.10.0
Maska podsiete	255.255.255.0
IP adresa brany	192.168.1.2
Sietove rozhranie	LAN

OK

zrusit

Diagnosticke nastroje >> Zobrazit routovaci tabulku

Aktualna routovacia tabulka

Obnovit

Key: C - connected, S - static, R - RIP, * - default, ~ - private			
*	0.0.0.0/	0.0.0.0	via 195.72.7.1, IF3
S~	192.168.10.0/	255.255.255.0	via 192.168.1.2, IFO
C~	192.168.1.0/	255.255.255.0	is directly connected, IFO
S~	211.100.88.0/	255.255.255.0	via 192.168.1.3, IFO

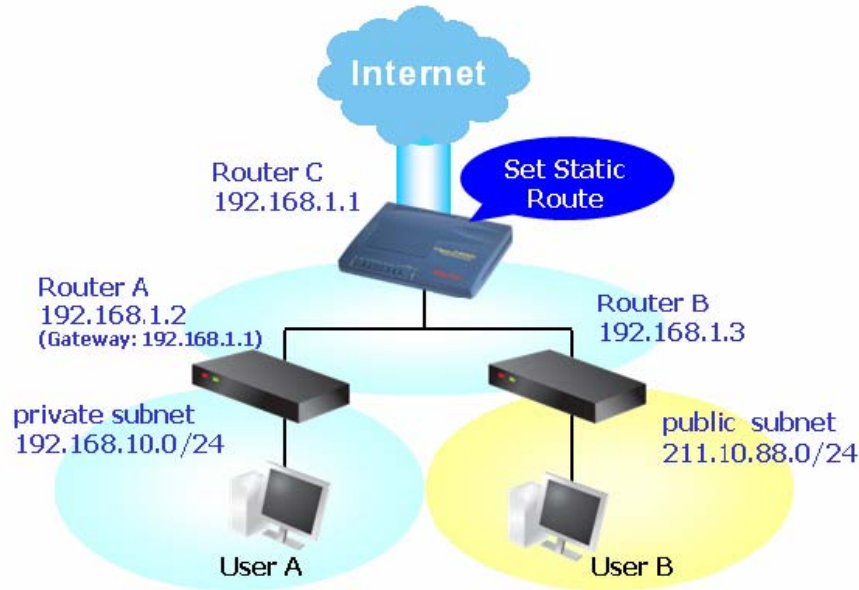
Pridajte statické cesty do súkromných a verejných sietí

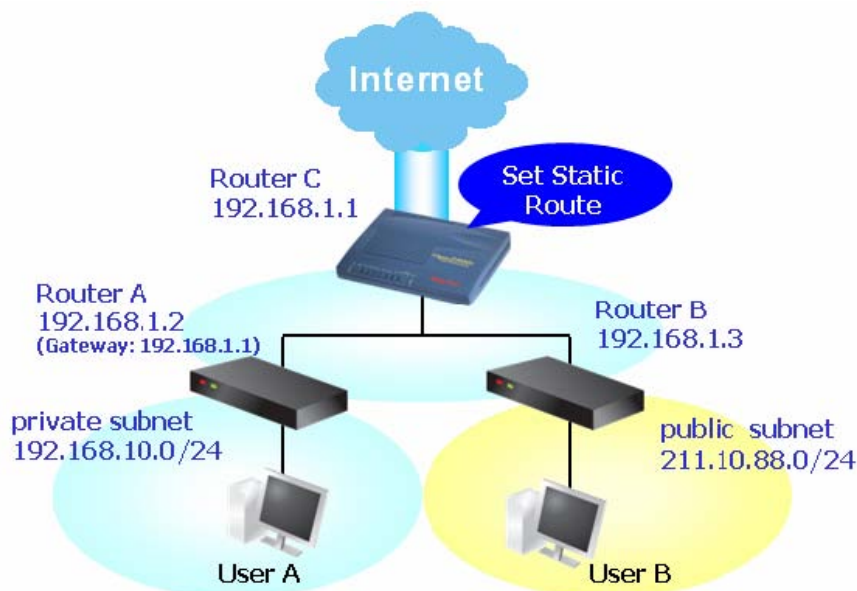
Tu je príklad nastavenia statickej cesty v hlavnu routery, tak že užívatelia A a B môžu spolu komunikovať z dvoch rozličných podsietí prostredníctvom routera za predpokladu, že prístup na internet je riadne nastavený a router správne pracuje.

- z Použite hlavný router na surfovanie na internete.
- z Vytvorte súkromnu podsieť 192.168.10.0 za použitia interného routera A (192.168.1.2)
- z Vytvorte verejnú podsieť 211.100.88.0 prostredníctvom interného routera B (192.168.1.3).

z Nastavte hlavný router 192.168.1.1 ako predvolenú bránu pre router A 192.168.1.2.

Kým nastavíte statickú cestu, užívateľ A nemôže komunikovať s užívateľom B, pretože router A môže preposielať rozpoznané pakety hlavnému routeru.





1. Chodíte na stránku LAN a kliknite na Hlavné nastavenie, zvolíte I. podsiet v menu Riadenie RIP protokolu. Potom kliknite na OK.

Poznámka: Použiť Riadenie RIP protokolu na prvej podsieti musíme z dvoch dôvodov. Po prvé rozhranie LAN môže vymieňať RIP pakety so susednými routami prostredníctvom prvej podsiete (192.168.1.0/24). Po druhé, hostelia na interných súkromných podsietach (192.168.10.0/24) majú prístup na Internet prostredníctvom routeru a kontinuálne vymieňajú routovacie informácie s rôznymi podsietami.

Kliknite na LAN – Statické routovanie a na Index cis. 1. Pridajte statickú cestu ako je znázornené nižšie. Tá zabezpečí že všetky pakety smerované na 192.168.10.0 budú presmerované na 192.168.1.2. Kliknite na OK.

Vráťte sa na stránku Nastavenie statickeho routovania. Kliknite na ďalšie číslo v stĺpci Index a pridajte ďalšiu statickú cestu ako je znázornené nižšie. Tá zabezpečí že všetky pakety smerované na 211.100.88.0 budú presmerované na 192.168.1.3.

LAN >> Nastavenie statickeho routovania

Index cis. 1

Stav/Akcja	Aktivne/Pridat
Cielova IP adresa	192.168.10.0
Maska podsiete	255.255.255.0
IP adresa brany	192.168.1.2
Sietove rozhranie	LAN

OK zrusit

LAN >> Nastavenie statickeho routovania

Index cis. 2

Stav/Akcja	Aktivne/Pridat
Cielova IP adresa	211.100.88.0
Maska podsiete	255.255.255.0
IP adresa brany	192.168.1.3
Sietove rozhranie	LAN

OK zrusit

4. Chodíte na Diagnostika a zvolíte Zobrazit routovaci tabulku aby ste overili terajšiu routovaci tabulku.

Aktualna routovacia tabuľka

[Obnovit](#)

Key: C - connected, S - static, R - RIP, * - default, ~ - private

```
*          0.0.0.0/          0.0.0.0 via 195.72.7.1, IF3
S~        192.168.10.0/      255.255.255.0 via 192.168.1.2, IF0
C~        192.168.1.0/       255.255.255.0 is directly connected, IF0
S~        211.100.88.0/      255.255.255.0 via 192.168.1.3, IF0
```

Zakázat Statické routování

Klikněte na číslo tej staického routování v slůpci Index, které chcete zakázat.
Zvolte z menu Neaktivne/Vypnute a klikněte na tlačítko OK.

Aktivne/Pridat
Prazdny/Vymazat
 Aktivne/Pridat
 Neaktivne/Vypnute

3.2.4. Virtualne LAN (VLAN)

Funkcia Virtualne LAN vám poskytuje veľmi výhodný spôsob, akko riadiť hostiteľov ich dávaním do skupín pomocou fyzických portov. Takisto môžete riadiť in/out prietok každého portu. Choďte do menu LAN a zvolte Virtualne LAN. Zobrazí sa nasledujúca stránka. Kliknite na Aktivovat, aby ste spustili funkciu Virtualne LAN.

Virtualne LAN (VLAN)

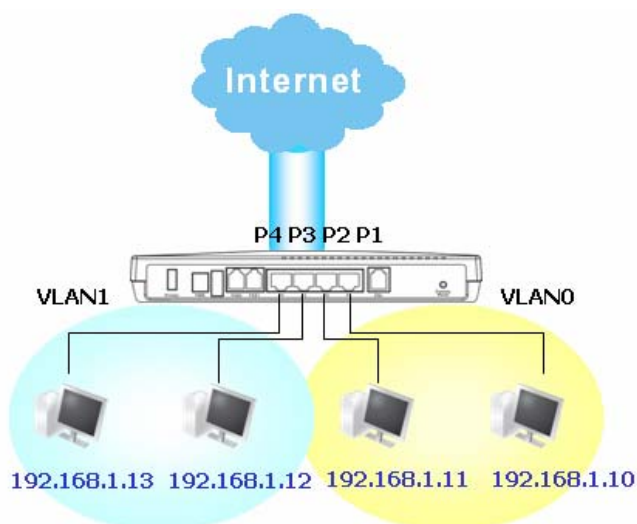
☒ Aktivovat

	P1	P2	P3	P4
VLAN0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK Vymazat Zrusit

Ak chcete pridať alebo odstrániť VLAN, urobte tak podľa nasledujúceho príkladu.

VLAN 0 pozostáva z hostiteľov pripojených na P1 a P2 a VLAN 1 pozostáva z hostiteľov pripojených na P3 a P4.



Po zaškrtnutí políčka Aktivovat zaškrtnete políčka v tabuľke podľa potreby ako na nasledujúcom obrázku.

Virtualne LAN (VLAN)

<input checked="" type="checkbox"/> Aktivovat				
	P1	P2	P3	P4
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Aby ste odstránili VLAN, zrušte zaškrtnutie políčok a kliknite na OK.

3.2.5 Spojit IP s MAC

Pomocou tejto funkcie je možné pridelovať DHCP servrom vždy tie isté IP adresy pre konkrétne MAC adresy, podľa zadefinovania v tomto okne

LAN >> Spojit IP adresu s MAC

Spojit IP adresu s MAC

Pozn: IP-MAC spojenie prestavi DHCP pridelenie.

Ak vyberiete striktné spojenie, nespecifikovani LAN klienti nemozu pristupovat do internetu.

☒ Zapnut ☐ Vypnut ☐ Striktne spojenie

ARP tabulka

[Oznacit vsetko](#)

[Zoradit](#)
[Obnovit](#)

Zoznam pripojenych IP

[Oznacit vsetko](#)
[Zoradit](#)

IP adresa	MAC adresa
192.168.1.10	00-12-F0-A0-E6-DB

Index	IP adresa	MAC adresa
-------	-----------	------------

Pridat a Upravit

IP adresa

MAC adresa

:::::

3.3 NAT

NAT

- Presmerovanie portov
- DMZ hostiteľ
- Otvorenie portov
- Zoznam portov

Zvyčajne router slúži ako NAT (Network Address Translation) router. NAT je mechanizmus, ktorý umožňuje že jedna alebo viac súkromných IP adries môžu byť zobrazené ako jedna verejná. Verejná IP adresa je zvyčajne priradená vašim poskytovateľom IS, za ktorú platíte. Súkromné IP adresy sú rozoznávané medzi internými hostiteľmi. Ak odchádzajúce pakety určené nejakému verejnému serveru na Internete dosiahnu NAT router, router zmení zdrojovú adresu na verejnú IP adresu routera, určí dosiahnuteľný verejný port a prepošle ho. Zároveň si zapíše do tabuľky vzťah adresy a portu. Ak verejný server odpovedá, prichádzajúce dáta sú nasmerované na verejnú IP adresu routera a router si to zapíše do vlastnej tabuľky. Preto interný hostiteľ môže ľahko komunikovať s vonkajším.

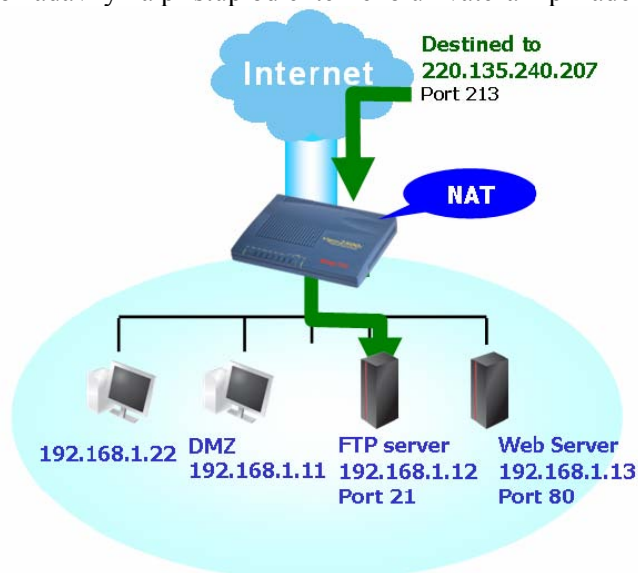
Výhody NAT:

- Šetrí náklady pri používaní verejných IP adries a zabezpečujú efektívne využívanie IP adries. NAT umožň/nuje internej IP adrese miestneho hostiteľa aby bola prekonvertovaná na verejnú, preto môžete mať pre všetkých interných hostiteľov jednu verejnú IP adresu.
- Zvyšuje bezpečnosť internej siete ukrytím IP adries. Mnoho útokov je smerovaných na IP adresy. Preto ak útočník nevidí IP adresy, interná sieť je zabezpečená.

Na stránke NAT sú súkromné IP adresy definované v RFC-1918. Zvyčajne používame pre router podsieť 192.168.1.0/24. Zariadenie NAT umožňuje spojiť jednu alebo viac IP adries a/alebo portov do rôznych služieb. Inými slovami, funkcia NAT môže byť dosiahnutá použitím metódami priradovania portov.

3.3.1 Presmerovanie portov

Presmerovanie portov je zvyčajne nastavená pre služby súvisiace so serverom vo vnútri miestnej siete, ako web servery, FTP servery, e-mailové servery atď. Vo väčšine prípadov potrebujete verejnú IP adresu pre každý server a táto IP adresa alebo názov domény sú známe všetkým užívateľom. V prípade, že server je umiestnený v miestnej sieti, chránený NAT routera a identifikovaný IP adresou alebo portom, úlohou tejto funkcie je presmerovať všetky požiadavky na prístup od externého užívateľa k priradeným IP adresám alebo portom na serveri.



Je možno ju použiť iba na prichádzajúce informácie

Aby ste použili túto funkciu, choďte na stránku NAT a zvolte Presmerovanie portov. Tabuľka ponúka desať vstupov na priradovanie portov pre interných hostiteľov.

NAT >> Configure Port Redirection Table

Port Redirection Table

Index	Service Name	Protocol	Public Port	Private IP	Private Port	Active
1	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
2	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
3	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
4	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
5	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
6	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
7	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
8	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
9	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
10	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>

OK

NAT >> Presmerovania portov

Tabuľka presmerovania portov

Index	Meno služby	Protokol	Verejný port	Privatná IP	Privatný port	Aktivne
1	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
2	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
3	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
4	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
5	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
6	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
7	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
8	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
9	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>
10	<input type="text"/>	--- <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="checkbox"/>

OK

Meno služby

Zadajte popis sieťovej služby.

Protokol

Zadajte protokol transportnej vrstvy(TCP alebo UDP).

Verejný port

Špecifikujte, ktorý port môže byť presmerovaný na určitú súkromnú IP adresu a port interného hostiteľa

Privatná IP

Špecifikujte súkromnú IP adresu interného hostiteľa poskytujúceho službu.

Privatný port

Špecifikujte číslo súkromného portu služby ponúkanej interným hostiteľom.

Aktivne

Zaškrtnite políčko aby ste aktivovali vami definované priradovanie portov.

Všimnite si, že router má zabudované vlastne služby (servery) ako Telnet, HTTP, FTP atď. Ak sú spoločné čísla portov týchto služieb (serverov), bude možno treba resetovať router, aby ste sa vyhli konfliktom. Napríklad zabudovaný web-konfigurator v routeri, ktorý má predvolený port 80, sa môže dostať do konfliktu s webovým serverom v miestnej sieti `http://192.168.1.13:80`. Preto je potrebné zmeniť http routeru na akékoľvek iné ako 80, aby sme sa vyhli konfliktu, ako napríklad 8080. Toto nastavenie možno vykonať v Správa systému >>>Spravovanie systému. Vstúpte na okno admin a pridáte príponu 8080, t.j. `http://192.168.1.1:8080` namiesto port 80.

Spravca systemu

Riadenie prístupu

- ☐ Aktivovať upgrade firmveru na diaľku(FTP)
- ☐ Povolit spravovanie z internetu
- ☒ Zakazat ping z internetu

Zoznam povolených prístupov

Zoznam	IP	Maska podsiete
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>

Nastavenie manažmentu portov

- ☐ Prednastavené porty (Telnet: 23, HTTP: 80, HTTPS: 443, FTP: 21)

- ☒ Užívateľom definované porty

Telnet Port	<input type="text" value="23"/>
HTTP Port	<input type="text" value="80"/>
HTTPS Port	<input type="text" value="443"/>
FTP Port	<input type="text" value="21"/>

SNMP nastavenie

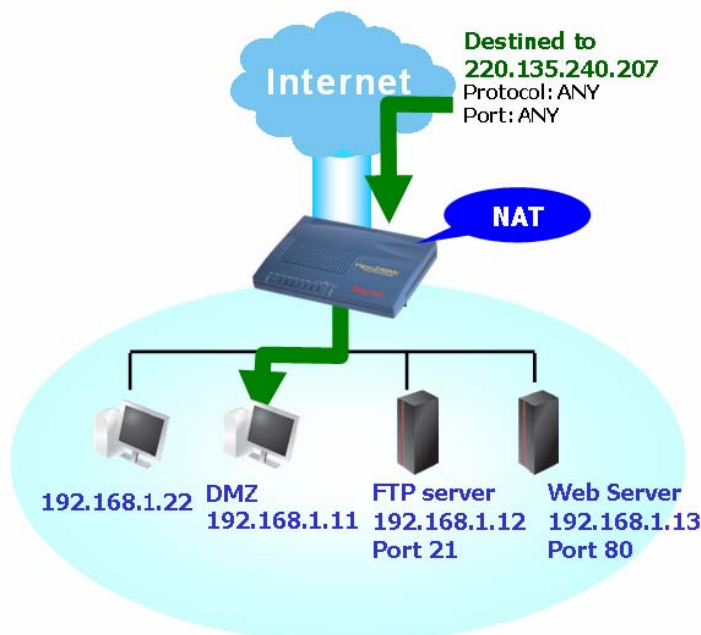
- ☐ Aktivovať SNMP Agent

Get Community	<input type="text" value="public"/>
Set Community	<input type="text" value="private"/>
Manager Host IP	<input type="text"/>
Trap Community	<input type="text" value="public"/>
Notification Host IP	<input type="text"/>
Trap Timeout	<input type="text" value="10"/> sec.

OK

3.2.3 DMZ hostiteľ

Ako bolo spomenuté, Presmerovanie portov môže presmerovať prichádzajúci TCP/UDP alebo iný prenos na konkrétnu súkromnú IP adresu alebo port hostiteľa v miestnej sieti. Ostatné IP protokoly, napríklad 50 (ESP) and 51 (AH) sa na pevnom porte nemenia. Router Vigor router poskytuje možnosť DMZ Host, ktorá priraduje všetky vyžiadané dáta akýmkoľvek protokolom jedinému portu miestnej siete. Bežné surfovanie po webe a podobné internetové aktivity budú nerušené fungovať. DMZ hostiteľ umožňuje definovanému internému užívateľovi byť viditeľný na internete, čo pomáha aplikáciám ako napríklad Netmeeting alebo hrám cez internet.



Ak nastavíte DMZ hostiteľ, čiastočne tým obídete bezpečnostné vlastnosti NAT. Navrhujeme pridať dodatočné pravidlá filtra a sekundárny firewall.

Kliknite na DMZ hostiteľ aby ste otvorili nasledujúcu stránku:

[NAT >> DMZ hostiteľ](#)

DMZ hostiteľ

Zapnutý

☐

Privatná IP

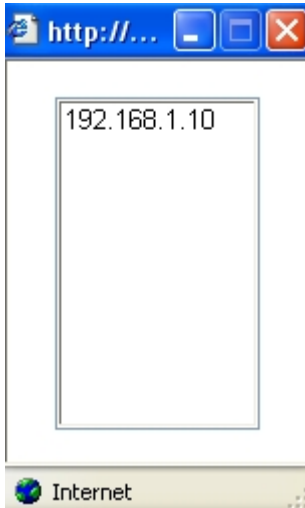
Vybrať PC

OK

Ak ste predtým nastavili WAN Alias v Prístup do internetu>>PPPoE/PPPoA alebo Prístup do internetu>>MPoA, najdete ich v Pripojene WAN IP adresy.

Zapnuty
Privatna IP
Vybrat PC

Zaškrtnite pre povolenie funkcie DMZ host.
Zadajte súkromnú IP adresu hostiteľa DMZ, alebo kliknite na Vybrat PC pre zvolenie. Kliknite na toto tlačítko a automaticky sa zobrazí okno aké vidíte nižšie. Skladá sa zo zoznamu súkromných IP adries všetkých hostiteľov vo vašej miestnej sieti. Zvoľte jednu z nich, ktorá bude hostiteľ DMZ.



Po tom ako ste zvolili jednu zo súkromných IP adries zobrazí sa na nasledujúcej stránke. Kliknite OK, aby ste uložili nastavenie.

3.3.3 Otvorenie skupiny portov

Otvorenie portov vám umožňuje otvoriť rozsah portov na prenos špeciálnych aplikácií. Spoločné aplikácie Open Ports zahŕňajú P2P aplikácie (ako napr. BT, KaZaA, Gnutella, WinMX, eMule a iné), webovú kameru a pod. Uistite sa, že udržiavate aplikáciu aktualizovanú, aby ste sa vyhli útoku na bezpečnosť vášho systému.

Kliknite na Otvorenie portov pre otvorenie nasledujúcej stránky:

[NAT >> Otvorenie skupiny portov](#)

Otvorenie skupiny portov

Index	Poznámka	Lokálna IP adresa	Stav
1.			x
2.			x
3.			x
4.			x
5.			x
6.			x
7.			x
8.			x
9.			x
10.			x

Vymazať

Index

Indikuje číslo pre konkrétny vstup, ktorého službu chcete vykonávať na miestnom hostiteľovi. Mali by ste kliknúť na konkrétne číslo, ak chcete upraviť alebo vymazať zodpovedajúce vstupy.

Poznámka

Upresní název definovanej sieťovej služby.

Pripojená WAN IP adresa

Zobrazí súkromnú IP adresu miestneho hostiteľa, ktorú určíte vo WAN Alias. Toto pole sa nezobrazí, ak ste neurčili žiadny Alias na stránke WAN Alias.

Lokálna IP adresa
Stav

Zobrazí súkromnú IP adresu miestneho hostiteľa vykonávajúceho službu.
Zobrazí stav zodpovedajúceho vstupu. X alebo V znamená Neaktívny alebo Aktívny.

Aby ste pridali alebo zmenili nastavenia portov, kliknite na indexové číslo na stránke. Zobrazí sa stránka nastavenia indexových vstupov. Pre každý vstup môžete určiť 10 rozsahov portov pre rôzne služby.

NAT >> Open Ports Setup >> Otvorenie skupiny portov

Index Cis. 1

☒ Aktivovať otvorenie skupiny portov

Poznamka

Lokálny počítač

	Protokol	Počiatkový Port	Konečný Port		Protokol	Počiatkový Port	Konečný Port
1.	TCP	4500	4700	6.	----	0	0
2.	UDP	4500	4700	7.	----	0	0
3.	----	0	0	8.	----	0	0
4.	----	0	0	9.	----	0	0
5.	----	0	0	10.	----	0	0

Ak ste už nastavili WAN Alias v Pripojenie do internetu>>PPPoE/PPPoA alebo Pripojenie do internetu >>MPoA, WAN IP bude medzi voľbami.

Aktivovať otvorenie skupiny portov Zaškrtnite, ak chcete povoliť tento vstup.

Poznamka Zadáajte názov definovanej sieťovej aplikácie/služby.

Lokálny počítač Zadáajte súkromnú IP adresu miestneho hostiteľa, alebo kliknite na Choose PC, ak si chcete zvoliť.

Vybrať PC Kliknite na toto tlačítko a automaticky sa zobrazí okno aké vidíte nižšie. Skladá sa zo zoznamu súkromných IP adries všetkých hostiteľov vo vašej miestnej sieti. Zvoľte jednu z nich, ktorá bude hostiteľ.

Protokol Určíte protokol transportnej vrstvy. Môže to byť TCP, UDP, alebo -----(žiaden).

Počiatkový Port Určíte počiatočné číslo portu vykonávajúceho službu na miestnom hostiteľovi.

Konečný Port Určíte konečné číslo portu vykonávajúceho službu na miestnom hostiteľovi.

Otvorenie skupiny portov

Index	Poznamka	. Pridana WAN IP	Lokalna IP adresa	Stav
1.	P2P	62.65.169.134	192.168.1.10	v
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x

Vymazať

3.3.4 Zoznam najbežnejších portov

Táto stránka vám poskytne prehľad známych portov.

[NAT >> Zoznam najbežnejších portov](#)

Zoznam najbežnejších portov

Služba/Aplikácia	Protokol	Cislo portu
File Transfer Protokol (FTP)	TCP	21
SSH Remote Login Protokol (ex. pcAnyWhere)	UDP	22
Telnet	TCP	23
Simple Mail Transfer Protokol (SMTP)	TCP	25
Domain Name Server (DNS)	UDP	53
WWW Server (HTTP)	TCP	80
Post Office Protokol ver.3 (POP3)	TCP	110
Network News Transfer Protokol (NNTP)	TCP	119
Point-to-Point Tunneling Protokol (PPTP)	TCP	1723
pcANYWHEREdata	TCP	5631
pcANYWHEREstat	UDP	5632
WinVNC	TCP	5900

3. 4 Firewall

Firewall

- Hlavné nastavenie
- Nastavenie filtrovania
- IM Blokovanie
- P2P Blokovanie
- DoS obrana
- URL obsahové filtrovanie

3.4.1 Základy pre firewall

Kým užívatelia širokopásmového internetu požadujú väčší prístup pre multimédiá, interaktívne aplikácie alebo diaľkové štúdium, najviac pozornosti si vyžaduje bezpečnosť. Firewall routera Vigor pomáha chrániť vašu miestnu sieť proti útokom neautorizovaných cudzích osôb. Okrem toho zamedzuje užívateľom v miestnej sieti pripojiť sa na Internet. Ďalej dokáže vyfiltrovať určité pakety, ktoré spúšťajú router, aby vybudoval neželané spojenie mimo siete. Najzákladnejší koncept bezpečnosti je nastavenie užívateľského mena a hesla pri inštalácii routera. Administrátorské prihlásenie zabráni neautorizovanej zmene nastavení routera.

Sprava systemu >> Nastavenie administratorskeho hesla

Heslo administratora

Stare heslo	<input type="password"/>
Nove Heslo	<input type="password"/>
Znovuzadanie noveho hesla	<input type="password"/>

OK

Príslušenstvo firewallu

Užívatelia na miestnej sieti sú chránení nasledovným príslušenstvom:

Užívateľom nastaviteľný IP filter (Call Filter/ Data Filter).

Stavova inspekcia paketov (SPI): vystopuje pakety a odmieta nežiadané dáta

Voliteľné Denial of Service (Odmietnutie služby - DoS) /Distributed DoS (distribúované DoS - DDoS) je obrana proti útokom

Filtrovanie obsahu URL

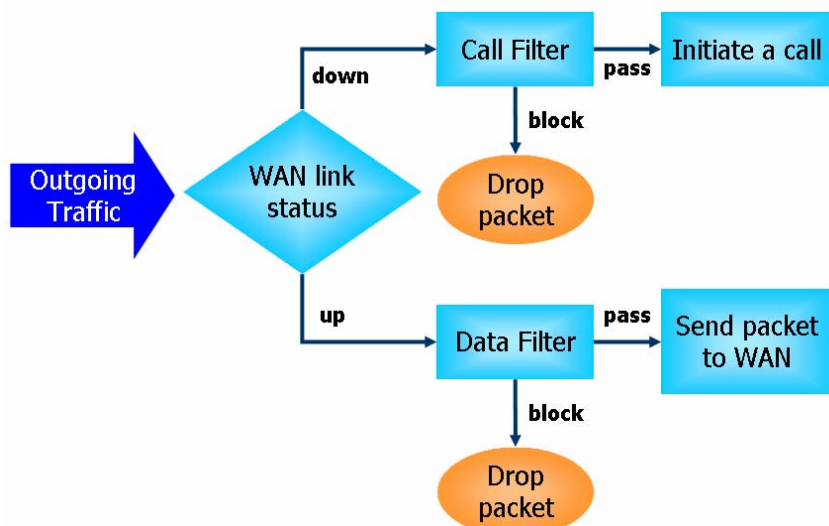
IP filtre

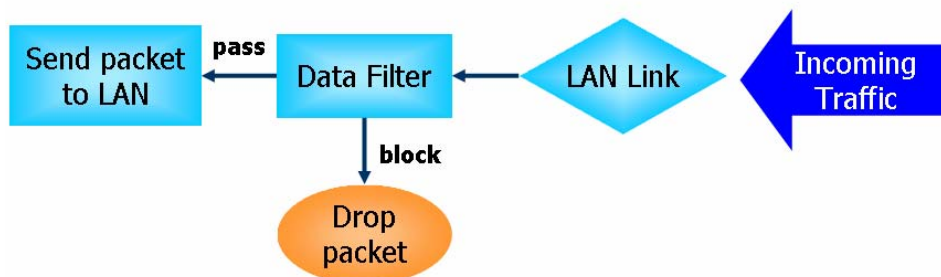
V závislosti na tom, či ste pripojení na Internet, inými slovami „WAN link status je UP alebo DOWN“, architektúra IP filtrov delí prenos dát do dvoch: Call filter (filter volaní) a Data filter (filter dát).

□ Call Filter –ak nie ste pripojení na Internet. Aplikuje sa na všetky odchádzajúce prenosy. Kontroluje odchádzajúce pakety. Ak sú dovolené, prejdú. Potom router iniciuje „volanie“ aby sa pripojil na Internet a pošle packet na Internet.

□ Data Filter – Pri pripojení na internet router kontroluje odchádzajúce i prichádzajúce pakety, ak je ich obsah povolený, prejdú routerom.

Takto pracuje router s prichádzajúcimi a odchádzajúcimi prenosmi.





Stateful Packet Inspection (SPI)

Stateful inspection (stavová inšpekcia) je architektúra firewallu, ktorá pracuje v sieťovej vrstve. Na rozdiel od legacy static packet filtering, ktoré kontroluje paket na základe hlavičky, stateful inspection kontroluje všetky pripojenia prebiehajúce cez akékoľvek rozhranie a uisťuje sa, že sú odôvodnené. Preto stavová inšpekcia routera Vigor nekontroluje len hlavičky paketov, ale monitoruje i stav pripojenia.

Blokovanie aplikácií Instant Messenger (IM) a Peer-to-Peer (P2P)

Ako rastie popularita týchto aplikácií, komunikácia už nemôže byť jednoduchšia. Napriek tomu, kým niektoré odvetvia prehlasujú tieto aplikácie za skvelé nástroje spojenia svojich zákazníkov, niektoré môžu mať rezervovanejší prístup, pretože potrebujú znížiť ich používanie počas pracovných hodín, prípadne eliminovať bezpečnostné medzery. Podobná situácia je pri zdieľaní súborov pomocou peer-to-peer aplikácií, ktoré je výhodné ale nebezpečné zároveň. Kvôli tomu ponúka router Vigor schopnosť blokovat' IM a P2P aplikácie.

Denial of Service (DoS) Defense (obrana pred zastavením prevádzky služieb)

DoS Defense pomáha detekovať a zmierniť útoky na prevádzku služieb. Obvykle sú delené na dva druhy – záplavové a poruchové. Záplavové útoky sa budú snažiť vyčerpať všetky systémové zdroje, kým poruchové sa budú snažiť paralyzovať systém útokom na poruchovosť protokolu alebo systému.

DoS Defense umožňuje routeru prehliadnuť každý prichádzajúci paket, ktorý má príznaky zhodné s paketmi v databáze znakov útoku. Každý zlomyseľný paket, ktorý by sa mohol duplikovať aby paralyzoval hostiteľa v bezpečnej miestnej sieti bude blokový a ako varovanie bude odoslaná správa Syslog, ak nastavíte server Syslog. Router Vigor takisto monitoruje prenos. Každý prenos, ktorý odporuje preddefinovaným parametrom, ako napríklad počet prahov, je identifikovaný ako útok a router aktivuje mechanizmy aby zmiernil útok v reálnom čase.

DoS/DDoS defense môže detekovať nasledujúce útoky:

- | | |
|-------------------|--------------------------|
| SYN flood attack | 9. Smurf attack |
| UDP flood attack | 10. SYN fragment |
| ICMP flood attack | 11. ICMP fragment |
| TCP Flag scan | 12. Tear drop attack |
| Trace route | 13. Fraggle attack |
| IP options | 14. Ping of Death attack |
| Unknown protocol | 15. TCP/UDP port scan |
| Land attack | |

Filtrovanie obsahu

Aby sme poskytli užívateľom primeraný virtuálny priestor, router Vigor je vybavený filtrom obsahu URL nielen aby obmedzil ilegálny prenos z a na nevhodné web stránky, ale obmedzuje aj iné webové súčasti, ktoré môžu obsahovať škodlivý kód.

Ak užívateľ zadá alebo klikne na URL s nevhodnými kľúčovými slovami, zariadenie na blokovanie kľúčových slov zamietne HTTP požiadavku na tú stránku a preto obmedzí prístup užívateľa. Môžete si predstaviť URL Content filter (filter obsahu URL) ako dobre vyškoleného predavača, ktorý nebude predávať týnedžerom časopisy pre dospelých.

V kancelárii poskytuje pracovné prostredie spojené len s výkonom práce a tým zvyšuje efektivitu práce pracovníkov. Ako môže URL Content Filter pracovať lepšie ako tradičný firewall? Pretože kontroluje reťazce URL alebo niektoré pakety HTTP, ktoré ukrývajú dáta, kým firewall prehliada iba pakety na základe TCP/IP hlavičky.

Na druhú stranu router Vigor zabráni užívateľom nechtiac sťahovať škodlivý kód z webovských stránok. Je zvyčajné, že škodlivé kódy skrývajú vo spustiteľných objektoch ako ActiveX, Java Applet, skomprimované súbory a iné spustiteľné súbory. Po stiahnutí týchto súborov je riziko ohrozenia systému. Napríklad prvky Active X sa používajú na vykonanie interaktívnych súčastí stránky. Ak skrývajú škodlivý kód, môže napadnúť užívateľov systém.

Filtrovanie webu

Všetci vieme že obsah internetu je ako všetky ostatné médiá a niekedy môže byť nevhodný. Ako zodpovedný rodič alebo zamestnávateľ by ste mali chrániť tých čo vám dôverujú pred nebezpečenstvom. So službou Web Filtering (filtrovanie webu) môžete chrániť vašu firmu pred ohrozeniami ako produktivita, legálna zodpovednosť, ohrozenia siete a bezpečnosti. Ako rodičia môžete chrániť vaše deti pred stránkami s obsahom pre dospelých.

Ak ste aktivovali službu Web Filtering v routeri Vigor a určili kategórie webovských stránok ktoré chcete zakázať, každá požadovaná URL (napr. www.bbc.co.uk) bude overená v našej databáze podporovanej SurfControl. Databáza pokrýva 70 rečí v 200 krajinách, asi miliardu webových stránok rozdelených do ľahko zrozumiteľných štyridsiatic kategórií. Je denne aktualizovaná globálnym tímom webových výskumníkov. Server vyhľadá URL a vráti routeru kategóriu. Ten sa potom rozhodne či prístup povolí alebo nie podľa kategórií, ktoré ste si určili. Všimnite si, že táto činnosť neovplyvní rýchlosť prehliadania stránok, pretože servery dokážu spracovávať milióny požiadaviek na kategorizáciu.

3.4.2 Hlavné nastavenie

Hlavné nastavenie vám umožní upraviť nastavenie IP filtra a základných možností. Môžete povoliť alebo zakázať Call Filter alebo Data Filter. Za istých okolností môžu vaše filtre fungovať postupne. Takže určíte len Start Filter Set (počiatočný filter). Takisto môžete nakonfigurovať nastavenia Log Flag a povoliť SPI Drop non-http connection on TCP port 80, a Accept incoming fragmented UDP packets.

Kliknite na Firewall a Hlavne nastavenie aby ste otvoril stránku všeobecných nastavení.

Firewall >> Hlavne nastavenie

Hlavne nastavenie

Fiter volani	<input checked="" type="radio"/> Zapnut <input type="radio"/> Vypnut	Startovacia sada filtrov	Sada#1
Datovy filter	<input checked="" type="radio"/> Zapnut <input type="radio"/> Vypnut	Startovacia sada filtrov	Sada#2
Priznak logovania	Vypnute		
<input type="checkbox"/> Zapnut stavovu kontrolu paketov (SPI)			
<input type="checkbox"/> Pouzit IP filter na pakety prichadzajuce cez VPN			
<input type="checkbox"/> Zrusit nie-http pripojenie na TCP porte 80			
<input checked="" type="checkbox"/> Akceptovat prichadzajuce fragmenty UDP paketov (pre niektore hry games, ex. CS)			

OK

Filter volani	Zaškrtnite Enable aby ste aktivovali funciu. Start Filter Set - Určite Call Filter ako počiatočný.
Datovy filter	Zaškrtnite Enable to activate the Data Filter function. Určite start filter set pre Data Filter.
Priznak logovania	Pre potrebu riešenia problémov musíte špecifikovať záznamy filtra.
Vypnute	funkcia nie je aktivovaná.
Blokovat	všetky blokovévané pakety budú zaznamenané.
Povolit	všetky prepustené pakety budú zaznamenané.
Nevyhovuje	budú zaznamenané všetky nezaradené pakety.

Poznámka: všetky záznamy budú zobrazené na termináli Telnet ak zadáte príkaz log -f.

Niektoré online hry (napr. Half Life) budú používať veľké množstvá UDP paketov na prenos dát hry. Router Vigor inštinktívne odmieta tieto čiastočné pakety, aby zamedzil útoku, pokiaľ si nenastavíte povoliť "Akceptovat

prichádzajúce fragmenty UDP paketov”. Zaškrtnutím tohoto políčka môžete hrať tento durh hier. Ak je vašou prioritou bezpečnosť, nemusíte toto povoliť.

3.4.3 Nastavenie filtrovania

Kliknite na Firewall a Nastavenie filtrovania aby ste otvorili stránku nastavení.

Firewall >> Nastavnie Filtrovania

Nastavnie Filtrovania

| [Nastaviť výrobné nastavenie](#) |

Skupina	Poznamky	Skupina	Poznamky
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

Kliknite na číslo skupiny, ak chcete pridať alebo upraviť individuálnu skupinu. Zobrazí sa vám nasledujúca stránka. Každý filter obsahuje sedem pravidiel. Kliknite na číslo pravidla aby ste ho mohli upraviť. Zaškrtnite Aktivne aby ste pravidlo povolili.

Firewall >> Nastavenie filtrovania >> Uprava sady filtrov

Sada filtrov 1

Poznamky :

Pravidlo filtrov	Aktivne	Poznamky
<input type="text" value="1"/>	<input checked="" type="checkbox"/>	Block NetBios
<input type="text" value="2"/>	<input type="checkbox"/>	
<input type="text" value="3"/>	<input type="checkbox"/>	
<input type="text" value="4"/>	<input type="checkbox"/>	
<input type="text" value="5"/>	<input type="checkbox"/>	
<input type="text" value="6"/>	<input type="checkbox"/>	
<input type="text" value="7"/>	<input type="checkbox"/>	

Nasledovna sada filtrov

OK

Vymazať

Zrusiť

Pravidlo filtrov

Kliknite na očíslované tlačítko (1 ~ 7), ak chcete upraviť pravidlo filtra. Kliknutím na tlačítko otvoríte stránku Edit Filter Rule web. Podrobnejšie viď ďalšia stránka.

Aktivne

Povoľte alebo zakážte pravidlo filtra.

Poznamky

Napište poznámky alebo popis filtra, maximálne 23 znakov.

Nasledovna sada filtrov

Nastavte odkaz na ďalší set filtra, ktorý má byť vykonaný po spustení filtra. Nedávajte mnoho filtrov do slučky.

Aby ste nastavili pravidlo filtra, kliknite na tlačítko s Číslom pravidla filtrov a vstúpte na stránku Uprava pravidla filtra.

Sada filtrov 1 Pravidlo 1

Poznámky : Block NetBios

☒ Oznacenim sa aktivuje pravidlo filtrovania

Prepusťit alebo blokovat		Pripojiť k inej sade filtrov	
Blokovať okamžite		Žiadny	
<input type="checkbox"/> Log			
Smer	Dnu	Protokol	TCP/UDP
Zdroj	IP adresa	Maska podsiete	Operator
	any	255.255.255.255 (/32)	=
Ciel	any	255.255.255.255 (/32)	=
		Start Port	End Port
		137	139
<input type="checkbox"/> Keep State		fragmenty	Nestarat sa

OK

Vymazať

Zrušiť

Poznámky

Napište poznámky alebo popis filtra, maximálne 14 znakov.

Oznacenim sa aktivuje pravidlo filtrovania- Zaškrtnite, ak chcete povoliť pravidlo filtra.

Prepusťit alebo blokovat

Povolit okamžite
Povolit okamžite
Blokovať okamžite
Povolit ak nesplna predchadzajúce pravidlo
Blokovať ak nesplna predchadzajúce pravidlo

Prepusťit alebo blokovat Upresňuje čo sa bude diať s paketom, ak zodpovedá pravidlu. Pass Immediately – pakety budú okamžite prepustené.

Blokovať okamžite pakety budú okamžite zamietnuté.

Povolit ak nesplna predchadzajúce pravidlo paket zodpovedajúci pravidlu, ktorý nezodpovedá žiadnemu inému pravidlu bude prepustený.

Blokovať ak nesplna predchadzajúce pravidlo - paket zodpovedajúci pravidlu, ktorý nezodpovedá žiadnemu inému pravidlu bude zamietnutý.

Pripojiť k inej sade filtrov Ak paket zodpovedá pravidlu, ďalšie pravidlo sa pridá do setu filtra. Určite ďalšie pravidlo z menu.

Log Zaškrtnite, aby ste povolili funkciu log. Použite Telnetový príkaz log-f aby ste zobrazili záznamy.

Smer Nastavte smerovanie toku paketov. Služi len pre Data filter. Pre Call Filter toto nastavenie neplatí, pretože tento filter slúži len pri odosielaní.

Protokol určite protokol/protokoly, ktoré má filter aplikovať.

IP adresa Určite zdrojovú a cieľovú IP adresu, na ktorú má filter pravidlo aplikovať. Ak zadáte symbol „!“ pred IP adresu, pravidlo nebude aplikované. Aby bolo aplikované na všetky IP adresy, zadajte any(akákoľvek), alebo nechajte pole prázdne.

Maska podsiete zvolte masku podsiete, na ktorú má byť pravidlo aplikované, z menu.

Operator, Start Port a End Port – kolonka Operátor špecifikuje nastavenia čísel portov. Ak je pole Start Port prázdne, Start Port a End Port budú ignorované. Pravidlo filtra bude aplikované na akýkoľvek filter. (=) ak je prázdne pole End Port pravidlo nastaví číslo portu ako Start Port. (=) V inom prípade rozsah čísel platí od Start Port po End Port vrátane ich čísel. (!=) Ak je pole End Port prázdne, číslo sa nerovná hodnote v poli Start Port. V inom prípade toto číslo nie je medzi Start Port a End Port vrátane ich hodnôt. (>) Špecifikuje číslo portu väčšie ako Start Port vrátane čísla Start Port.

Keep State

Táto funkcia pracuje naraz so smerovaním, protokolom, IP adresou, maskou podsiete, operátorom, Start Port-om a End Portom. Používa sa len pre Data Filter.

Pojem Keep State je podobný ako pojem Stateful Packet Inspection. Stopuje pakety a akceptuje pakety, ktoré sú uznané protokolom. Odmieťa nevyžiadané dáta. Môžete nastaviť akýkoľvek protokol spomedzi TCP, UDP, TCP/UDP, ICMP a IGMP.

fragmenty

Nestarat sa

Zrusit

Nestarat sa
Nefragmentovane
Fragmentovane
Prilis kratke

Fragmenty

Špecifikuje čo sa bude diať s fragmentovanými paketmi. Používa sa len pre Data Filter. Nestarat sa –fragmentované pakety budú ignorované. Nefragmentovane –Aplikuje pravidlo na nefragmentované pakety. Fragmentovane –Aplikuje pravidlo na fragmentované pakety. Prilis kratke – Aplikuje pravidlo len na pakety, ktoré sú príliš krátke na to aby obsahovali úplnú hlavičku.

Príklad

Každý prenos bude oddelený a posúdený jedným z dvoch IP filtrov – call filter alebo data filter. Môžete predvoliť 12 call filterov a data filterov v Filter Setup a nastaviť ich aby fungovali postupne. Každý filter set pozostáva zo siedmich pravidiel, ktoré môžu byť ďalej definované. Potom, v General Setup (všeobecné nastavenie), môžete špecifikovať jeden set pre call filter a jeden pre data filter, ktorý má byť spustený prvý.

Firewall >> General Setup

General Setup

Call Filter ☒ Enable ☐ Disable Start Filter Set Set#1

Data Filter ☒ Enable ☐ Disable Start Filter Set Set#2

Log Flag None

☐ Enable stateful packet inspection
☐ Apply IP filter to VPN incoming packets
☐ Drop non-http connection on TCP port 80
☒ Accept incoming fragmented UDP packets (for some games, ex. CS)

OK

Firewall >> Filter Setup

Filter Setup

Set	Comments	Set	Comments
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1

Comments: Default Call Filter

Rule	Active	Comments
1	<input checked="" type="checkbox"/>	Block NetBios
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	
7	<input type="checkbox"/>	

Next Filter

Firewall >> Edit Filter Rule >> Edit Filter Rule

Filter Set 1 Rule 1

Comments: Block NetBios

☒ Check to enable the Filter Rule

Pass or Block Block Immediately

Branch to Other Filter Set None

☐ Log

Direction IN Protocol TCP/UDP

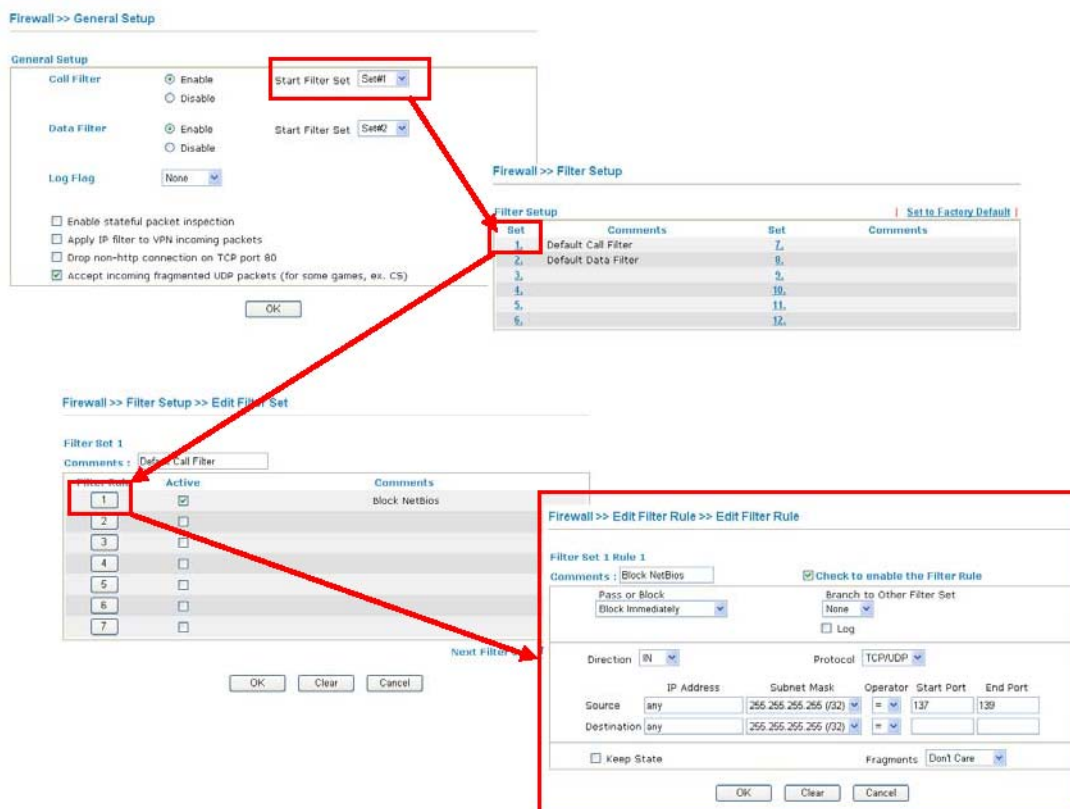
IP Address Subnet Mask Operator Start Port End Port

Source any 255.255.255.255 (32) = 137 139

Destination any 255.255.255.255 (32) =

☐ Keep State Fragments Don't Care

OK Clear Cancel



3.4.4 Blokovanie IM

Kliknite na Firewall a IM blkovanie aby ste otvorili stránku nastavení. Uvidíte zoznam zvyčajných IM (ako MSN, Yahoo, ICQ/AOL). Zaškrtnite Enable IM blokovanie a zvolíte tie, ktoré chcete blokovať. Ak ich chcete blokovať v určitých časových rozmedziach, nastavte ich v programe Aplikácie >> Planovac.

Firewall >> IM Blocking Setup

Blokovanie Messenger aplikácií

- ☐ Aktivovat IM blokovanie
- ☐ Blokovat MSN Messenger
 - ☐ Blokovat Yahoo Messenger
 - ☐ Blokovat ICQ/AOL

Casovy planovac

Index(1-15) v [Planovaci](#) Nastavenie: , , ,

Poz.: Akcia a Zostavajuci cas bude ignorovany.

OK

Zrusit

3.4.5 P2P blokovanie

Kliknite na Firewall a P2P blokovanie aby ste otvorili stránku nastavení.. Uvidíte zoznam zvyčajných aplikácií P2P. Zaškrtnite Aktivovat P2P blokovanie a zvolíte tie, ktoré chcete blokovať. Ak ich chcete blokovať v určitých časových rozmedziach, nastavte ich v programe Aplikácie >> Planovac.

Nastavenie blokovania zdieľania Peer-to-Peer aplikácii

☐ Aktivovať P2P blokovanie

Protokol	Aplikácie	Akcia
eDonkey	eDonkey, eMule, Shareaza, MLDonkey	<input checked="" type="radio"/> Povolit <input type="radio"/> Nepovolit <input type="radio"/> Nepovolit upload
FastTrack	KazaA, iMesh, MLDonkey	<input checked="" type="radio"/> Povolit <input type="radio"/> Nepovolit
Gnutella	BearShare, Gnucleus, Limewire, Phex, Swapper, XoloX, Shareaza, MLDonkey	<input checked="" type="radio"/> Povolit <input type="radio"/> Nepovolit
BitTorrent	BitTorrent	<input checked="" type="radio"/> Povolit <input type="radio"/> Nepovolit

Časový plánovač

 Index(1-15) v [Planovaci](#). Nastavenie: , , ,
Poz.: Akcia a čas nečinnosti budú ignorované.

OK

Zrušiť

Akcia

Povolit

Nepovolit

Nepovolit upload

Špecifikuje činnosť každého protokolu.

Dovolí klientovi prístup k aplikácii cez špecifikovaný protokol.

Zakáže klientovi prístup k aplikácii cez špecifikovaný protokol.

Zakáže klientovi prístup k aplikácii cez špecifikovaný protokol pri downloade. Upload je povolený.

3.4.6 DoS obrana

V nastavení DoS obrany je 15 typov funkcií na detekovanie a obranu, ako podfunkcia IP Filtra/Firewallu. Nastavenie DoS obrany je predvolené ako „zakázaný“.

Kliknite na Firewall a DoS obrana aby ste otvorili stránku nastavenia.

Nastavenie DoS obrany

<input type="checkbox"/> Aktivovat DoS obranu			
<input type="checkbox"/> Aktivovat SYN flood obranu	Prah	<input type="text" value="50"/>	pakety / sec
	Odpojit po	<input type="text" value="10"/>	sec
<input type="checkbox"/> Aktivovat UDP flood obranu	Prah	<input type="text" value="150"/>	pakety / sec
	Odpojit po	<input type="text" value="10"/>	sec
<input type="checkbox"/> Aktivovat ICMP flood obranu	Prah	<input type="text" value="50"/>	pakety / sec
	Odpojit po	<input type="text" value="10"/>	sec
<input type="checkbox"/> Aktivovat detekciu skenovania portov	Prah	<input type="text" value="150"/>	pakety / sec
<input type="checkbox"/> Blokovat IP options	<input type="checkbox"/> Blokovat TCP flag skenovanie		
<input type="checkbox"/> Blokovat Land	<input type="checkbox"/> Blokovat Tear Drop		
<input type="checkbox"/> Blokovat Smurf	<input type="checkbox"/> Blokovat Ping of Death		
<input type="checkbox"/> Blokovat trace route	<input type="checkbox"/> Blokovat ICMP fragment		
<input type="checkbox"/> Blokovat SYN fragment	<input type="checkbox"/> Blokovat neznamyProtokol		
<input type="checkbox"/> Blokovat Fraggle utok			
<div></div>			

OK

Vymazat

Zrusit

Aktivovat DoS obranu
Enable SYN flood defense

Zaškrtnite políčko aby ste aktivovali DoS Defense Funkcionalitu. Zaškrtnite ak chcete aktivovať funkciu. Ak paket prekročí prahovú hodnotu TCP SYN, Vigor začne náhodne rušiť ďalšie pakety na dobu, ktorá je definovaná v poli Odpojit po. Cieľom je zabrániť paketom TCP SYN, ktoré sa snažia vyčerpať obmedzené prostriedky routera. Hodnoty množstva a času sú predvolené na 50 paketov za 10 sekúnd.

Enable UDP flood obranu

Zaškrtnite políčko aby ste aktivovali obranu UDP flood defense. Ak hodnota prijatých UDP paketov z internetu prekročí určenú hranicu, router Vigor začne náhodne vymazávať ďalšie UDP pakety na čas stanovený v Odpojit po. Hodnoty množstva a času sú predvolené na 150 paketov za 10 sekúnd.

Enable ICMP flood obranu

Zaškrtnite políčko aby ste aktivovali obranu ICMP flood defense. Ak hodnota prijatých ICMP paketov z internetu prekročí určenú hranicu, router Vigor začne náhodne vymazávať ďalšie ICMP pakety na čas stanovený v Odpojit po. Hodnoty množstva a času sú predvolené na 50 paketov za 10 sekúnd.

Aktivovat detekciu skenovania portov – útoky skenovaním portov útočia na router posielaním veľkým množstvom paketov na viac portov, aby útočník našiel prienikové nezabezpečené miesto. Zaškrtnite políčko aby ste aktivovali detekciu skenovania portov. Vždy, keď router detekuje zasielanie paketov nad určitý počet, ktoré by mohlo byť škodlivé, upozorní vás na to. Predvolené množstvo je 150 paketov za sekundu.

Block IP options

Zaškrtnite políčko, ak chcete aktivovať funkciu Block IP options function. The Vigor router bude ignorovať IP pakety s IP option v hlavičke datagramu. Obmedziť tieto IP options je vhodné kvôli bezpečnosti miestnej siete. Obsahuje totižto informácie o bezpečnosti, TCC (uzavretá skupina užívateľov), internetové adresy, smerovacie odkazy apod. with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series

	of Internet addresses, routing messages...etc. Útočník zvonku sa tak môže dozvedieť súkromné detaily o vašej sieti.
Block Land	Zaškrtnite políčko, ak chcete posilniť obranu routera proti útoku Land-Attack. Land-Attack kombinuje útok SYN s IP spoofingom. Objaví sa, keď útočník zasiela falošné SYN pakety s identickou zdrojovou i cieľovou adresou ako aj číslom portu, obeti.
Block Smurf	Zaškrtnutím aktivujete funkciu Block Smurf function. Router bude ignorovať každú požiadavku vysielania ICMP echo.
Block trace router	Zaškrtnite, ak chcete aby router nepreposielal trace route pakety (stopovacie pakety).
Block SYN fragment	Zaškrtnite, ak chcete aktivovať funkciu Block SYN fragment. Router pustí všetky pakety označené SYN a viacfragmentové sety bitov.
Block Fraggle útok	Zaškrtnite, ak chcete aktivovať funkciu Block fraggle Attack. Bude blokované každé vysielanie UDP paketov prijatých z internetu. Aktivovanie obrany DoS/DDoS defense môže blokovať aj niektoré legálne pakety. Napríklad keď aktivujete obranu Fraggle attack, všetky UDP pakety z internetu sú blokované, preto môžu byť pustene RIP pakety.
Block TCP flag skenovanie	Zaškrtnite, ak chcete aktivovať funkciu Block TCP flag scan. Budú vylúčené všetky TCP pakety. Toto skenovanie zahŕňa no flag scan, FIN without ACK scan, SYN FINscan, Xmas scan a full Xmas scan.
Block Tear Drop	Zaškrtnite, ak chcete aktivovať funkciu Block Tear Drop. Pri prijíme ICMP datagramov sa mnohé prístroje môžu zrútiť, ak tieto prekračujú maximálnu dĺžku. Aby sme sa vyhlí tomuto typu útoku, router je schopný vymazať akýkoľvek fragmentovaný ICMP paket dlhší ako 1024 octets.
Block Ping of Death	Zaškrtnite, ak chcete aktivovať funkciu Block Ping of Death. Týmto útokom posíla útočník prekrývajúce sa pakety cieľovým hostiteľom, takže tí sú nečinní kým nie sú pakety rekonštruované. Router zablokuje všetky pakety vykonávajúce tento typ útoku.
Block ICMP Fragment	Zaškrtnite, ak chcete aktivovať funkciu Block ICMP fragment. Všetky ICMP pakety s viacerými bitovými setmi fragmentov sú vylúčené.
Block NeznamyProtokol	Zaškrtnite, ak chcete aktivovať funkciu Block Unknown Protocol. Individuálny IP paket má v datagramovej hlavičke pole protokolu, aby indikoval typ protokolu v hornej vrstve. Typy protokolu väčšie ako 100 nie sú definované. Preto router môže takéto pakety odmietnuť.
Warning Messages (výstražné správy)	Router poskytuje funkciu Syslog, aby užívateľ mohol obdržať správu ostave DoS. Router posíla správy ako Syslog klient. Všetky výstražné správy na základe DoS obrany sú posielané užívateľovi, ktorý si ich môže prehliadať cez Syslog daemon. Najdite v správe heslo DoS nasledované menom a zistíte aký typ útoku bol detekovaný.

Zaznamenavanie systému

Zaznamenavanie systému (SysLog)

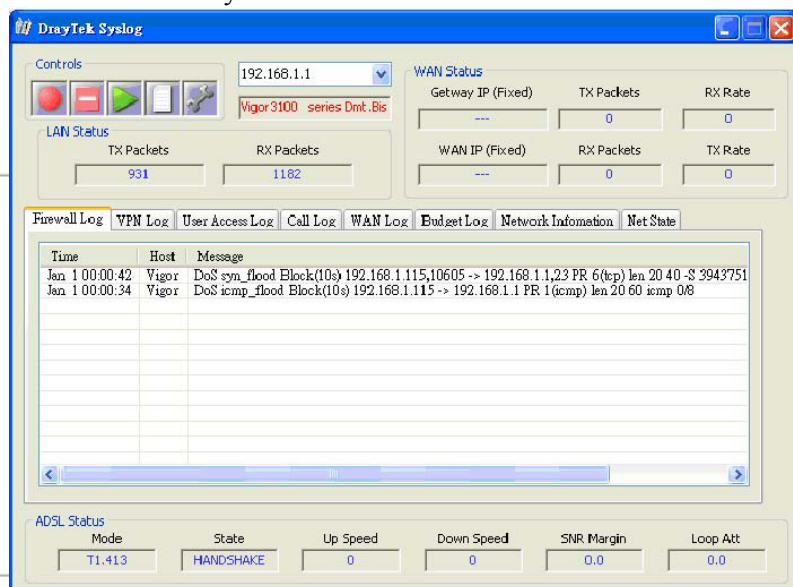
☒ Zapnut

IP adresa servra

Cielovy port

Aktivovat zaznamenavanie sprav:

- ☒ Firewall zaznamy
- ☒ VPN zaznamy
- ☒ Zaznamy uzivatelskych pristupov
- ☒ zaznamenavanie volania
- ☒ WAN zaznamy
- ☒ Router/DSL informacie



3.4.7 Obsahové filtrovanie

Na základe zoznamu hesiel definovaných užívateľom, prehliada router reťazce URL pri každej HTTP požiadavke. Či už je URL úplná alebo čiastočná, ak obsahuje definované heslo, router preruší spojenie HTTP.

Například ak vložíte slovo ako „sex“, router obmedzí přístup na stránky typu „www.sex.com“, „www.backdoor.net/images/sex/p_386.html“. Případne můžete určit aj čiastočnú URL ako například „sex.com“. Takisto router Vigor zamietne každú požiadavku, ktorá sa snaží získať škodlivý kód. Kliknite na Firewall a URL Content Filter aby ste otvorili stránku nastavení.

Firewall >> URL obsahove filtrovanie

Obsahove filtrovanie

☐ Aktivovat blokovanie pristupu na URL

- ☒ Black List (blokovat hodiace sa klucove slova)
☐ White List (povolit hodiace sa klucove slova)

Cis	Akt	Retazec	Cis	Akt	Retazec
1	<input type="checkbox"/>	<input type="text"/>	5	<input type="checkbox"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	6	<input type="checkbox"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	7	<input type="checkbox"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	8	<input type="checkbox"/>	<input type="text"/>

moznost zadat viac retazcov oddelenim medzerou, napr: **hotmail yahoo msn**

☐ Ochranit pristup na internet z IP adries

☐ Aktivovat zakaz pristupu na web stránky

- ☐ Java ☐ ActiveX ☐ Komprimovane subory ☐ Spustitelne subory ☐ Multimedialne subory
☐ Cookie ☐ Proxy

☐ Aktivovat vynimky podsieti

Cis	Akt	IP adresa		Maska podsiete
1	<input type="checkbox"/>	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	~	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
2	<input type="checkbox"/>	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	~	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
3	<input type="checkbox"/>	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	~	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
4	<input type="checkbox"/>	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	~	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>

Casovy planovac

Index(1-15) v **Planovaci** Nastavenie: , , ,

Poz.: Akcia a nastavenie doby necinnosti bude ignorovane.

OK

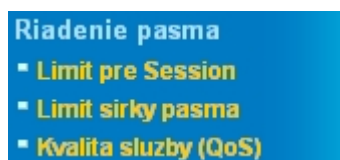
Zmazat vset

Zrusit

Aktivovat blok.pristupu na URL Zaškrtnite, ak chcete aktivovať URL Access Control (kontrola prístupu URL).

Black List (čierny zoznam, zablokuje tieto heslá)	Kliknite na tlačítko, ak chcete zablokovať prístup na stránky obsahujúce zodpovedajúce heslá.
White List (biely zoznam, povolí tieto heslá)	Kliknite na tlačítko, ak chcete povoliť prístup na stránky obsahujúce zodpovedajúce heslá.
Retazec	Router Vigor poskytuje 8 rámcov pre užívateľov, aby si mohli zadať heslá, každý z nich podporuje hromadné heslá. Môže to byť slovo, časť slova alebo úplný reťazec URL. Hromadné heslá v rámci sú oddelené medzerou, čiarkou alebo bodkočiarkou. Maximálna dĺžka je 32 znakov. Po určení hesla router odmietne prístup ku stránkam, ktoré ho obsahujú. Čím je heslo jednoduchšie, tým efektívnejšiu ochranu zabezpečí.
Ochraniť prístup na int. Z IP adries	Zaškrtnite, ak chcete zabrániť surfovaniu po webe s použitím IP adresy ako napr. http://202.6.3.2.. Účelom je nemožnosť obísť URL Access Control. Aby filtrovanie obsahu URL fungovalo správne, musíte najprv vymazať cache vášho prehliadača
Aktivovať zákaz prístupu na web str.	- Zaškrtnite, ak chcete aktivovať funkciu.
Java	Zaškrtnite, ak chcete blokovat' objekty Java. Router vylúči objekty Java prijímané z Internetu.
ActiveX	Zaškrtnite, ak chcete blokovat' objekty Active X. Router vylúči objekty Active X prijímané z Internetu.
Compressed file	Zaškrtnite ak chcete blokovat' prijímanie komprimovaných súborov. Budú odmietnuté súbory s nasledujúcou príponou: zip, rar, .arj, .ace, .cab, .sit
Executable file	Zaškrtnite, ak chcete aby router odmietol sťahovanie spustiteľných súborov z Internetu, ktoré obsahujú prípona ako: .exe, .com, .scr, .pif, .bas, .bat, .inf, .reg
Cookie	Zaškrtnite, ak chcete aby router Vigor filtroval prenos súborou cookie pre ochranu užívateľovho súkromia.
Proxy	Zaškrtnite, ak chcete odmietnuť všetky prenosy proxy. Aby ste si efektívne ustrážili obmedzenú šírku prenosu, je vhodné blokovat' sťahovanie multimediálnych súborov z Internetu ktoré obsahujú prípony ako: .mov .mp3 .rm .ra .au .wmv .wav .asf .mpg .mpeg .avi .ram
Aktivovať výnimky podsietí	Spod kontroly prístupu URL je možné vyňať štyri IP adresy alebo podsiete. Aby ste povolili vstup, kliknite na prázdne políčko nazvané ACT pred daným vstupom.
Casový plánovač	špecifikuje program v akom čase bude filter činný.

3.5 Riadenie Pasma



3.5.1 Limit pre session

Pomocou tejto funkcie je možné nastaviť limit používaných session pre konkrétnu IP adresu. Session – je to každá požiadavka prístupu a spojenia do internetu akejkoľvek aplikácie v PC.

Limitovanie pre session

☒ Zapnut ☐ Vypnut

Prednastavene limitovanie pre session:

Zoznam limitovani

Index	Pociatocna IP	Konecna IP	Limitovanie pre session
1	192.168.1.10	192.168.1.12	20
2	192.168.1.20	192.168.1.30	30

Specifikovanie limitovania

Pociatocna IP: Konecna IP:

Limit pre session:

Planovac volani

Index(1-15) v [Planovac](#) Nastavenie: , , ,

Poz.: Akcia a nastavenie casu necinnosti bude ignorovane.

Zapnut	Aktivuje funkciu limitovanie session
Vypnut	Deaktivuje funkciu limitovanie session
Prednastavene limitovanie pre session	Ak je funkcia zapnuta nie je pridany ziadny zaznam do Zoznamu limitovani, bude pre kazdu IP v LAN pouzita zadana hodnota
Zoznam Limitovani	Zobrazi vytvorene zaznamy
Pociatocna IP	Pociatocna IP noveho zaznamu
Konecna IP	Konecna IP noveho zaznamu
Limit pre session	Pocet povolenych session pre zaznam
Pridat	Pridat novy zaznam z pola Pociatocana IP, Konecna IP a Limit pre session
Upravit	Upravit ozanceny zaznam v okne Zoznamu limitovani
Odstranit	Odstranit ozanceny zaznam v okne Zoznamu limitovani
Planovac volani	Umožňuje funkciu limitovania session zahrnúť do plánovača

3.5.2 Limit sirky pasma

Pomoco tejto funkcie je možné limitovať prietok pre zadefinované IP adresy v sieti LAN, a to aj smerom von a dnu.

Limit sirky pasma

☒ Zapnut
 ☐ Vypnut

Prednastaveny TX Limit: Kbps
 Prednastaveny RX Limit: Kbps

Zoznam limitovani

Index	Pociatocna IP	Konecna IP	TX limit	RX limit
1	192.168.1.35	192.168.1.40	64	64
2	192.168.1.50	192.168.1.55	128	128

Specifikovanie limitovania

Pociatocna IP:
 Konecna IP:

TX Limit: Kbps
 RX Limit: Kbps

Planovac

Index(1-15) v [Planovac](#) Nastavenie: , , ,

Poz.: Akcia a cas necinnosti budu ignorovane.

Zapnut	Aktivuje funkciu limitovanie šírky pásma
Vypnut	Deaktivuje funkciu limitovanie šírky pásma
Prednastavený TX Limit	Ak je funkcia zapnuta nie je pridany ziadny zaznam do Zoznamu limitovani, bude pre kazdu IP v LAN pouzita zadana hodnota a bude limitovaný prietok vysielaných paketov
Prednastavený RX Limit	Ak je funkcia zapnuta nie je pridany ziadny zaznam do Zoznamu limitovani, bude pre kazdu IP v LAN pouzita zadana hodnota a bude limitovaný prietok prichádzajúcich paketov
Zoznam Limitovani	Zobrazí vytvorene zaznamy
Pociatocna IP	Pociatocna IP noveho zaznamu
Konecna IP	Konecna IP noveho zaznamu
TX limit	Hodnota limitovania odosielaných paketov v kbps
RX limit	Hodnota limitovania prijímaných paketov v kbps
Pridat	Pridat novy zaznam z pola Pociatocana IP, Konecna IP a TX limit a RX limit
Upravit	Upravit ozanceny zaznam v okne Zoznamu limitovani
Odstranit	Odstranit ozanceny zaznam v okne Zoznamu limitovani
Planovac volani	Umožňuje funkciu limitovania šírky pásma zahrnúť do plánovača

3.5.3 QoS - Kvalita služby

Riadenie kvality služieb zaručuje, že všetky aplikácie budú mať k dispozícii dostatočnú úroveň služieb a dostatočnú šírku prenosu, aby vyhoveli očakávaniam, čo je dôležitý aspekt modernej podnikovej siete.

Dôvodom pre QoS je, že aplikácie na báze TCP stále zvyšujú rýchlosť vysielania a spotrebúvajú celú šírku prenosu, čo sa nazýva pomalý štart TCP. Keď nie sú ostatné aplikácie chránené QoS, obmedzí to ich výkon v preplnenej sieti. To

je dôležité najmä pre tie aplikácie, ktoré sa ťažko vyrovnávajú so stratou, oneskorením alebo chvením ako napríklad voice over IP, videokonferencie, streamové video alebo dáta.

Ďalším dôvodom súvisí s tým, že pri upchatí interseckcií, ktorých rýchlosti sú rozdielne alebo sa zbiera prenos, pakety sa nahromadia a prenos sa spomalí. Ak nie je nadefinovaná priorita špecifikovať, ktorý paket má byť vymazaný z rady, pakety z aplikácií spomenutých vyššie môžu byť tie ktoré vypadnú.

Ako to ovplyvní výkon aplikácií?

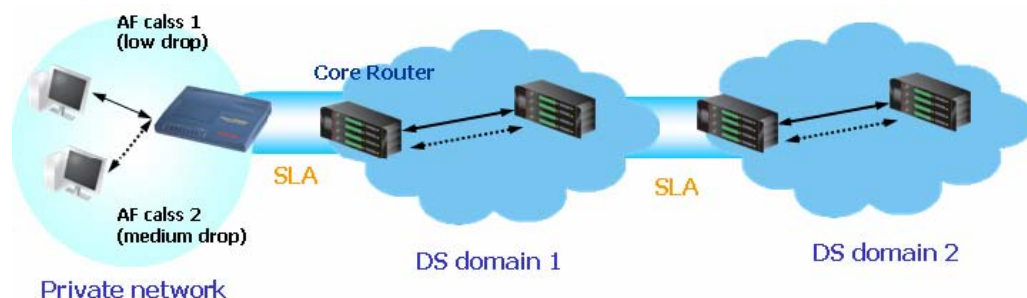
klasifikácia: identifikovanie kritických aplikácií alebo aplikácií s nízkou latenciou a označenie za vysokú prioritu pri prenose po sieti

časové programovanie založené na klasifikácii pri priradovaní paketov do radov a asociovaných typov služieb.

Základná implementácia QoS v routeri Vigor zahŕňa klasifikáciu a časové naprogramovanie paketov založené na hlavičke IP. Napríklad vzdialený pracovník môže na spojenie s ústredím použiť index riadenia QoS aby si rezervoval dostatočnú šírku prenosu pre spojenie HTTPS počas používania niekoľkých aplikácií naraz.

Širšia implementácia je aplikovať DSCP (Differentiated Service Code Point) a IP Precedence na at 3. vrstve.

V porovnaní s odkazom, IP precedence používajúci pole IP hlavičky Type of Service (ToS), ktoré definuje osem tried služieb, DSCP je jeho nasledovník vytvárajúci 64 tried so spätnou kompatibilitou na IP Precedence. V sieti so spustenou QoS alebo systémom Differentiated Service (DiffServ alebo DS) vlastní DS domény môže podpísať Service License Agreement (Zmluvu o licencií služby - SLA) s inými vlastními domén DS, aby si zadefinovali úroveň služby poskytovanej prenosu z rôznych domén. Potom každý DS uzol v týchto doménach bude spracovávať prenos prioritne. Nazýva sa to per-hop-behavior (správanie na skok PHB). Definícia PHB zahŕňa Expedited Forwarding (zrýchlené preposielanie - EF), Assured Forwarding (zaistené preposielanie - AF), a Best Effort (najlepšia snaha - BE). AF definuje štyri triedy doručenia (alebo preposlania) a tri úrovne prednosti prepadnutia v každej triede. Routery Vigor ako okrajové routery domén DS skontrolujú hodnoty DSCP v IP hlavičke obídeného prenosu aby takto pridelili určité množstvo zdrojov na vykonanie zodpovedajúcej kontroly, klasifikácie a časového naprogramovania. Jadrové routery na kostre vykonávajú tú istú kontrolu kým vykonávajú spracovanie, aby zaistili konzistenciu úrovne služby celou sieťou s povoleným QoS.



Aj tak môže mať každý uzol rôzny postoj k paketom s vysokou prioritou napriek tomu, že sú spojené dohodom SLA medzi rôznymi vlastníkmi DS domén. Je ťažké docieľiť deterministický a konzistentný prenos QoS celou sieťou aj napriek snahe routera Vigor.

Pre efektívnejšie nastavenie QoS, mali by ste si pozrieť dosiahnuteľné rýchlosti ADSL upstream a downstream na stránke Online Stav, kým budete konfigurovať nastavenia QoS.

ADSL informácie		(Verzia ADSL firmware: 1311302_B)				
ATM statistiky	TX bloky		RX bloky	Upravené bloky		Neupravené bloky
	2036		2278	0		3
ADSL stav	Mod	Stav	Rychlost odosielania	Rychlost prijimania	Odstup signal-sum	Trmenie linky
	G.DMT	SHOWTIME	320000	3072000	10	49

Nasledujúce taktiky QoS budú definované vo forme rýchlosti pomeru upstream/downstream. Ako vodičko k dosiahnutiu tohoto cieľa vám poskytneme aplikáciu QoS requirement. Hodnoty nastavenia sa budú meniť v závislosti na podmienkach siete.

Kliknite na Riadenie pásma>>Kvalita služby (QoS). Zobrazí sa nasledujúce okno.

Qvalita sluzby (QoS)

[Nastavit do vyrobného nastavenia](#)

☒ Aktivovat QoS kontrolu

Smer: VON

Index	Nazov skupiny	Rezervovany pomer pasma	Nastavenie	
1.	<input type="text"/>	<input type="text" value="25"/> %	<input type="button" value="Zakladne"/>	<input type="button" value="Rozsirene"/>
2.	<input type="text"/>	<input type="text" value="25"/> %	<input type="button" value="Zakladne"/>	<input type="button" value="Rozsirene"/>
3.	<input type="text"/>	<input type="text" value="25"/> %	<input type="button" value="Zakladne"/>	<input type="button" value="Rozsirene"/>
4.	Ostatne	<input type="text" value="25"/> %		

☐ Aktivovat kontrolu UDP pasma

Pomer pre limitovane pasmo %

[Online statistiky](#)

OK

vymazat

Aktivovat' QoS kontrolu

Smer

Index

Názov skupiny

Rezervovaný pomer pásma

Nastavenie

Aktivovat' kontrolu UDP pásma

Pomer pre limitované pásmo

Základné tlačítko

Pri modeloch V je predvolené nastavenie enable (povoliť)

Definujte, na ktorý prenos majú byť aplikované nastavenia. IN – len na prichádzajúce prenosy. VON – len na odchádzajúce prenosy.

Indexové číslo nastavení QoS Control. Celkovo sú 4 skupiny.

Definujte názov skupiny.

Je rezervované pre skupinu vo forme podielu rezervovanej šírky pásma prenosu a rýchlosti upstream a rezervovanej šírky pásma prenosu a rýchlosti downstream.

Sú dve úrovne nastavenia: základné nastavenie – Rezervovaná šírka pásma prenosu na základe typu prenosovej služby. Poskytli sme vám zoznam bežných typov služieb.

Rozšírené nastavenie – nastavenie rezervovanej šírky pásma prenosu na základe zdrojovej adresy, cieľovej adresy DiffServ CodePoint a type služby.

Zaškrtnite a nastavte obmedzenú šírku pásma v pravom poli Control. Toto ochráni TCP aplikácie, keď prenos UDP aplikácií, ako napríklad streamové video, vyčerpá väčšinu šírky pásma.

Tento pomer je používaný na obmedzenie celkovej šírky pásma používaného UDP aplikáciami.

Kliknite na toto tlačítko, ak chcete otvoriť základnú konfiguráciu každého indexu.

[Bandwidth Management >> Quality of Service](#)

Zakladne nastavenie QoS

Index skupiny #1

ANY

AUTH(TCP:113)

BGP(TCP:179)

BOOTPCCLIENT(UDP:68)

BOOTPSERVER(UDP:67)

CU-SEEME-HI(TCP/UDP:24032)

CU-SEEME-LO(TCP/UDP:7648)

DNS(TCP/UDP:53)

FINGER(TCP:79)

Poz.: V základnom nastavení nastavujeme iba typ služby.
Zdrojova/cielova adresa bude nahradena hociakou ak stlacite "OK".

OK

Vymazat

Zrusit

Zvoľte jednu z položiek z ľavého boxu a kliknite na ADD>>. Zvolená položka sa objaví v pravom. Aby ste odstránili položku z pravého boxu, označte ju a kliknite na <<Remove.

Rozsirenie

Kliknite na toto tlačítko, ak chcete otvoriť rozšírenú konfiguráciu indexu. Na tejto stránke môžete vkladať, presúvať, upravovať alebo vymazávať pravidlá.

Bandwidth Management >> Quality of Service

Rozsirene nastavenie QoS

Index skupiny # 1					
NIE	Stav	Zdrojova adresa	Cielova adresa	DiffServ CodePoint	Typ sluzby
1.		Prazdny	-	-	-

nove pravidlo pred (Cislo pravidla).

oznacene pravidlo (oznacte Index cislo) do (Cislo pravidla).

oznacene pravidlo

oznacene pravidlo

Ak chcete vložiť pravidlo, kliknite na Insert na nasledujúcej stránke.

Bandwidth Management >> Quality of Service

Qvalita sluzby (QoS)

ACT	Zdrojova adresa	Cielova adresa	DiffServ CodePoint	Typ sluzby
<input type="checkbox"/>	Any <input type="button" value="ZdrojUprava"/>	Any <input type="button" value="CielUprava"/>	ANY	ANY <input type="button" value="Pridat"/> <input type="button" value="Uprava"/> <input type="button" value="Vymazat"/>

Poz.: Prosim vyberte/nastavenie typu sluzby najskor.

ZdraojUpravat

umožňuje vám upravovať informácie o zdrojovej adrese.

CielUprava

umožňuje vám upravovať informácie o cieľovej adrese. Ak kliknete na jedno z tlačítok, uvidíte nasledujúce dialógové okno.

Zo zoznamu Typ adresy si zvolíte daný typ adresy. Zadajte počiatočnú a konečnú IP adresu a masku podsiete.

DiffServ CodePoint – všetky pakety budú rozdelené do dvoch úrovní a spracované podľa typu úrovne. Zvoľte si úroveň dát na spracovanie s kontrolou QoS.

DiffServ CodePoint

ANY

ANY

IP precedence 1

IP precedence 2

IP precedence 3

IP precedence 4

IP precedence 5

IP precedence 6

IP precedence 7

AF Class1 (Low Drop)

AF Class1 (Medium Drop)

AF Class1 (High Drop)

AF Class2 (Low Drop)

AF Class2 (Medium Drop)

AF Class2 (High Drop)

AF Class3 (Low Drop)

AF Class3 (Medium Drop)

AF Class3 (High Drop)

AF Class4 (Low Drop)

AF Class4 (Medium Drop)

AF Class4 (High Drop)

EF Class

Typ služby – Predurčuje typ služby spracovania dát s QoS Control. Môže byť upravovaný. Jednoducho kliknite na Pridat/Uprava/Vymazať a dostanete sa na nasledujúcu stránku.

Typ služby

ANY

ANY

AUTH(TCP:113)

BGP(TCP:179)

BOOTPCCLIENT(UDP:68)

BOOTPSERVER(UDP:67)

CU-SEEME-LO(TCP/UDP:7648)

CU-SEEME-HI(TCP/UDP:24032)

DNS(TCP/UDP:53)

FINGER(TCP:79)

FTP(TCP:20~21)

H.323(TCP:1720)

HTTP(TCP:80)

HTTPS(TCP:443)

IKE(UDP:500)

IPSEC-AH(IP:51)

IPSEC-ESP(IP:50)

IRC(TCP/UDP:6667)

L2TP(UDP:1701)

NEWS(TCP:144)

NFS(UDP:2049)

NNTP(TCP:119)

PING(IP:1)

POP3(TCP:110)

PPTP(TCP:1723)

RCMD(TCP:512)

REAL-AUDIO(TCP:7070)

RTSP(TCP/UDP:554)

SFTP(TCP:115)

SMTP(TCP:25)

SNMP(TCP/UDP:161)

Ak potrebujete, môžete zadať nový názov služby. Môžete takisto upraviť alebo vymazať službu, ktorú ste pridali predtým.

[Bandwidth Management >> Quality of Service](#)

Typ služby

Meno služby

Typ služby

Konfigurácia portu

Typ ☒ Jediný ☐ Rozsah

Císlo portu -

Aplikovať

Zrušiť

Zadajte prosím Meno služby a zvolte typ služby (TCP/UDP a obe). Ďalej zvolte jeden z typov konfigurácie portu (jediný alebo rozsah) a zadajte rozsah počtu portov v Číslo portu.

3.6 Aplikácie

Aplikácie

- Dynamicke DNS
- Planovac
- RADIUS
- UPnP
- IGMP
- Wake on LAN

3.6.1 Dynamické DNS

Poskytovateľ IS vám často poskytuje na pripojenie k Internetu dynamickú IP adresu. To znamená, že verejná IP adresa vášho routera sa mení pri každom pripojení. Dynamické DNS umožňuje priradiť názov domény k dynamickej IP adrese. Dovoľuje routeru aktualizovať súhrn IP adries na určitom dynamickom DNS serveri. Od pripojenia routeru online budete môcť používať registrovaný názov domény alebo interný virtuálny server z internetu. Je to praktické, ak poskytujete hosťateľský web server, FTP server alebo iný server za routerom.

Kým použijete Dynamické DNS, musíte zadarmo požiadať poskytovateľa služby DDNS o DDNS. Router poskytuje tri účty u troch rôznych poskytovateľov DDNS. Router Vigor je kompatibilný s www.dyndns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic-nameserver.com. Pre registráciu navštívte ich webové stránky. Povoľte funkciu a pridajte Dynamické DNS účet.

Za predpokladu že máte zaregistrovanú DDNS doménu u poskytovateľa DDNS, povedzme hostname.dyndns.org a účet s užívateľským menom test a heslom test.

V menu nastavenia Dynamicke DNS zaškrtnite Aktivovat Dynamicke DNS.

[Aplikácie >> Dynamicke DNS](#)

Dynamicke DNS

☒ Aktivovat Dynamicke DNS

Zobr. Log

Urychlit update

Ucty :

Index	Domena	Aktivovane
1.	---	x
2.	---	x
3.	---	x

OK

Zmazať

Zvoľte index 1 a pridajte účet pre router. Zaškrtnite Aktivovat Dynamické DNS a vyberte poskytovateľa služby: dyndns.org, zadajte registrované hosťateľské meno a príponu dyndns.org do bloku domény. Do nasledujúcich blokov by malo byť zadané meno a heslo „test“.

Index : 1

<input checked="" type="checkbox"/> Aktivovať Dynamický DNS účet	
Poskytovateľ služby	dyndns.org (www.dyndns.org) ▼
Typ služby	Dynamický ▼
Doména	chrono1 . dyndns.org ▼
Login	chrono678 (max. 23 znakov)
Heslo	•••••• (max. 23 znakov)
<input type="checkbox"/> Wildcards	
<input type="checkbox"/> Záložný MX	
Mail Extender	

OK Vymazať Zrušiť

Poskytovateľ služby	Zvoľte poskytovateľa služby
Typ služby	Zvoľte typ služby (Dynamic, Custom, Static).
Doména	Vyplňte použitý názov domény
Login	Prihlasovacie meno nastavené pre použitú doménu
Heslo	Zadajte heslo nastavené pre použitú doménu.

Kliknite na tlačítko OK, aby ste aktivovali nastavenia. Zobrazia sa uložené nastavenia.

Súčasti Wildcard a Záložný MX nie sú poskytovateľmi Dynamických DNS podporované. Podrobnejšie informácie získate z ich stránok.

Zrušiť funkciu a všetky účty DNS

V Menu nastavení DDNS odškrtnite Aktivovať Dynamické DNS, a kliknite na tlačítko Vymazať.

Vymazať účet DNS – v menu nastavení DDNS kliknite na index, ktorý chcete vymazať a kliknite na tlačítko Vymazať.

3.6.2 Plánovač

Router Vigor má zabudované hodiny v reálnom čase, ktorých čas sa aktualizuje manuálne alebo automaticky podľa Network Time Protocol (sieťových časových protokolov – NTP). To znamená, že môžete nastaviť router nielen aby sa pripojil v určitom čase, ale tiež zakázať prístup na Internet v určitých hodinách, takže používatelia sa môžu pripojiť na Internet v určitých hodinách, povedzme pracovných. Program je aplikovateľný aj na iné funkcie.

Kým nastavíte program, musíte nastaviť čas. V menu údržba systému>> Nastavenie času kliknite na tlačítko Nastaviť čas a nastavte čas routera podľa vášho PC. Pri odpojení routera z elektrickej siete alebo jeho resetovaní sa resetujú aj hodiny. Iným spôsobom môžete nastaviť čas požiadavkov na NTP server (časový server), aby synchronizoval hodiny routera. Tento spôsob môžete aplikovať až po pripojení na internet.

Planovac:

Index	Stav	Index	Stav
1.	x	9.	x
2.	x	10.	x
3.	x	11.	x
4.	x	12.	x
5.	x	13.	x
6.	x	14.	x
7.	x	15.	x
8.	x		

Stav: v --- Aktivny, x --- Neaktivny

Vymazať

Môžete nastaviť až 15 programov a aplikovať ich na prístup na internet
Pre nastavenie programu kliknite na index a nastavte ho vid' nižšie.

[Aplikácie >> Planovac](#)

Index cis. 1

☒ Aktivovať Planovac

Start datum (rrrr-mm-dd)

2000

-

1

-

1

Start Čas (hh:mm)

0

:

0

Čas trvania (hh:mm)

0

:

0

Akcia

Spustiť

Odpojit po

0

min(s).(max. 255, 0 standardne)

Ako často

☐ Jedenkrát
 ☒ Dni v týždni

☐ Ned
 ☒ Pon
 ☒ Ut
 ☒ Str
 ☒ Stv
 ☒ Pia
 ☐ Sob

OK

Clear

Zrusiť

Aktivovať Plánovač

Štart Dátum (rrrr-mm-dd)

Štart Čas (hh:mm)

Čas trvania (hh:mm)

Akcia

Zaškrtnite aby ste povolili program.

Upresnite dátum začiatku programu.

Upresnite počiatočný čas programu.

Upresnite trvanie programu.

Upresnite, na ktorú činnosť program volania má byť aplikovaný počas trvania programu.

Spustiť –Udržiavať pripojenie. Vypnúť –Udržiavať pripojenie odpojené. Aktivovať spojeni na požiadanie – špecifikujte, že pripojenie má byť nadviazané na požiadanie a nastavte hodnotu kedy má byť nečinné v poli Idle Timeout. Deaktivovať pripojenie na požiadanie –Určite, že pripojenie bude udržiavané kým prebieha na linke prenos. Ak je pripojenie nečinné dlhšie ako nastavený Idle Timeout, pripojenie sa zruší a už sa nenadviaže počas programu. Idle Timeout určite trvanie pre program. How often – špecifikujte ako často bude program aplikovaný. Once –program bude aplikovaný len raz. Weekdays –určite, ktoré dni v týždni bude program aplikovaný.

Príklad

Ak chcete, aby prístup PPPoE Internet bol pripojený neustále (Spustiť) od 9:00 do 18:00 celý týždeň, ostatný čas bude Internet odpojený (Vypnúť).

(Spustiť) Pon - Ned 9:00 do 18:00



Uistite sa že PPPoE pripojenie a nastavenie času riadne pracujú

Nakonfigurujte vždy zapnuté od 9:00 do 18:00 na celý týždeň.

Nakonfigurujte Vypnúť od 18:00 po ďalší deň do 9:00 na celý týždeň

Priradíte tieto dva profily k profilu prístupu PPPoE Internet. Teraz bude prístup PPPoE Internet pripojený podľa programu.

3.6.3 Radius

Remote Authentication Dial-In User Service (RADIUS) je protokol bezpečnostnej autentifikácie medzi klientom a serverom, ktoré podporuje autentifikáciu, autorizáciu a účtovanie. Je široko používaný poskytovateľmi IS. Je to najpoužívanejší spôsob autentifikácie a autorizácie užívateľov dial-up pripojenia a tunelovaných sietí.

Zabudované príslušenstvo routera RADIUS client umožňuje routeru asistovať vzdialenému dial-in užívateľovi alebo bezdrôtovej stanici a RADIUS serveru pri vykonávaní vzájomnej autentifikácie. Umožňuje centralizovanú autentifikáciu so vzdialeným prístupom pre správu siete..

Aplikácie >> RADIUS

RADIUS server

<input checked="" type="checkbox"/> Zapnut	
IP adresa servra	<input type="text"/>
Cielovy port	<input type="text"/>
Zdielany kluc	<input type="text"/>
Zopakovat zdielany kluc	<input type="text"/>

OK

Vymazat

Zrusit

Zapnúť

Zaškrtnite, aby ste zapli RADIUS

IP adresa servra

Zadajte IP adresu servra RADIUS

Cieľový port

Číslo UDP portu, ktoré RADIUS server používa. Predvolená hodnota na základe RFC 2138 je 1812.

Zdieľaný kľúč

Server a klient zdieľajú kľúč ktorý sa používa na overovanie správ medzi nimi. Obe strany musia mať nakonfigurovaný ten istý kľúč.

Zopakovať zdieľaný kľúč

Zadajte kľúč ešte raz.

3.6.4 UPnP

UPnP (Universal Plug and Play) protokol je podporovaný, aby umožnil inštalovať zariadenia pripojenie na sieť s ľahkosťou, s akou sa inštalujú periférie počítača pomocou už existujúceho Windowsového Plug and Play systému. Pre routery NAT je hlavnou súčasťou UPnP "NAT Traversal". NAT Traversal umožňuje aplikáciám pred firewallom automaticky otvárať porty ktoré potrebujú. Je to spoľahlivejšie ako vyžadovať od routera aby sám určil ktoré porty majú byť otvorené. Okrem toho užívateľ nemusí manuálne nastavovať združovanie portov alebo DMZ. UPnP je k

dispozícii na Windows XP a router poskytuje potrebnú podporu plnému využitiu hlasových, video možností i správ na MSN Messengeri.

Aplikácie >> UPnP

UPnP

- ☒ Aktivovať UPnP službu
- ☒ Aktivovať službu kontroly pripojenia
- ☒ Aktivovať službu stavu pripojenia

Poz.: Ak hodľate mať spustenú UPnP službu vo vnútri vašej LAN, je treba zaskrtnúť príslušné služby aby bola povolená kontrola uvedených služieb, tak ako aj príslušné UPnP nastavenia.

OK

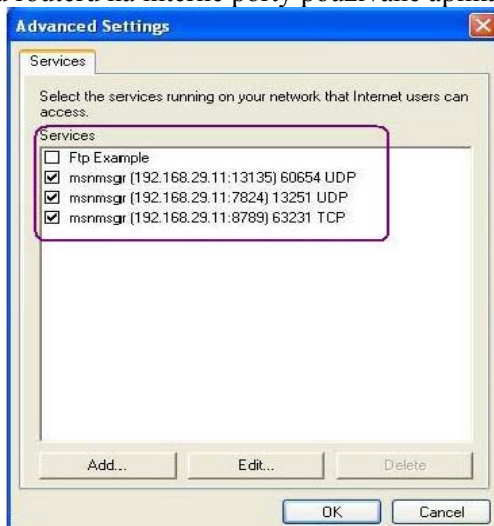
Vymazať

Zrušiť

Aktivovať UPnP službu Môžete aktivovať buď službu kontroly pripojenia službu stavu pripojenia. Ak nastavíte Aktivovať UPnP službu zobrazí sa ikona IP Broadband Connection on Router on Windows XP/Network Connections. Stav pripojenia a stav riadenia môže byť aktivovaný. NAT Traversal UpnP umožňuje multimediálnym príslušenstvám aplikácií pracovať. Združovanie portov je nastavené manuálne alebo inou metódou. Obrázky ukazujú možnosti tohto zariadenia.



Zariadenie UPnP v routeri umožňuje aplikáciám, ktoré poznajú UPnP, ako MSN Messenger, zistiť čo sa nachádza za routerom NAT. Aplikácia spozná aj externú IP adresu a nakonfiguruje mapovanie portov na routery. Následne toto zariadenie prepošle pakety z externého portu routeru na interné porty používané aplikáciou.



Nemôže pracovať s firewallovým softvérom

Povolenie firewallových aplikácií na vašom PC môže spôsobiť, že UPnP nebude pracovať správne. Je to z toho dôvodu, že tieto aplikácie zablokujú možnosť prístupu na niektoré porty.

Bezpečnosť

Aktivácia funkcie UPnP vo vašej sieti môže spôsobiť ohrozenie bezpečností. Preto pred jej aktiváciou by ste mali zvážiť riziká.

niektoré operačné systémy Microsoft zistili slabosti UPnP, preto by ste mali mať stiahnuté všetky ServicePacks a záplaty

neprivilegovaní užívatelia môžu riadiť niektoré funkcie routera, ako pridávanie a odstraňovanie mapovaní portov. UPnP dynamicky pridáva mapovania na základe UPnP aplikácií. Ak sa aplikácie neukončia riadne tieto mapovania nesmú byť odstránené.

3.6.5. IGMP

IGMP je skratka pre Internet Group Management Protocol. Je to komunikačný protokol využívaný hlavne na riadenie členstva v skupinách Internet Protocol multicast. Aby ste spustili službu IGMP Snooping, zaškrtnite Zapnut IGMP Proxy

Aplikácie >> IGMP

IGMP

☐ Zapnut IGMP Proxy

IGMP Proxy pracuje ako multicast proxy pre hostiteľov v LAN. Zapnite IGMP Proxy, ak nebude prístup do žiadnej multicast skupiny. Ale táto funkcia **nema žiadny efekt ak je aktivovaný Bridge mod.**

☐ Zapnut IGMP Snooping

Zapnutie IGMP Snooping, multicast prenosu je iba presmerovanie na porty ktoré majú členstvo v tejto skupine.

Vypnutím IGMP snooping, multicast prenos vychádza z toho istého spôsobu ako broadcast prenos.

OK

Zrušiť

| [Refresh](#) |

Pracovne Multicast Skupiny

Index	Group ID	P1	P2	P3	P4
-------	----------	----	----	----	----

Zapnúť IGMP Proxy

Zaškrtnite, ak chcete povoliť funkciu. Aplikácia multivysielania bude vykonaná cez port WAN siete.

Zapnúť IGMP Snooping

Zaškrtnite, ak chcete povoliť funkciu. Aplikácia multivysielania bude vykonaná pre klientov miestnej siete.

Group ID

Toto pole zobrazuje ID portu skupiny multivysielania. Rozsah začína od 224.0.0.0 do 239.255.255.254.

P1 až P4

It indicates the LAN port used for the multicast group.

Refresh

Click this link to renew the working multicast group status.

Ak zaškrtnete len Zapnúť IGMP Proxy, dostanete sa na nasledujúcu stránku. Všetky multicast skupiny budú v zozname a všetky LAN porty (P1 až P4) sú použiteľné.

Ak zaškrtnete len Zapnúť Snooping, dostanete sa na nasledujúcu stránku. Aj keď budú v zozname všetky skupiny, všetky LAN porty (P1 až P4) nie sú použiteľné.

Working Multicast Groups					
Index	Group ID	P1	P2	P3	P4
1.	224.0.0.9	v	v	v	v
2.	239.255.255.250	v	v	v	v
3.	225.0.0.1	v	v	v	v

3.6.6. Wake on LAN

Použitím tejto funkcie je možné zobudiť PC zo spánku. Túto funkciu musí podporovať aj sieťová karta v PC a musí byť aktivovaná.

Aplikácie >> Wake on LAN

Wake on LAN (Zobudenie po sieti)

Poz.: Wake on LAN integrované s [Spojit IP s MAC](#) funkciou, iba spojené počítače sa môžu zobudiť použitím zobudenia cez IP.

Zobudiť pomocou:

MAC adresa ▼

IP adresa:

--- ▼

MAC adresa:

: : : : :

Zobudiť!

Výsledok

3.7 VPN a vzdialený prístup

VPN a vzdialený prístup

- Riadenie vzdialeného prístupu
- PPP hlavné nastavenie
- IPSec hlavné nastavenie
- IPSec Peer totožnosť
- Vzdialené prihlasený užívateľ
- LAN to LAN
- Správa spojenia

Virtual Private Network (virtuálna súkromná sieť - VPN) je rozšírenie súkromnej siete, ktoré zahŕňa linky zo zdieľaných alebo verejných sietí ako Internet. V skratke touto technológiou môžete posilať dáta z počítača na počítač cez verejnú alebo zdieľanú sieť spôsobom ako by šlo o súkromnú linku point-to-point. Router Vigor 2700VoIP umožňuje simultánne používanie 2 VPN tunelov.

3.7.1 Riadenie vzdialeného prístupu

Povoľte službu VPN, ak potrebujete. Ak zamýšľate prevádzkovať VPN server v rámci vašej miestnej siete, mali by ste zakázať službu VPN routera Vigor, aby ste umožnili prechod VPN tunela, ako aj nastavenie NAT ako napr. DMZ alebo Otvorenie portov.

Nastavenie kontroly vzdialeneho pristupu

- ☒ Aktivovat PPTP VPN sluzbu
- ☒ Aktivovat IPSec VPN sluzbu
- ☒ Aktivovat L2TP VPN sluzbu
- ☐ Aktivovat ISDN Dial-In

Poz.: Ak chcete aby fungoval VPN server vo vasej LAN, je potrebne odznacit potrebny protokol, aby bol povoleny prechod pre danu sluzbu, tak ako aj prislusne NAT nastavenie.

OK Vymazat Zrusit

- Aktivovat' PPTP VPN Službu Zaškrtnite, ak chcete aktivovat' službu VPN cez PPTP protokol.
- Aktivovat' IPSec VPN Službu Zaškrtnite, ak chcete aktivovat' službu VPN cez IPSec protokol.
- Aktivovat' L2TP VPN Službu Zaškrtnite, ak chcete aktivovat' službu VPN cez L2TP protokol. .
- Aktivovat' ISDN Dial-IN Toto políčko bude výhodné pre užívateľov v Európe.

3.7.2 PPP Hlavné nastavenie

Toto menu je aplikovateľné len na pripojenia VPN spojené s PPP ako napr. PPTP, L2TP, L2TP cez IPSec.

VPN a vzdialeny pristup >> PPP hlavne nastavenie

PPP hlavne nastavenie

PPP/MP Protokol	Pridelovanie IP adres pre Dial-In uzivatelov
Overovanie volania dnu PAP alebo CHAP	Start IP adresa 192.168.1.200
PPP kryptovanie volania dnu(MPPE) Bezne MPPE	
Vzajomne overovanie (PAP) <input type="radio"/> Ano <input checked="" type="radio"/> Nie	
Uzivateľske meno	
Heslo	

OK

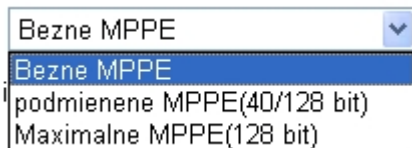
Overovanie volania dnu
Authentication PAP Only
PAP or CHAP

Zvoľte túto možnosť, ak chcete aby router overil volanie dnu. používateľa s PAP protokolom.

Zvolenie tejto možnosti znamená, že router bude autentifikovať dial-in užívateľov najskôr protokolom CHAP. Ak užívateľ tento protokol nepodporuje, použije router na autentifikáciu PAP protokol.

PPP kryptovanie volania dnu MPPE

Táto možnosť znamená, že router použije pri vzdialenom dial-in užívateľovi kódovaciu metódu MPPE. Ak vzdialený dial-in užívateľ túto metódu nepodporuje, router vyšle pakety „no MPPE encrypted (nekódované MPPE)“. Inak bude na kódovanie dát použitá kódovacia schéma MPPE.



Požadovať MPPE (40/128bits)	– Zvolením tejto možnosti prikážete routeru kódovať pakety kódovacím algoritmom MPPE. Okrem toho vzdialený užívateľ použije na kódovanie 128 bitové kódovanie namiesto 40 bitového. Inými slovami, ak nie je dostupná 128 bitová metóda bude použitá 40 bitová. Maximum MPPE – Táto možnosť indikuje, že router použije na kódovanie len schému s maximom bitov (128 bitov).
Vzájomné overovanie	Táto funkcia sa používa najmä pri iných routeroch alebo klientoch, ktorí potrebujú dvojsmernú autentifikáciu za účelom vyššej úrovne bezpečnosti, napríklad routery Cisco. Ak váš router vyžaduje vzájomnú autentifikáciu, mali by ste túto funkciu povoliť. Okrem toho by ste mali zadať Užívateľské meno a heslo.
Štart IP Adresa	Zadajte počiatočnú IP adresu dial-in PPP pripojenia. Mali by ste zvoliť IP adresu z vašej súkromnej siete. Napríklad, ak adresa vašej siete je 192.168.1.0/255.255.255.0, mali by ste zvoliť ako počiatočnú IP adresu 192.168.1.200. Ale nezabudnite, že prvé dve adresy 192.168.1.200 a 192.168.1.201 sú rezervované pre užívateľa dial-in ISDN.

3.7.3 IPSec hlavné nastavenie

Vo všeobecnom nastavení IPSec sa nachádzajú dve hlavné časti konfigurácie.

IPSec má dve fázy

- Fáza 1: dohodnutie parametrov IKE vrátane kódovania, rušenia, hodnôt parametrov Diffie-Hellman, dobu ochrany nasledujúcich IKE výmen, autentifikácia oboch peerov, ktoré používajú buď spoločný kľúč alebo digitálny podpis (x.509). Peer, ktorý začne dohadovanie podá návrh postupu vzdialenému peeru a vzdialený peer sa snaží nájsť adekvátny postup s najvyššou prioritou. Nakoniec je nastavený bezpečný tunel pre Fázu 2.
- Fáza 2: dohodnutie bezpečnostných metód IPSec vrátane autentifikačnej hlavičky (Authentication Header (AH)) alebo Encapsulating Security Payload (ESP), pre nasledujúcu výmenu IKE a vzájomné preskúšanie zriadeného bezpečného tunela.

Existujú dve metódy zapúzdrenia, ktoré sú používané v IPSec, Transport a Tunnel. Transportný režim pridá AH/ESP objem a použije originálnu IP hlavičku aby zapúzdрил len objem dát. Môže to byť aplikované len na miestny paket, napríklad L2TP cez IPSec. Tunelový režim nielen pridá objem AH/ESP ale použije aj novú (tunelovú) IP hlavičku aby zapúzdрил pôvodný IP paket. Autentifikačná hlavička (Authentication Header (AH)) poskytuje autentifikáciu dát integrity IP paketov poslaných medzi dvomi VPN peermi. Na to slúži kľúčová funkcia jednosmerného rozdelenia, ktorá vytvorí súhrn správ. Tento súhrn je pridaný do AH a vysielaný spolu s paketmi. Na strane príjemateľa prebehne rovnaké rozdelenie a hodnoty sa porovnajú s hodnotami v prijatej AH. Encapsulating Security Payload (Zapúzdrujúci bezpečnostný objem - ESP) je bezpečnostný protokol, ktorý dátam poskytuje dôvernitosť a ochranu s možnosťou autentifikácie a detekcie opakovania.

VPN IKE/IPSec hlavne nastavenie

Nastavenie volania dnu pre vzdialene prihlaseneho uzivatela a dynamickeho IP klienta (LAN to LAN).

IKE overovacia metoda
 Zdielany kluc
 Zopakovat zdielany kluc
IPSec bezpecnostna metoda
☒ Stredne (AH)
 Data budu overovane, ale nebudu kryptovane.
 Vysoke (ESP) ☒ DES ☒ 3DES ☒ AES
 Data budu kryptovane a overovane.

Autentifikačná metóda IKE Zvyčajne sa aplikuje na tých vzdialených dial-in užívateľov alebo uzly (LAN-to-LAN), ktoré používajú dynamickú IP adresu a pripojenie VPN vzťahujúce sa na IPSec – pripojenia ako L2TP cez IPSec a IPSec tunel.

Zdieľaný kľúč špecifikujete kľúč na IKE overenie.

Zopakovať zdieľaný kľúč zadajte kľúč znova.

IPSec bezpečnostná metóda Stredne(AH) dáta budú overované ale nebudú kryptované Vysoké (ESP) – dáta budú overované i kryptované. Môžete si stanoviť kryptovací Data Encryption Standard (DES), Triple DES (3DES) a AES.

3.7.4 IPSec Peer totožnosť

Tu môžete upravovať tabuľku certifikátov peer, ak chcete používať digitálne certifikáty na autentifikáciu peerov v pripojení LAN-to-LAN alebo vzdialenom dial-in pripojení.

VPN a vzdialeny pristup >> IPSec Peer totoznost

X509 Peer ID ucty:

[Vyrobné nastavenie](#)

Index	Meno	Index	Meno
1.	???	9.	???
2.	???	10.	???
3.	???	11.	???
4.	???	12.	???
5.	???	13.	???
6.	???	14.	???
7.	???	15.	???
8.	???	16.	???

<< [1-16](#) | [17-32](#) >>

[Dalej](#) >>

Výrobné nastavenia

Kliknite, ak chcete vymazať všetky indexy.

Index

Kliknite na číslo v stĺpci Index, ak chcete vstúpiť na stránku nastavení totožnosti IPSec Peer.

Meno

Zobrazí meno indexu.

Ďalej

Kliknite na odkaz a vstúpte na ďalšiu stránku pre nastavenie viacerých účtov.

Kliknite na každý index, ak chcete upraviť digitálny certifikát peeru. Sú tri úrovne bezpečnosti autentifikácie digitálnym podpisom. Vyplňte každé pole, aby ste autentifikovali vzdialený peer. Nasledujúce vysvetlenie vás

prevedie vyplňaním polí

VPN a vzdialeny pristup >> IPSec Peer totoznost

Profile Index : 1

Meno profilu	???
<input checked="" type="radio"/> Neakceptovat ziadne Peer ID	
<input type="radio"/> Akceptovat alternativne meno osoby	
Typ	IP Adresa ▼
IP	
<input type="radio"/> Akceptovat meno osoby	
Krajina (C)	
Stat (ST)	
Miesto (L)	
Organizacia (O)	
Organizacna jednotka (OU)	
Bezne meno (CN)	
Email (E)	

OK

vymazat

Zrusit

Meno profilu

Zadajte meno profilu.

Akceptovat' každé Peer ID

Zakliknite, ak chcete akceptovat' každý peer nezávisle na identite.

Akceptovat' alternativne
meno osoby

Zakliknite, ak chcete akceptovat' jedno špecifické pole

digitálneho podpisu peeru so zodpovedajúcou hodnotou. Môže to byť IP adresa, doména alebo e-mailová adresa. Pole pod poľom typ sa zobrazí na základe zvoleného typu.

Akceptovat' meno osoby

Zakliknite, ak chcete akceptovat' špecifické polia digitálneho podpisu peeru s zodpovedajúcou hodnotou. Pole zahŕňa krajinu (C), štát (ST), miesto (L), organizácia (O), organizačná jednotka (OU), bežné meno (CN), and Email (E).

3.7.5 Vzdialene prihlásený užívateľ

Môžete riadiť vzdialený prístup tabuľkou účtov vzdialených užívateľov, takže užívatelia môžu byť autentifikovaní pri dial-in alebo nadviazať spojenie VPN. Môžete nastaviť parametre vrátane upresneného spojenia peerID, typ pripojenia (VPN vrátane PPTP, IPSec Tunel a L2TP samotné alebo cez IPSec) a zodpovedajúce bezpečnostné metódy apod.

Router poskytuje 32 prístupových účtov užívateľov dial-in. Pritom môžete rozšíriť účty na RADIUS server cez zabudovanú funkciu RADIUS klient. Nasledujúci obrázok znázorňuje sumárnu tabuľku.

Ucty vzdialenych uzivatelov:

[Nastavit do vyrobneho nastavenia](#) |

Index	Uzivatel	Stav	Index	Uzivatel	Stav
1.	???	x	9.	???	x
2.	???	x	10.	???	x
3.	???	x	11.	???	x
4.	???	x	12.	???	x
5.	???	x	13.	???	x
6.	???	x	14.	???	x
7.	???	x	15.	???	x
8.	???	x	16.	???	x

<< [1-16](#) | [17-32](#) >>[Dalej](#) >>**Stav:** v --- Aktivny, x --- Neaktivny

Nastavit' do výrobného nastavenia Kliknite, ak chcete vymazať všetky indexy.

Index Kliknite na číslo indexu, aby ste vstúpili na stránku nastavenia užívateľa vzdialeného.

Užívateľ Zobrazuje užívateľské meno dial-in užívateľa účtu LAN-to-LAN. Symbol ??? znamená, že účet je prázdny.

Stav Zobrazuje stav prístupu určitého užívateľa. Symbol V a X znázorňuje či je užívateľ aktívny alebo neaktívny.

Ďalej Kliknite na Ďalej pre vstup na ďalšiu stránku na nastavenie viacerých účtov.

Kliknite na každý index, ak chcete upraviť účet jedného vzdialeného užívateľa. Každý typ Dial-in vyžaduje vyplnenie zodpovedajúcich polí vpravo. Ak sú polia šedé, znamená to, že ich môžete nechať prázdne. Nasledujúce vysvetlenie vás prevedie vyplňaním dôležitých polí.

Index c. 1

Uzivatel'sky ucet a overovanie <input checked="" type="checkbox"/> Aktivovat tento ucet Odpojit po <input type="text" value="300"/> sek.(s)		Uzivatelske meno <input type="text" value="david"/> Heslo <input type="password" value="....."/>
Typ povoleného volania dnu <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec Tunel <input checked="" type="checkbox"/> L2TP s IPSec politikou <input type="text" value="Ziadna"/>		IKE overovacia metóda <input checked="" type="checkbox"/> Zdielany kluc IKE zdielany kluc <input type="text"/> <input checked="" type="checkbox"/> Digitalny podpis (X.509) <input type="text" value="???"/>
<input type="checkbox"/> Specifikovat vzdialeny uzol IP vzdialeneho klienta alebo ISDN cislo <input type="text"/> alebo lokalne ID <input type="text"/>		IPSec bezpecnostna metoda <input checked="" type="checkbox"/> Stredna (AH) Vysoka (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Lokalne ID <input type="text"/> (volitelne)
Funkcia spatneho volania <input type="checkbox"/> Aktivovat funkciu spatne volanie <input type="checkbox"/> Aktivovat cislo spatneho volania Cislo spatneho volania <input type="text"/> <input checked="" type="checkbox"/> Aktivovat kontrolu poplatkov spatneho volania Poplatky spatneho volania <input type="text" value="30"/> min.(s)		

Aktivovať tento účet

Zaškrtnite, ak chcete povoliť funkciu.

Odpojiť po- Ak je užívateľ nečinný po limite, router zruší pripojenie. Predvolené nastavenie je 300 sekúnd.

ISDN

Povolíte vzdialené pripojenie ISDN dial-in. Môžete aj nastaviť funkciu spätného volania. Mali by ste nastaviť Užívateľské meno a heslo vzdialeného užívateľa. Toto príslušenstvo obsahuje len model i.

PPTP

Umožníte vzdialenému užívateľovi vytvoriť pripojenie PPTP VPN cez internet. Natavte užívateľské meno a heslo

IPSec Tunel

Umožníte vzdialenému užívateľovi vytvoriť IPSec VPN pripojenie cez internet

L2TP

Umožníte vzdialenému užívateľovi vytvoriť pripojenie L2TP VPN cez Internet. Môžete zvoliť L2TP samotné alebo s IPSec. Zvoľte si spomedzi:

Žiadna – Neaplikuje politiku IPSec. Vzhľadom k tomu môže byť pripojenie VPN s L2TP bez IPSec politiky zobrazené ako jediné L2TP pripojenie. Pekné mať – aplikuje najprv politiku IPSec, ak je počas vyjednávania aplikovateľná. V inom prípade pripojenie VPN ostane len L2TP. Musí – určite IPSec politiku, aby bola určite aplikovaná na L2TP pripojenie.

Špecifikovať vzdialený uzol

Zaškrtnite políčko – môžete špecifikovať IP adresu vzdialeného užívateľa alebo peer ID (použitím agresívneho režimu IKE).

Nezaškrtnite políčko – zvolený typ pripojenia použije bezpečnostné a autentifikačné metódy nastavené v hlavnom nastavení.

Užívateľské meno	Toto pole je aplikovateľné, ak zvolíte PPTP alebo L2TP s/bezIPSec politiky.
Heslo	Toto pole je aplikovateľné, ak zvolíte PPTP alebo L2TP s/bezIPSec politiky.
Overovacia metóda IKE	Táto skupina polí je aplikovateľná na IPSec Tunely a L2TP s IPSec Politikou, ak upresníte IP adresu vzdialeného uzla. Jediná výnimka je digitálny podpis (X.509). Môže byť nastavený ak zvolíte IPSec tunel s/bez upresnenia IP adresy vzdialeného uzla. Zdieľaný kľúč – Zaškrtnite, ak chcete spustiť funkciu a zadajte požadované znaky (1-63). Digitálny podpis (X.509) – Zaškrtnite, ak chcete spustiť túto funkciu a zvolte si preddefinovaný v účtoch X.509 Peer ID.
IPSec bezpečnostná metóda	Táto skupina polí je nevyhnutná pre IPSec Tunely a L2TP s IPSec politikou, keď upresníte vzdialený uzol. Aby ste zvolili bezpečnostnú metódu, zaškrtnite Medium, DES, 3DES alebo AES. Stredná (AH) znamená, že dáta budu overené, ale nie kódované. Toto je predvolená možnosť. Môžete odškrtnúť políčko, ak ju chcete zakázať. Vysoká - means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it. Vysoká (ESP) znamená, že objem (dáta) budú overené a zakódované. Môžete si zvoliť kódovací algoritmus Data Encryption Standard (DES), Triple DES (3DES) a AES. Miestne ID –upresnite miestne ID ktoré má byť použité na nastavenie dial-in v nastavení účtu LAN-to-LAN. Táto položka je voliteľná a môže byť použitá len v agresívnom režime IKE.
Funkcia spätné volanie	Táto funkcia poskytuje službu spätného volania len pre užívateľa ISDN (model i). Vlastníkovi routeru bude telekomom zaúčtovaný poplatok za pripojenie. Zaškrtnite, ak chcete funkciu povoliť. Špecifikujte číslo spätného volania – slúži na vyššiu bezpečnosť. Ak špecifikujete číslo, router bude volať späť len na zadané číslo. Aktivovať kontrolu poplatkov spätného volania – upresnite časový rozpočet pre užívateľa. Rozpočet bude automaticky znížený pri pripojení spätným volaním.

3.7.6 LAN to LAN

Tu môžete spravovať pripojenia LAN-to-LAN pomocou tabuľky účtov pripojenia. Môžete nastaviť parametre vrátane smerovania pripojenia (dial-in – dnu alebo dial-out - von), peer ID, typ pripojenia (VPN s PPTP, IPSec Tunel a L2TP samotne alebo s IPSec) a zodpovedajúce bezpečnostné metódy atď.

Router poskytuje 32 účtov, čo znamená že podporuje 32 VPN tunelov súčasne. Nasledujúci obrázok znázorňuje sumárnu tabuľku

VPN a vzdialeny pristup >> LAN to LAN

LAN-to-LAN profily:

[Nastaviť do výrobného nastavenia](#)

Index	Meno	Stav	Index	Meno	Stav
1.	???	x	9.	???	x
2.	???	x	10.	???	x
3.	???	x	11.	???	x
4.	???	x	12.	???	x
5.	???	x	13.	???	x
6.	???	x	14.	???	x
7.	???	x	15.	???	x
8.	???	x	16.	???	x

<< [1-16](#) | [17-32](#) >>

[Dalej](#) >>

Stav: v --- Aktivne, x --- Neaktivne

Nastaviť do výr. nastavenia	Kliknite, ak chcete vymazať všetky indexy.
Meno	Indikuje meno účtu LAN-to-LAN. Symbol ??? ukazuje že účet je prázdny.
Stav	Indikuje stav individuálneho účtu. Symboly V a X ukazujú, či je účet aktívny alebo neaktívny.

Kliknite na každý index, ak chcete upraviť účet a dostanete sa na ďalšiu stránku. Každý účet zahŕňa 4 podskupiny. Ak sú polia šedé, znamená to, že ich môžete nechať voľné. Nasledujúci výklad vás prevedie vyplnením dôležitých polí:

VPN a vzdialený prístup >> LAN to LAN

Profil Index : 1

Bezne nastavenie

Meno profilu <input type="text" value="draytek"/> <input checked="" type="checkbox"/> Aktivovať tento profil	Smer volania <input checked="" type="radio"/> Obidva <input type="radio"/> Von <input type="radio"/> Dnu <input type="checkbox"/> Vždy zapnutý Vypnut po <input type="text" value="300"/> sec.(s) <input type="checkbox"/> Aktivovať PING aby tunel zostal aktívny PING na IP <input type="text"/>
---	--

Nastavenie volania von

Typ volaného servra <input type="radio"/> ISDN <input type="radio"/> PPTP <input type="radio"/> IPSec tunel <input checked="" type="radio"/> L2TP s IPSec politikou <input type="text" value="Musi"/>	Typ linky <input type="text" value="64k bps"/> Užívateľské meno <input type="text" value="???"/> Heslo <input type="text"/> PPP overovanie <input type="text" value="PAP/CHAP"/> VJ komprimácia <input checked="" type="radio"/> On <input type="radio"/> Off
Server IP/Host meno pre VPN. (ako draytek.com alebo 123.45.67.89) <input type="text" value="172.16.3.112"/>	IKE overovacia metóda <input checked="" type="radio"/> Zdieľaný kľúč <input type="text" value="IKE zdieľaný kľúč"/> <input type="text"/> <input type="radio"/> Digitálny podpis(X.509) <input type="text" value="???"/>
	IPSec bezpečnostná politika <input checked="" type="radio"/> Stredná(AH) <input type="radio"/> Vysoká (ESP) <input type="text" value="DES bez overovania"/> <input type="text" value="Rozšírenie"/>
	Index(1-15) v Planovaci Nastavenie: <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
	Funkcia spätneho volania (CBCP) <input type="checkbox"/> Vyzaduje vzdialene spatne volanie <input type="checkbox"/> Poskytnut ISDN cislo vzdialenej strane

Meno profilu	Meno profilu pripojenia.
Aktivovať tento profil	Zaškrtnite, ak chcete aktivovať tento profil.
Smer volania	Zadajte povolený smer volania tohoto LAN-to-LAN profilu: Obidva- iniciátor/odpovedajúci Von – len iniciátor Von – len odpovedajúci

Vždy zapnutý alebo Vypnúť po – Vždy zapnutý – zaškrtnite, ak chcete trvalé pripojenie VPN. Vypnúť po – predvolená hodnota je 300 sekúnd. Ak je pripojenie nečinné nad túto hodnotu, router pripojenie zruší.

Aktivovať PING aby tunel zostal aktívny – Táto funkcia pomáha routeru predurčiť stav IPSec VPN pripojenia, je najmä užitočná v prípade nezvyklého narušenia tunelu. Pre podrobnejšie informácie viď poznámka nižšie. Zaškrtnite aktivovať prenos PINGových paketov určitej IP adresy. Zadajte IP adresu vzdialeného hostiteľa umiestneného na druhom konci tunela.

PING na IP

Poznámka:

Aktivovať PING aby tunel zostal aktívny sa používa pri nezvyklom prerušení IPSec VPN pripojenia. Poskytne stav pripojenia VPN, aby sa router rozhodol či bude volať znova. Keď chce za normálnych okolností jeden peer ukončiť spojenie, mala by nasledovať výmena paketov, aby sa navzájom informovali. Ak sa odpojí vzdialený peer bez upozornenia, router Vigor nebude vedieť vyhodnotiť situáciu. Pre riešenie tejto dilemy router kontinuálnym posielaním paketov spozná skutočný stav spojenia a správne konať. Je to nezávislé od DPD (dead peer detection – mŕtva detekcia peeru).

ISDN

Nadviaže ISDN spojenie so serverom. Mali by ste nastaviť typ linky a identitu ako užívateľské meno a heslo pre overenie vzdialeného serveru. Môžete ďalej nastaviť spätné volanie (CBCP). Toto príslušenstvo je užitočné len pre model i.

PPTP

Nadviaže PPTP VPN spojenie so severom cez internet. connection to the server through the Internet. Mali by ste nastaviť typ linky a identitu ako užívateľské meno a heslo pre overenie vzdialeného serveru.

IPSec Tunel

Nadviaže so serverom spojenie IPSec VPN cez Internet.

L2TP s ...

Nadviaže spojenie L2TP VPN cez Internet. Môžete zvoliť samotné L2TP alebo s IPSec. Žiaden: Neaplikuje IPSec politiku. Vzhľadom na to spojenie VPN figuruje ako samostatné L2TP spojenie. Pekné mať: Aplikuje najskôr politiku IPSec počas vyjednávania. V opačnom prípade volanie von cez spojenie VPN bude samostatné spojenie L2TP. Musí: IPSec politika bude určite aplikovaná na spojenie L2TP.

Užívateľské meno

Toto pole je aplikovateľné, ak zvolíte PPTP alebo L2TP s alebo bez IPSec politiky.

Heslo

Toto pole je aplikovateľné, ak zvolíte PPTP alebo L2TP s alebo bez IPSec politiky.

PPP overovanie

Toto pole je aplikovateľné, ak zvolíte PPTP alebo L2TP s alebo bez IPSec politiky. PAP/CHAP je najbežnejšia možnosť pri dvojkovej kompatibilite.

VJ komprimácia

Toto pole je aplikovateľné, ak zvolíte PPTP alebo L2TP s alebo bez IPSec politiky. VJ komprimácia jej používaná pre protokolovú hlavičku TCP/IP protokolu. Normálne sa nastavuje na Áno, aby bolo zlepšené využitie šírky pásmového prenosu.

IKE overovacia metóda

Táto skupina polí je aplikovateľná na IPSec Tunely a L2TP s IPSec politikou. Zdieľaný kľúč - zadajte 1-63 znakov kľúča. Digitálny podpis (X.509) – určte jeden z preddefinovaných X.509 Peer ID profilov.

IPSec bezpečnostná metóda

Táto skupina polí je nevyhnutná pre IPSec Tunely a L2TP s IPSec politikou.

Stredná

Overovacia hlavička Authentication Header (AH) znamená, že dáta budú overené, ale nie kódované. Táto voľba je predvolená ako aktívna.

Vysoká (ESP-Encapsulating Security Payload)- znamená, že objem (dáta) budú zakódované a overené. Zvoľte: DES bez overenia –použije DES kódovací algoritmus a nepoužije žiadnu overovaciu schému. DES s overením – použije kódovací algoritmus DES a MD 5 alebo SHA-1 overovací algoritmus. 3DES without Authentication-Use triple DES encryption algorithm and not apply any authentication scheme. 3DES s overením-použije trojitý algoritmus kódovania DES a aplikuje MD5 alebo SHA-1 overovací algoritmus. AES bez overenia- použije kódovací algoritmus AES encryption algorithm a neaplikuje žiadnu overovaciu schému. AES s overením –použije algoritmus kódovania AES a aplikuje MD5 alebo SHA-1 overovací algoritmus.

Rozšírené

Upresní mód, návrh a životnosť kľúča každej IKE fázy, bránu atď. Okno rošíreného nastavenia je znázornené nižšie:

http://192.168.1.1 - IKE rozsirene nastavenie - Microsoft Internet Explorer

IKE rozsirene nastavenie

Mod IKE fazy 1	<input checked="" type="radio"/> Zakladny mod	<input type="radio"/> Agresivny mod
Navrh IKE fazy 1	DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2 ▼	
IKE faza 2 navrh	HMAC_SHA1/HMAC_MD5 ▼	
Faza 1 zivotnosti IKE kluca	28800	(900 ~ 86400)
Faza 2 zivotnosti IKE kluca	3600	(600 ~ 86400)
Navrh dokonalého kluca	<input checked="" type="radio"/> Vypnut	<input type="radio"/> Zapnut
Lokalne ID	<input type="text"/>	

OK Close

Hotovo Internet

- Mód IKE fázy 1** Zvoľte základný alebo agresívny mód. Výstupom je výmena bezpečnostných návrhov, aby bol vytvorený bezpečný kanál. Základný mód je bezpečnejší ako agresívny, pretože pri viac výmen je realizovaných bezpečným kanálom pre nastavenie IPSec session. Agresívny mód je rýchlejší. Predvolený je základný mód.
- Návrh IKE fázy 1** navrhne miestnu dostupnú schému overenia a algoritmus kódovania VPN peerom a prijme odozvu, aby našiel zhodu. Sú dostupné dve kombinácie pre agresívny a deväť pre základný mód. Navrhujeme, aby ste zvolili kombináciu, ktorá pokryje čo najviac schém.
- Návrh IKE fázy 2** navrhne miestnu dostupnú schému overenia a algoritmus kódovania VPN peerom a prijme odozvu, aby našiel zhodu. Sú dostupné tri kombinácie pre každý mód. Navrhujeme, aby ste zvolili kombináciu, ktorá pokryje čo najviac algoritmov.
- Fáza 1 životnosti IKE kľúča** mala by byť definovaná z bezpečnostných dôvodov. Predvolená hodnota je 28800 sekúnd. Môžete zadať hodnotu medzi 900 a 86400 sekundami.
- Fáza 2 životnosti IKE kľúča** by byť definovaná z bezpečnostných dôvodov. Predvolená hodnota je 3600 sekúnd. Môžete zadať hodnotu medzi 900 a 86400 sekundami.
- Návrh dokonalého kľúča (PFS)**- kľúč IKE Fázy 1 bude znova použitý, aby bolo predídene komplikovanosti spracovania v druhej fáze. Predvolená hodnota je nečinná.
- Lokálne ID** v agresívnom móde slúži lokálne ID namiesto IP adresy počas overovania so vzdialeným VPN serverom. Dĺžka je obmedzená na 47 znakov.
- Funkcia spätného volania (iba i modely)** táto funkcia poskytuje službu spätného volania oddelene od PPP len pre užívateľov ISDN volania dnu. Vlastníkovi routera bude účtovaný poplatok za pripojenie telekomunikačnou spoločnosťou.
- Vyžadovať spätné volanie od vzdialeného** – Aktivujte, ak chcete aby router vyžadoval vzdialený peer aby volal späť na neskoršie spojenie.

Nastavenia volania dnu

Typ povoleného volania dnu	
<input checked="" type="checkbox"/> ISDN	
<input checked="" type="checkbox"/> PPTP	
<input checked="" type="checkbox"/> IPSec tunel	
<input checked="" type="checkbox"/> L2TP s IPSec politikou	Musi <input type="button" value="v"/>
<input type="checkbox"/> Specifikovať Vzdialenu VPN branu alebo IP pripájneho VPN servera <input type="text"/> alebo lokálne ID <input type="text"/>	
Užívateľské meno <input type="text" value="???"/> Heslo <input type="text"/> VJ komprimácia <input checked="" type="radio"/> On <input type="radio"/> Off	
IKE overovacia metóda <input checked="" type="checkbox"/> Zdieľaný kľúč <input type="button" value="IKE zdieľaný kľúč"/> <input type="text"/> <input type="checkbox"/> Digitálny podpis(X.509) <input type="text" value="???"/> <input type="button" value="v"/>	
IPSec bezpečnostná politika <input checked="" type="checkbox"/> Vysoká (AH) Vysoká (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES	
Funkcia spätného volania (CBCP) <input type="checkbox"/> Aktivovať funkciu spätného volania <input type="checkbox"/> Použiť nasledujúce číslo pre spätné volanie Číslo spätného volania <input type="text"/> Poplatky spätného volania <input type="text" value="0"/> min.(s)	
Nastavenie TCP/IP siete	
Moja WAN IP	<input type="text" value="0.0.0.0"/>
IP vzdialenej brány	<input type="text" value="0.0.0.0"/>
IP vzdialenej siete	<input type="text" value="0.0.0.0"/>
Maska vzdialenej siete	<input type="text" value="255.255.255.0"/>
	<input type="button" value="Viac"/>
RIP smerovanie	<input type="button" value="TX/RX obidva"/> <input type="button" value="v"/>
RIP verzia	<input type="button" value="Ver. 2"/> <input type="button" value="v"/>
Pre NAT operácie, zaobchádzať so vzdialenou podsietou ako s <input type="button" value="Privatná IP"/> <input type="button" value="v"/>	
<input type="checkbox"/> Zmeniť štandardnú cestu cez tento tunel	

Typ povoleného volania dnu
ISDN

PPTP

IPSec Tunel
L2TP s ...

Predurčí spojenie volaním dnu rozličným typom.
 Povolí ISDN volanie dnu . Môžete nastaviť funkciu spätného volania. Mali by ste nastaviť užívateľské meno a heslo pre overenie vzdialeného používateľa volajúceho dnu. Toto prísľušenstvo je užitočné len pre model i.
 Povolí PPTP VPN spojenie cez internet. Mali by ste nastaviť užívateľské meno a heslo pre overenie vzdialeného používateľa volajúceho dnu.
 Umožní vzdialenému používateľovi volania dnu spojenie IPSec VPN cez Internet.

Špecifikovať vzdialenú VPN bránu alebo IP pripájaného VPN servera	Umožní vzdialenému používateľovi volania dnu vytvoriť spojenie L2TP VPN cez Internet. Môžete zvoliť samotné L2TP alone alebo s IPSec. Žiaden: Neaplikuje IPSec politiku. Vzhľadom na to spojenie VPN figuruje ako samostatné L2TP spojenie. Pekné mať: Aplikuje najskôr politiku IPSec počas vyjednávania. V opačnom prípade volanie von cez spojenie VPN bude samostatné spojenie L2TP. Musí: IPSec politika bude určite aplikovaná na spojenie L2TP.
Môžete špecifikovať vzdialenú VPN bránu alebo IP pripájaného VPN servera (malo by byť rovnaké ako nastavený typ ID volania dnu) zaškrtnutím políčka. Zadať číslo peeru ISDN, ak vyššie zvolíte ISDN (len i model). Takisto by ste mali podrobnejšie špecifikovať zodpovedajúcu bezpečnostnú metódu na pravej strane.	
Ak nezaškrtnete políčko, typ	spojenia použije bezpečnostnú metódu nastavenú v základných nastaveniach.
Užívateľské meno	Toto pole je aplikovateľné, ak zvolíte PPTP alebo L2TP s alebo bez IPSec politiky.
Heslo	Toto pole je aplikovateľné, ak zvolíte PPTP alebo L2TP s alebo bez IPSec politiky.
VJ komprimácia	Toto pole je aplikovateľné, ak zvolíte PPTP alebo L2TP s alebo bez IPSec politiky. VJ komprimácia jej používaná pre protokolovú hlavičku TCP/IP protokolu. Normálne sa nastavuje na Áno, aby bolo zlepšené využitie šírky pásmového prenosu.
IKE overovacia metóda	Táto skupina polí je aplikovateľná na IPSec Tunely a L2TP s IPSec politikou ak špecifikujete IP pripájaného VPN servera alebo číslo ISDN vzdialenej VPN brány, alebo IP peeru VPN servera. Zdieľaný kľúč - zadajte 1-63 znakov kľúča. Digitálny podpis (X.509) – určte jeden z preddefinovaných X.509 Peer ID profilov.
IPSec bezpečnostná metóda	Táto skupina polí je nevyhnutná pre IPSec Tunely a L2TP s IPSec politikou. Stredná Overovacia hlavička Authentication Header (AH) znamená, že dáta budú overené, ale nie kódované. Táto voľba je predvolená ako aktívna. Vysoká (ESP-Encapsulating Security Payload)- znamená, že objem (dáta) budú zakódované a overené. Môžete zvoliť kódovací algoritmus Data Encryption Standard (DES), trojitý DES a AES.
Funkcia spätného volania	poskytuje službu spätného volania iba používateľom ISDN volania dnu (len i model). Vlastníkovi routera bude účtovaný poplatok za pripojenie. Zaškrtnite Aktivovať funkciu spätného volania pre aktiváciu funkcie. Použiť nasledujúce číslo pre spätné volanie - je pre extra bezpečnosť. Ak ho aktivujete, bude vám môcť volať iba zvolené číslo. Poplatky spätného volania – je predvolený určitý čas spätného volania. Keď sú poplatky vyčerpané, funkcia bude deaktivovaná. Poplatky spätného volania (jednotka: minúty) – upresnite čas, koľko vám môže používateľ volať. Hodnota sa čerpaním automaticky znižuje. Nastavenie hodnoty 0 znamená, že nie je žiadne obmedzenie.
Moja WAN IP	Toto pole je aplikovateľné len ak zvolíte PPTP alebo L2TP s alebo bez IPSec politiky. Predvolená hodnota je 0.0.0.0, čo znamená, že router Vigor dostane PPP IP adresu počas fázy vyjednávania. Keď je nastavená fixná adresa na vzdialenej strane, špecifikujte ju aj tu.
IP vzdialenej brány	Toto pole je aplikovateľné len ak zvolíte PPTP alebo L2TP s alebo bez IPSec politiky. Predvolená hodnota je 0.0.0.0, čo znamená, že router Vigor dostane PPP IP adresu vzdialenej brány počas fázy vyjednávania. Keď je nastavená fixná adresa na vzdialenej strane, špecifikujte ju aj tu.
IP vzdialenej siete/maska vzdialenej siete	pridajte statický router aby ste nasmerovali všetky prenosy smerované na túto IP vzdialenej siete/masku vzdialenej siete cez spojenie VPN. Pre IPSec je ID cieľového klienta fázou 2 rýchleho módu.
Viac	Pridajte statický router aby ste nasmerovali všetky prenosy smerované na viac IP adries vzdialených sietí alebo masiek vzdialených sietí cze spojenie VPN. Toto sa zvyčajne používa, ak je za VPN routerov viac podsietí.
RIP smerovanie	Táto možnosť špecifikuje smerovanie RIP (Routing Information Protocol – protokol routovacích informácií) paketov. Môžete ju aktivovať alebo deaktivovať. Ponúkame štyri možnosti: TX/RX obidve, len TX , len RX , a Zakázať.
RIP verzia	Zvoľte verziu protokolu RIP. Pre najširšiu kompatibilitu zvoľte verziu 2.

Pre NAT operácie zaobchádzať so vzdialenou podsiet'ou ako Počas komunikácie so vzdialenou podsiet'ou s ňou môže router zaobchádzať ako so súkromnou sieťou posielaním paketov so súkromnou IP adresou routeru, alebo ako s verejnou podsiet'ou posielaním paketov s verejnou IP adresou routera.

3.7.7 Sprava spojenia

Dostupná je sumárna tabuľka všetkých pripojení VPN. Môžete odpojiť každé VPN pripojenie kliknutím na tlačítko Zrušiť. Takisto môžete volať von v agresívnom móde kliknutím na tlačítko vytočiť v nástroji na vytočenie VPN tunela.

VPN a vzdialený prístup >> Manazment pripojenia

Najstroj na vytocenie VPN tunela

Znovuzobrazenie : 10

<input type="text"/>	<input type="button" value="Vytocit"/>
----------------------	--

VPN stav spojenia

Aktualna Stranka: 1

VPN Typ	Vzdialena IP	Virtualna siet	Tx pakety	Tx prietok	Rx pakety	Rx prietok	Cas od spustenia
---------	--------------	----------------	-----------	------------	-----------	------------	------------------

xxxxxxxx : Data su kryptovane.

xxxxxxxx : Data niesu kryptovane.

Vytočiť Kliknite na toto tlačítko, ak chcete vykonať volanie von.

Znovuzobrazenie Zvoľte si čas znovuzobrazenia z možností 5, 10, a 30 sekúnd.

Obnoviť Kliknite, ak chcete obnoviť stav pripojenia.

3.8 Správa certifikátov

Sprava certifikatov

- Lokálny certifikát
- Dôveryhodný CA certifikát

Digitálny certifikát pracuje ako elektronická identita, ktorá je vydaná dôveryhodným zdrojom (certification authority – CA). Obsahuje informácie ako vaše meno, sériové číslo, dátumy expirácie atď. a digitálny podpis tohto zdroja, aby si mohol príjemca overiť, že certifikát je skutočný. Router Vigor podporuje digitálne certifikáty štandardu X.509.

Každá entita, ktorá chce využívať digitálny certifikát musí oň najskôr požiadať na CA serveri. Mala by takisto získať certifikáty od rôznych CA serverov, aby mohla overiť peer certifikátom vydaným týmito CA servermi.

Tu môžete spravovať generovanie a správu lokálnych certifikátov a nastavovať dôveryhodné CA certifikáty. Nezabudnite nastaviť čas routera, aby ste získali platný časový rozsah certifikátu.

3.8.1 Lokálny certifikát

Sprava certifikátov >> Lokálny certifikát

X509 konfigurácia lokálneho certifikátu

Meno	Predmet	Stav	Zmeniť
Local	---	---	<input type="button" value="Zobraziť"/> <input type="button" value="Vymazať"/>

X509 Lokálny Certifikát

Generovať Kliknite na tlačítko, ak chcete tvoriť okno generovania certifikátov.

Sprava certifikátov >> Lokálny certifikát

Generovať požiadavku na certifikát

Alternatívne meno predmetu

Typ

IP adresa ▾

IP

Meno osoby

Krajina (C)

Stat (ST)

Miesto (L)

Organizácia (O)

Organizačná jednotka (OU)

Bezne meno (CN)

Email (E)

Typ kľuca

RSA ▾

Veľkosť kľuca

1024 Bit ▾

Zadajte všetky požadované informácie a opäť kliknite Generovanie.

Importovať Kliknite na toto tlačítko pre importovanie uloženého súboru s informáciami o certifikáte.

Obnoviť Kliknite pre obnovenie informácií.

Zobraziť Kliknite pre podrobnejšie nastavenie požiadavky na certifikát.

Po kliknutí na Generovanie, generované informácie sa zobrazia v okne nižšie:

X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/C=TW/O=Draytek/OU=RD Depart...	Requesting	View Delete

[GENERATE](#)
[IMPORT](#)
[REFRESH](#)

X509 Local Certificate Request

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBvTCCASYCAQAwWzELMAkGA1UEBhMCVFcxEDAOBgNVBAAoTB0RyYX10ZWsxZjAU
BgNVBAsTDVJEIERlcGFydG1lbmQxIjAgBgkqhkiG9w0BCQEWB3N1cnZpY2VAZHJh
eXRlay5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgYOAQIGJAoGBAAyCa1K2vcBeeO+M
P101M8zTbUKPq19OPefEvoE1WCN6Vv1MZeJL0hfbMzjzqzWsXcQkC54zDhJUv6r
B1u43GEY507NdY6YrsEFgRWbjSVJeYNMeFfZs1cR+DMGfc12f6WdSUUpTnwlaXqu
11v3+pSS2U+6f1WtFpLnskQ8tt3BAgMBAAAGIjAgBgkqhkiG9w0BCQ4xEzARMA8G
A1UdEQQIMAAHBKwQA+UwDQYJKoZIhvcNAQEFBQADgYEABgtWjFrL5XECxE4CV9pq
1AwSLTxN4XHd51a2haRQjDYGZ43Cd1Vz+g1sMXV4h2G/Fd1xfexQE027BHJB1iK
kcZyc2U1SDS9T+JRxi/cff+vQRC1wWK2J7pX5M0wkTvkn4yww8yaISkBs8Gbb1fq
JH1AH+PwDmyck8A1EFH5oxE=
-----END CERTIFICATE REQUEST-----

```

3.8.2 Dôveryhodný CA certifikát

Dôveryhodný CA certifikát má v zozname tri sety certifikátov.

Sprava certifikatov >> Dôveryhodny CA Certifikat

X509 Konfiguracia doveryhodnych CA certifikatov

Meno	Predmet	Stav	Zmenit	
Dôveryhodny CA-1	---	---	Zobrazit	Vymazať
Dôveryhodny CA-2	---	---	Zobrazit	Vymazať
Dôveryhodny CA-3	---	---	Zobrazit	Vymazať

[IMPORT](#)
[Obnovit](#)

Aby ste importovali uložený certifikát, kliknite na **IMPORT** aby ste otvorili nasledujúce okno. Použite Prehľadávať... aby ste našli požadovaný súbor. Potom kliknite na Import. Importovaný certifikát bude na zozname certifikátov v okne Dôveryhodný CA certifikát. Potom kliknite na Import, aby ste použili uložený súbor.

Sprava certifikatov >> Dôveryhodny CA certifikat

Import X509 doveryhodneho CA certifikatu

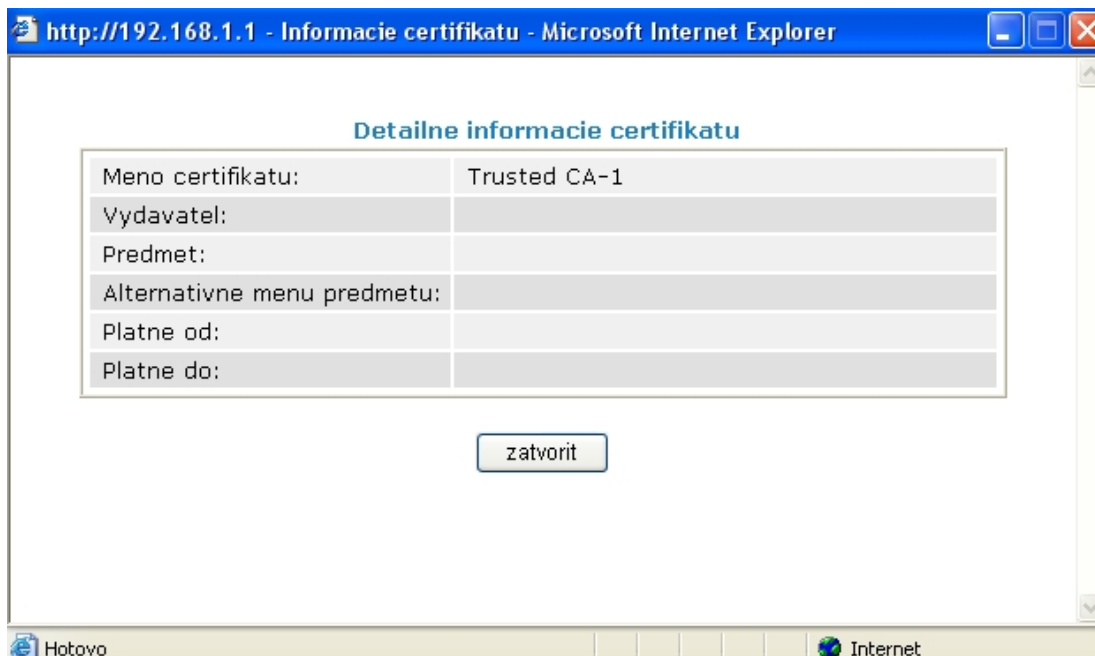
Vyber suboru doveryhodneho CA certifikatu

[Prehľadávať...](#)

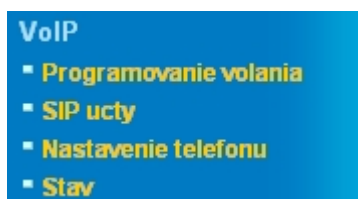
Kliknite na **Import** pre uploadovanie certifikatu.

[Import](#)
[Zrusit](#)

Kliknite na Zobrazit', ak chcete zobrazit' každý Dôveryhodný CA certifikát v podrobnom informačnom okne. Ak chcete certifikát vymazať, zvolte ho a kliknite na Vymazať. Odstránia sa všetky infomácie o certifikáte.



3.9 VoIP



Sieť Voice over IP (hlas cez IP - VoIP) vám umožňuje použiť širokopásmové pripojenie na Internet na hlasový prenos cez Internet vysokej kvality.

Je mnoho signálových protokolov, metód ktorými zariadenia VoIP spolu komunikujú. Najpopulárnejšie protokoly sú SIP, MGCP, Megaco a H.323. Tieto protokoly však nie sú všetky navzájom kompatibilné (výnimka je via a soft-switch server).

Vigor podporuje protokol SIP, ktorý je ideálny pre ITSP (poskytovateľ telefónnych služieb - Internet Telephony Service Provider) a softphone, a ktorý má širokú podporu. SIP je end-to-end (koniec-koniec), signálový protokoly, ktorý zriaďuje užívateľovi prítomnosť a mobilitu v štruktúre VoIP. Každý, kto chce komunikovať používa jej/jeho SIP Uniform Resource Identifier – tzv SIP adresu. Štandardný formát SIP URI je

sip: cislo@voi.t-com.sk: port

Niektoré polia pri rôznych druhoch využitia môžu byť voliteľné. Vo všeobecnosti t-com.sk je doména. "Userinfo" (informácie o užívateľovi) zahŕňajú pole „user“, heslo pole „password a nasleduje znak@“. Je to podobné ako URL a je možné to nazývať "SIP URL". SIP podporuje priame peer-to-peer volanie a takisto volanie prostredníctvom SIP proxy servera (rola podobná ako strážca brány v sieťach H.323), kým protokol MGCP používa architektúru klient/server, a teda spôsob volania sa podobá dnešným sieťam PSTN.

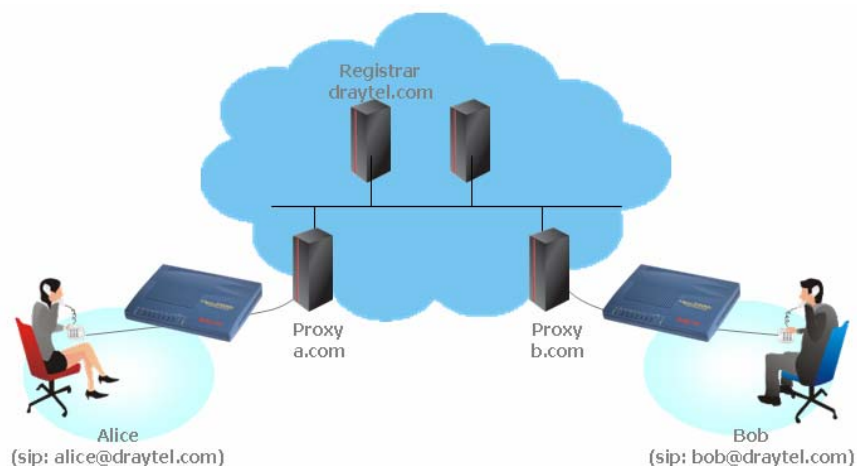
Keď je hovor nadviazaný, plynie hlasový prenos prostredníctvom RTP (Real-Time Transport Protocol – protokol prenosu v priamom čase). Do RTP paketov môžu byť vsadené rôzne kodeky (metódy kompresie a kódovania). Modely Vigor V models poskytujú rôzne kodeky vrátane G.711 A/μ-law, G.723, G.726 a G.729 A & B. Každý kodek používa rôznu šírku pásma prenosu a preto poskytuje rôznu kvalitu prenosu hlasu. Čím širšie pásmo kodek využije, tým lepšia je kvalita hlasu, ale kodek musíte prispôbiť svojmu Internetovému pripojeniu.

Volanie prostredníctvom SIP serverov

Najskôr sa Vigor sa zaregistruje tajomníkovi SIP zaslaním registračných správ, aby sa overila jeho platnosť.

Potom SIP proxy servery oboch strán prepošlú sekvencie správ volajúcemu, aby zriadili hovor.

Ak sa obaja zaregistrujú tomu istému SIP tajomníkovi, stane sa nasledovné:



Najväčšia výhoda tohoto módu je, že si nemusíte pamätať IP adresu vášho priateľa, ktorá sa môže, ak je dynamická, často meniť. Namiesto toho použijete programovanie volaní, alebo priamo vytočíte meno účtu vášho priateľa ak ste u toho istého SIP tajomníka.

3.9.1 Programovanie volaní

Táto stránka vám umožňuje nastaviť si telefónny zoznam a digitálnu mapu pre funkcie VoIP. Kliknite na odkaz Telefónny zoznam alebo Digitálna mapa na stránke, aby ste vstúpili na ďalšie stránky nastavení Programovania volaní.

[VoIP >> Programovanie volaní](#)

Programovanie volania

[Telefonny zoznam](#)

[Digitalna mapa](#)

Telefónny zoznam

V tejto sekcii môžete zadať do telefónneho zoznamu nazvanému „programovanie volaní“ svoje kontakty. Pomôže vám to nadväzovať hovory rýchlejšie použitím „rýchleho vytáčania“ telefónneho čísla. Je celkovo 60 vstupov – SIP adries, ktoré si môžete uložiť v programovaní volaní.

VoIP >> Programovanie volania

Telefonny zoznam

Index	Telefonne cislo	Zobrazovane meno	SIP URL	Stav
1.				x
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x
11.				x
12.				x
13.				x
14.				x
15.				x
16.				x
17.				x
18.				x
19.				x
20.				x

<< [1-20](#) | [20-40](#) | [40-60](#) >>

[Dalej](#) >>

Stav: v --- Aktivny, x --- Neaktivny, ? --- Prazdny

Kliknite na korýkoľvek index aby ste zobrazili stránku programovania volania.

VoIP >> Programovanie volania

Index cislo pre telefonny zoznam 1

<input checked="" type="checkbox"/> Aktivovat	
Telefonne cislo	<input type="text" value="1"/>
Zobrazovane meno	<input type="text" value="polly"/>
SIP URL	<input type="text" value="1234567"/> @ <input type="text" value="sip.voi.t-com.sk"/> <input type="button" value="v"/>

OK

Vymazat

Zrusit

Aktivovat'

kliknite aby ste aktivovali tento vstup.

Telefónne číslo

číslo rýchleho volania tohoto indexu. Môže to akékoľvek vami zvolené číslo zložené číslami 0-9 a * .

Zobrazované meno

Identifikácia volajúceho, ktorú chcete aby sa zobrazila na obrazovke vášho priateľa. Tak bude ľahko vedieť kto volá, namiesto aby si musel pamätať SIP adresu.

SIP URL

Zadajte priateľove telefónne číslo

Digitálna mapa

Táto stránka umožňuje užívateľovi upraviť číslo prefixu účtu SIP pridaním čísla, odstránením čísla alebo výmenou čísla. Používa sa na pomoc užívateľovi tým, že bude môcť rýchlo a ľahko volať cez VoIP rozhranie.

VoIP >> DialPlan Setup

Nastavenie digitalnej mapy

Zapnute	Cislo Prefixu	Mod	OP Cislo	Min dl.	Max dl.	Rozhranie
<input checked="" type="checkbox"/>	003	nahradiť	8863	7	9	VoIP1
<input checked="" type="checkbox"/>	886	Odkryť	886	7	9	VoIP2
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1
<input type="checkbox"/>		Ziadny		0	0	VoIP1

OK

Zrusit

Zapnuté

zaškrtnite ak chcete aktivovať nastavenie.

Číslo prefixu

číslo tu nastavené je použité na pridanie, odkrytie alebo nahradenie OP čísla.

Mód

Žiadny – žiadna aktivita. Pridať – ak zvolíte tento mód, OP číslo bude pridané k číslu prefixu pri volaní cez špecifické rozhranie. odkryť – OP číslo bde vymazané číslom prefixu na volanie cez VoIP rozhranie. Ako príklad si všimnite obrázok vyššie (tabuľka nastavenia prefixov), OP číslo 886 bude vymazané, pretože op číslo je nastavené na 886. Nahradiť – v tomto móde bude OP číslo nahradené číslom prefixu pri volaní cez určité rozhranie. Ako uvedené na obrázku vyššie, OP číslo 8863 bude nahradené číslom 03, pretože je číslo prefixu zadané 03.

Mod

nahradit ▼

Ziadny

Pridat

Odkryt

nahradit

OP číslo	predné číslo ktoré sem zadáte je prvá časť čísla účtu, z ktorého chcete vykonať určitú funkciu (vzhľadom na určený mód) použitím čísla prefixu.
Min DL	Nastavte minimálnu dĺžku volaného čísla na aplikovanie čísla prefixu. Ako zobrazené vyššie, keď je číslo medzi 7 a 9, to číslo môže aplikovať nastavenia čísla prefixu.
Max DL	Nastavte maximálnu dĺžku volaného čísla, ktoré môže aplikovať nastavenia čísla prefixu.
Rozhranie	Zvoľte si to, ktoré chcete aktivovať na číslo prefixu, spomedzi dvoch uložených SIP účtov.

3.9.2 Účty SIP

V tejto sekcii si môžete upraviť vlastné nastavenia SIP účtov. Keď požiadate o účet, váš poskytovateľ služby SIP vám dodá meno účtu alebo užívateľa, tajomníka SIP, proxy a názov domény (pričom posledné tri môžu byť identické). Potom oznámite známim vaše telefónne číslo ako Meno účtu@názov domény.

Keď zapnete Vigor VoIP Router, zaregistruje sa u tajomníka použitím autorizácia užívateľa@doména/oblasť. Potom bude váš hovor vedený cez SIP proxy k destinácii za použitia identity meno účtu@doména/oblasť.

VoIP >> SIP ucty

Zoznam SIP uctov

Obnovenie

Index	Profil	Doména/Oblasť	Proxy	Meno účtu	Vyzvanací port	Stav
1	VOI	sip.voi.t-com.sk	sip.voi.t-com.sk	change_me	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	-
2	VVN	as	sip.vvn.t-com.sk	change_me	<input type="checkbox"/> VoIP1 <input checked="" type="checkbox"/> VoIP2	-

R: uspesna registracia na SIP servri
-: neuspesna registracia na SIP servri

NAT Traversal nastavenie

STUN server:	<input type="text"/>
Externa IP:	<input type="text"/>
SIP PING interval:	<input type="text" value="150"/> sec

OK

Index	Kliknite na odkaz aby ste vstúpili na stránku nastavenia účtu SIP.
Profil	Zobrazí meno profilu účtu.
Doména/oblasť	Zobrazí názov domény alebo IP adresu tajomníka SIP servera.
Proxy	Zobrazí názov domény alebo IP adresu SIP proxy servera.
Meno účtu	Zobrazí meno účtu telefónneho čísla pred @. Vyzvákací port – špecifikujte, ktorý port bude zvonit' pri prijímaní hovoru. STUN Server – zadajte IP adresu STUN servera. Externá IP Zadajte IP brány. SIP PING interval – predvolená hodnota je 150 sekúnd. Je

užitočná pre Nortel NAT server traversar support.

Stav

Zobrazuje stav zodpovedajúci SIP účtu. R znamená, že účet je úspešne zaregistrovaný na SIP serveri. – znamená, že účet sa nezaregistroval.

VoIP >> SIP ucty

SIP ucet Index cislo 1

	VOI (HCI) ▼
Meno profilu	VOI (11 znak. max.)
Registrovať cez	Ziadny ▼ <input type="checkbox"/> Volanie bez registrácie
SIP Port	5061
Domain/Realm	sip.voi.t-com.sk (63 znakov max.)
Proxy	sip.voi.t-com.sk (63 znakov max.)
	<input type="checkbox"/> Pracovať ako outbound proxy
Zobrazované meno	(23 znakov max.)
Cislo uctu/meno	change_me (63 znakov max.)
<input type="checkbox"/> Overovacie ID	(63 znakov max.)
Heslo	(63 znakov max.)
Cas expiracie	1 hodina ▼ 3600 sek
NAT Traversal podpora	Ziadny ▼
Vyzvanaci port	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2
Vyzvanacia vzorka	1 ▼

OK Zrusit

Meno profilu

Priradiť meno profilu pre identifikáciu. Môžete zadať meno podobné ako názov domény. Napríklad ak je názov domény *draytel.org*, môžete zadať *draytel-1*.

Registrovať cez

Ak chcete volať cez VoIP bez registrácie osobných údajov, prosím zvolte Žiadny a zaškrtnite políčko. Niektoré SIP servery umožňujú užívateľom využívať VoIP funkcie bez registrovania. Pre taký server zaškrtnite Volanie bez registrácie. Doporučené je zvoliť Auto.

Ziadny ▼
Ziadny
Auto
WAN
LAN/VPN

SIP Port

Zadajte číslo portu pre posielanie/príjmanie SIP správ pre uskutočnenie hovoru. Predvolená je hodnota 5060. Váš peer musí nastaviť tú istú hodnotu u jeho tajomníka.

Domain/Realm

Zadajte názov domény alebo IP adresu servera tajomníka SIP.

Proxy

Nastavte meno domény alebo IP adresu SIP proxy servera. Môžete zadať :číslo portu, ak chcete upresniť cieľový port prenosu dát (napr. nat.draytel.org:5065)

Pracovať ako Outbound Proxy

Zaškrtnite, ak chcete, aby proxy pracoval ako Outbound proxy.

Zobrazované meno

ID volajúceho, ktoré chcete zobrazovať na priateľovej obrazovke.

Číslo/meno účtu

Zadajte meno účtu alebo telefónne číslo, napr. všetok text pred @.

Overovacie ID

Zaškrtnite, ak chcete aktivovať funkciu a zadajte meno alebo číslo používané na SIP overovanie u tajomníka SIP. Nemusíte zadávať, ak je rovnaké ako meno účtu.

Heslo	Heslo, ktoré vám bolo dodané, keď ste sa zaregistrovali na službu SIP.
Čas expirácie	Čas, po ktorý si bude SIP tajomník držať váš záznam. Pred vypršaním času zašle router SIP tajomníkovi ďalšiu požiadavku.
NAT Traversal podpora	Keď router (napr. širokopásmový router) k If the router (e.g., broadband router), ktorý používate, sa pripojí na internet iným zariadením, musíte nastaviť túto funkciu podľa potreby

Ziadny

Ziadny
Stun
manual
nortel

Žiadny	deaktivuje funkciu
Stun	ak je pre váš router poskytnutý Stun server.
Manual	Ak chcete nastaviť externú IP adresu ako NAT transversal podporu.
Nortel	ak soft-switch, ktorý používate, podporuje riešenie nortel, zvolte túto možnosť.
Vyzváňací port	Nastavte VoIP 1 alebo VoIP 2 ako predvolený vyzváňací port.
Vyzváňacia vzorka	Zvoľte vyzváňací tón

1

1
2
3
4
5
6

Nižšie je znázornený zoznam úspešných SIP účtov.

VoIP >> SIP ucty

Zoznam SIP uctov

Obnovenie

Index	Profil	Domena/Oblast	Proxy	Meno uctu	Vyzvanaci port	Stav
1	VOI	sip.voi.t-com.sk	sip.voi.t-com.sk	692099040	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2	R
2	VVN	as	sip.vvn.t-com.sk	253410203	<input type="checkbox"/> VoIP1 <input checked="" type="checkbox"/> VoIP2	R

R: uspesna registracia na SIP servri
-: neuspesna registracia na SIP servri

NAT Traversal nastavenie

STUN server:	<input type="text"/>
Externa IP:	<input type="text"/>
SIP PING interval:	<input type="text" value="150"/> sec

OK

3.9.3 Nastavenia telefónu

Táto stránka umožňuje užívateľovi upraviť nastavenia telefónu buď pre VoIP 1 alebo VoIP 2.

Zoznam telefonov

Index	Port	Znak volania	Kodek	Ton	Hlasitosť (Mic/Sluchadlo)	Default SIP účet	DTMF Relay
1	VoIP1		G.729A/B	Slovakia	5/5	VOI	OutBand
2	VoIP2		G.729A/B	Slovakia	5/5	VVN	OutBand

RTP

☐ Symmetrické RTP

Počiatkový dynamický RTP port

Konečný dynamický RTP port

RTP TOS

OK

Symetrické RTP

Zaškrtnite aby ste aktivovali funkciu. Aby prenos dát prešiel oboma koncami bez toho, aby sa stratil kvôli strate IP (napríklad pri poslaní dát z verejnej IP adresy vzdialeného routera na súkromnú IP adresu miestneho), zaškrtnutím políčka vyriešite tento problém.

Počiatkový dynamický RTP port - špecifikuje počiatkový port RTP streamu. Predvolená hodnota je 10050.

Konečný dynamický RTP port – špecifikuje končný port RTP streamu. Predvolená hodnota je 15000. RTP TOS – rozhoduje úroveň balíka VoIP. Vyberte si zo zoznamu.

IP precedence 5 ▼

Manual

- IP precedence 1
- IP precedence 2
- IP precedence 3
- IP precedence 4
- IP precedence 5
- IP precedence 6
- IP precedence 7
- AF Class1 (Low Drop)
- AF Class1 (Medium Drop)
- AF Class1 (High Drop)
- AF Class2 (Low Drop)
- AF Class2 (Medium Drop)
- AF Class2 (High Drop)
- AF Class3 (Low Drop)
- AF Class3 (Medium Drop)
- AF Class3 (High Drop)
- AF Class4 (Low Drop)
- AF Class4 (Medium Drop)
- AF Class4 (High Drop)
- EF Class

Kliknite na číslo **1** alebo **2** v stĺpci index a vstúpte na nasledujúcu stránku pre konfigurovanie nastavení telefónu.

Tel. Index cis. 1

Znak volania <input type="checkbox"/> Hotline <input type="text"/> <input type="checkbox"/> Casovac sedenia <input type="text" value="3600"/> sec <input type="checkbox"/> T.38 Fax funkcia Presmerovanie volania <input type="text" value="zrusit"/> <input type="button" value="v"/> SIP URL <input type="text"/> Cas do skoncenia <input type="text" value="30"/> sec <input type="checkbox"/> DND(Do Not Disturb) mod Index(1-15) v Planovaci Nastavenie: <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/> Poz.: Akcia a cs necinosti budu ignorovane. <input type="checkbox"/> Cakajuce volanie <input type="checkbox"/> Presmerovanie hovoru		Codecs Preferovany kodek <input <input="" type="button" value="v"/> <input type="checkbox"/> Jediny kodek Velkost paketu <input <input="" type="button" value="v"/> Detektor hlasovej aktivity (VAD) <input <input="" type="button" value="v"/> Default SIP ucet <input type="checkbox"/> Hrat oznamovaci ton ak je ucet registrovany
--	--	---

OK Zrusit Rozsirene

Hotline	Zaškrtnite políčko, ak ju chcete aktivovať. Zadaťte SIP URL, ktorá bude automaticky volaná keď dvihnete telefón.
Časovač sedenia	Zaškrtnite, ak chcete aktivovať funkciu. Ak počas času, ktorý zadáte do políčka, nebude žiadna odpoveď, automaticky sa ukončí spojenie
T.38 Fax funkcia	Ak podporuje FAX funkciu aj vzdialený kokniac, môžete ju zaškrtnutím povoliť.
Presmerovanie volania	Máte štyri možnosti.
Zrušiť	zavrie funkciu presmerovania.
Vždy	všetky hovory budú presmerované na SIP URL bezpodmienečne.
Obsadené	prichádzajúce hovory budú presmerované, keď je miestny systém obsadený.
Bez odpovede	ak prichádzajúce hovory ostávajú bez odpovede, po uplynutí času bude hovor presmerovaný na danú SIP URL.

SIP URL – zadajte SIP URL (napr. aaa@draytel.org or abc@t-com.sk) čas do skončenia – nastavte časovač, predvolených je 30 sekúnd.

DND (Do Not Disturb - nevyrušujte) mód – nastavte čas kedy nechcete byť vyrušovaní VoIP hovormi. Počas tohto obdobia bude ten čo volá počuť tón obsadené a miestny užívateľ nebude počuť vyzváňanie.

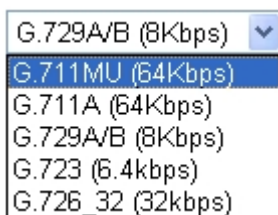
Plánovanie – Zadaťte index plánovacieho profilu, aby ste riadili DND podľa predvoleného plánu, vid' sekcia 3.5.2.

Čakajúce volanie Zaškrtnite, ak chcete spustiť funkciu. Zaznie tón poznámky, že nový hovor očakáva odpoveď. Kliknite na háčik aby ste dvihli.

Presmerovanie hovoru Zaškrtnite, ak chcete spustiť funkciu. Kliknite na háčik aby ste iniciovali ďalší hovor. Keď sa spojenie podarí, zaveste. Druhé dve strany môžu komunikovať.

Preferovaný kodek Zvoľte jeden z piatich kodekov ako predvolený pre vaše VoIP hovory. Kodek a kodeku

by sa peery mali dohodnúť pred každým sedením, preto to niekedy nemusí byť vaša voľba. Predvolený kodek je G.729A/B; potrebuje malú šírku pásma a udržiava dobrú kvalitu hlasu. Pri rýchlosti odosielania dát (upstream) 64 Kbps tento kodek nepoužívajte. Najlepšie je mať upstream 256 Kbps.



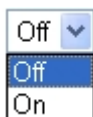
Jediný kodek

ak je políčko zaškrtnuté, bude aplikovaný len zvolený kodek. Veľkosť paketu – množstvo dát, ktoré jeden paket obsahuje, predvolená hodnota je 20 ms, čo znamená že paket bude obsahovať 20 ms hlasu.



Detektor hlasovej aktivity

Táto funkcia detekuje, či je hlas na oboch stranách aktívny alebo nie. Ak nie je, router ušetrí šírku pásma. Kliknite na On na aktiváciu a Off na deaktiváciu.



Default SIP účet

Sú dve skupiny účtov SIP, ktoré môžete nastaviť. Vyberte si z menu meno profilu a účet, ktorý chcete predvoliť.

Hrať oznamovací tón len keď je účet registrovaný – Zaškrtnite pre aktiváciu funkcie.

Rozsirene nastavenia telefonu

Tato možnosť sa zobrazí po kliknutí na tlačidlo Rozsirene v menu VOIP – Nastavenie telefonu – Index.1.

Je možné tu nastaviť tón v sluchadle telefonu pripojeného do FXS portu, a to pomocou ponuky Region, kde sú pre jednotlivé štáty predvolené frekvencie tónov, alebo je možné nastaviť aj manuálne.

Advance Settings >> Telefon Index Cis. 1

Nastavenia tonu

Region Typ zobrazovania ID

	Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Oznamovací ton	<input type="text" value="425"/>	<input type="text" value="0"/>	<input type="text" value="330"/>	<input type="text" value="330"/>	<input type="text" value="660"/>	<input type="text" value="660"/>
Vyzvanací ton	<input type="text" value="425"/>	<input type="text" value="0"/>	<input type="text" value="1000"/>	<input type="text" value="4000"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Obsadzovací ton	<input type="text" value="425"/>	<input type="text" value="0"/>	<input type="text" value="330"/>	<input type="text" value="330"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Ton chyby	<input type="text" value="425"/>	<input type="text" value="0"/>	<input type="text" value="165"/>	<input type="text" value="165"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Zisk hlasitosti

Hlasitosť mikrofónu(1-10)

Hlasitosť reproduktora(1-10)

DTMF

DTMF mod

Payload Type(rfc2833)

Rozne

Uroveň oznamovacieho tonu

Vyzvanacia frekvencia

OK

Zrusit

Region

Typ zobrazovania ID

Hlasitosť mikrofónu

Hlasitosť reproduktora

DTMF mod

Vyber regionu, s predvolenými hodnotami ako Typ zobrazovania ID, frekv. Tonu..

Možnosť vyber normy pre zobrazovanie ID (Caller ID)

Nastavenie hlasitosti mikrofónu v sluchadle pripojeného telefónu

Nastavenie hlasitosti reproduktora v sluchadle pripojeného telefónu

InBand alebo OutBand

3.9.4 Stav

V časti VoIP stav môžete nájsť stav kodeku, pripojenia, alebo iné dôležité informácie o stave hovoru pre oba VoIP porty.

Stav

Obnovovací interval : 10

Port	Stav	Kodek	PeerID	Čas spojenia	Tx Pak.	Rx Pak.	Rx strat	Rx Jitter (ms)	Pri. volania	Odch. volania	Hlasitosť sluchadla
VoIP1	IDLE			0	0	0	0	0	0	0	5
VoIP2	IDLE			0	0	0	0	0	0	0	5

Zaznamy volaní

Date (mm-dd-yyyy)	Time (hh:mm:ss)	Duration (sec)	In/Out	Peer ID
00-00-00	00:00:00	0	-	
00-00-00	00:00:00	0	-	
00-00-00	00:00:00	0	-	
00-00-00	00:00:00	0	-	
00-00-00	00:00:00	0	-	
00-00-00	00:00:00	0	-	
00-00-00	00:00:00	0	-	
00-00-00	00:00:00	0	-	
00-00-00	00:00:00	0	-	
00-00-00	00:00:00	0	-	
00-00-00	00:00:00	0	-	

Obnovovací interval	špecifikujte interval obnovenia informácií o volaní VoIP. Informácie sú aktualizované hneď, keď kliknete na tlačítko Obnoviť.
Port	Zobrazuje stav pripojenia portov VoIP1 a VoIP2.
Stav	Zobrazuje stav pripojenia VoIP. Nečinný - IDLE – funkcia je nečinná. Zavesený - HANG_UP –pripojenie sa neuskutočnilo (tón obsadený) Spája - CONNECTING –Užívateľ volá. Očakáva odpoveď - WAIT_ANS – hovor bol iniciovaný a čaká na odpoveď vzdialeného užívateľa. Upozorňuje - ALERTING –Prichádzajúci hovor
Kodek	Aktívny - ACTIVE- spojenie VoIP je aktívne. Zobrazuje použitý kodek.
PeerID	Súčasný ID peeru volajúceho von alebo dnu (formát môže byť IP alebo doména).
Čas spojenia	V sekundách.
Tx Pak	Celkový počet prenesených hlasových paketov počas hovoru.
Rx Pak	Celkový počet prijatých hlasových paketov počas hovoru.
Rx Strat	Celkový počet stratených hlasových paketov počas hovoru.
Rx Jitter	Kolísanie hlasových paketov.
Pri Calls	Akumulovaný čas prichádzajúcich hovorov.
Odch Calls	Akumulovaný čas odchádzajúcich hovorov.
Hlasitosť sluchadla	Hlasitosť súčasného hovoru.
Log	Zobrazí log hovoru VoIP.

3.11 Správa systému

Sprava systému

- Stav systému
- Administratorske heslo
- Zálohovanie konfigurácie
- Zaznamenávanie systému
- Čas a Datum
- Sprava systému
- Restartovanie systému
- Upgrade firmveru

Pre nastavenie systému, je niekoľko položiek, ktoré je potrebné vedieť ako nastaviť: Status, Administrator Password, Configuration Backup, Syslog, Time and Date, Reboot System and Firmware Upgrade.

3.11.1 Stav systému

Stav systému poskytuje základné nastavenie siete routra Vigor. Zahŕňa informácie o rozhraní LAN a WAN. Teda, teda môžete zistiť aktuálnu verziu firmware.

Stav systému

Nazov modelu : Vigor2700 series
Verzia firmware : 2.6.2.1_RC3
Datum a čas výroby : Aug 7 2006 17:22:44

LAN

MAC adresa : 00-50-7F-D8-ED-F0
1. IP adresa : 192.168.1.1
Maska 1. podsiete : 255.255.255.0
DHCP Server : Ano

VoIP

Port : 1 2
SIP server : sip.voi.t-com.sk as
Meno/Cislo uctu : 692099040 253410203
Registracia na SIP : Yes Yes
Kodek :
Prichadzajúce volania : 0 0
Odchadzajúce volania : 0 0

WAN

Stav linky : **Connected**
MAC adresa : 00-50-7F-D8-ED-F1
Spojenie : PPPoE
IP adresa : 62.65.169.134
Prednastavená brana : 195.72.7.1
DNS : 195.12.128.1

Bezdrôtová LAN

MAC adresa : 00-50-7f-d8-ed-f0
Frekvencná doména : Europa
Verzia firmware : 1.0.4.0

Názov modelu Zobrazuje meno modelu routra.
Verzia firmware Zobrazuje verziu firmware routra.
Datum a čas výroby Zobrazuje dátum a čas výroby firmware routtra.

LAN:

MAC adresa Zobrazuje MAC adresu LAN rozhrania routra.
1. IP adresa Zobrazuje IP adresu LAN rozhrania.
Maska 1. podsiete Zobrazuje adresu masky podsiete LAN rozhrania.
DHCP Server Zobrazuje aktuálny stav DHCP servera v LAN rozhraní.

WAN:

MAC adresa	Zobrazuje MAC adresu WAN rozhrania.
IP adresa	Zobrazuje IP adresu WAN rozhrania.
Prednastavena brana	Zobrazuje pridelené IP adresy prednastavenej brány.
DNS	Zobrazuje pridelenú IP adresu primárneho DNS.

VOIP:

Port	Zobrazuje číslo FXS portu
Registracia na SIP	Zobrazuje názov SIP servra, pre VoIP telefonovaniu (Yes – Ano, No - Nie)
Meno/Cislo uctu	Zobrazuje názov účtu pre VOIP, ktorý poskytuje ISP
Register	Zobrazuje stav FXS portov, či sú registrované alebo nie.
Kodek	Zobrazuje typ predvoleného kodeku pre daný FXS port
Prichadzajúce volania	Zobrazuje počet volaní smerom dnu
Odchadzajúce volania	Zobrazuje počet volaní smerom von

Wireless LAN:

MAC adresa	Zobrazuje MAC adresu rozhrania bezdrôtovej siete.
Frekvencna domena	Zobrazuje dostupný kanál podporovaný bezdrôtovým produktom. Závisí to od krajiny, Európa (13 použiteľných kanálov), USA (11 použiteľných kanálov). Firmware Version Zobrazuje informácie o ovládačoch karty WLAN.

3.11.2 Heslo administrátora

Táto stránka umožňuje nastaviť nové heslo.

Sprava systemu >> Nastavenie administratorskeho hesla

Heslo administratora

Stare heslo	<input type="password"/>
Nove Heslo	<input type="password"/>
Znovuzadanie noveho hesla	<input type="password"/>

OK

Stare heslo	Zadajte staré heslo. Výrobné nastavenie hesla je: „admin“.
Nove heslo	Do tohto poľa zadajte nové heslo.
Znovuzadanie noveho hesla	Znovu zadajte nové heslo. Ak kliknete OK, zobrazí sa okno so zadaním nových prihlasovacích údajov. Prosím použite nové heslo pre prístup do WEB konfiguratéra

routra.

3.11.3 Zálohovanie konfigurácie

Podľa nasledovných krokov je možné vykonať zálohovanie nastavení routra.

Chodíte do **Sprava systému >> zálohovanie konfigurácie systému**. Ukáže sa nasledovne okno (vid. dole)

1. Klikni **Zalohovanie** zobrazí sa nasledujúce okno. Klikni na **Save** a otvorí sa ďalšie okno pre uloženie konfigurácie.
2. V **Save As** dialogu, prednastavene meno je **config.cfg**. Môžete ho zmeniť.
3. Kliknite **Save**, bude stiahnuta z routra a uložená pod menom **config.cfg**.

Sprava systému >> Zálohovanie konfigurácie systému

Zalohovanie konfigurácie systému

Obnovenie konfigurácie zo suboru

Vybrať konfiguracný subor.

Prehľadávať...

Klikni a obnovi sa záloha konfigurácie zo suboru.

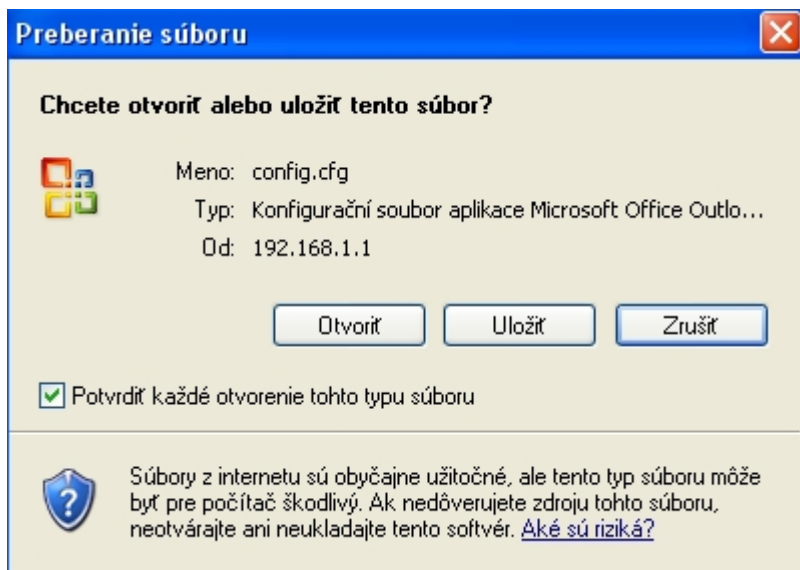
Obnovenie zo zálohy

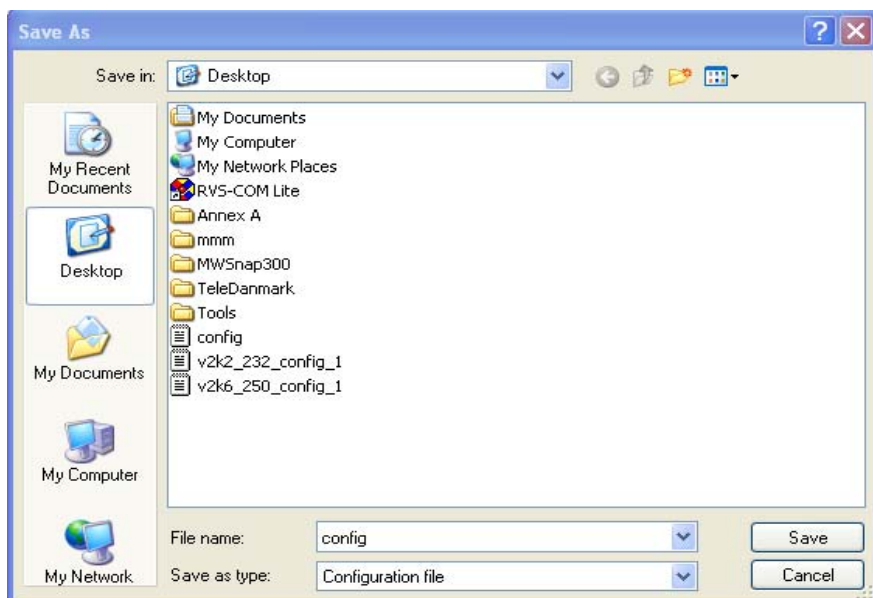
Zalohovanie

Klikni a zálohuje sa aktuálna konfigurácia systému do suboru.

Zalohovanie

Zrušiť





V príklade je požitá platforma **Windows** pre demoštráciu príkladu. **Mac** alebo **Linux** bude mať odlišné zobrazenie okien, ale funkcia zálohovania je stále rovnaká.

Obnovenie konfigurácie systému

- 1 Kliknite na **Sprava systému >> zálohovanie konfigurácie systému**.. Zobrazí sa nasledujúce okno, ako na obrázku dole.
- 2 Kliknite na **Prehľadávať** tlačítko pre vybratie konfiguračného súboru, ktorým chcete obnoviť nastavenie v routri.
- 3 Kliknite na **Obnovenie zo zálohy** tlačítko a počkajte, kým vám ďalšie okno oznámi že proces zálohovania bol úspešný.

Sprava systému >> Zálohovanie konfigurácie systému

Zalohovanie konfigurácie systému

Obnovenie konfigurácie zo suboru

Vybrať konfiguračný súbor.

Klikni a obnovi sa záloha konfigurácie zo suboru.

Zalohovanie

Klikni a zalohuje sa aktuálna konfigurácia systému do suboru.

3.11.4 Zaznamenávanie systému

SysLog funkcia je poskytovaná užívateľom pre pomoc monitorovania routra. Nie je potrebné vstupovať do WEB konfigurácie routra a zisťovať v nastaveniach stavy jednotlivých činností routra.

Zaznamenavanie systemu

Zaznamenavanie systemu (SysLog)	Upozornenie e-mailom
<input checked="" type="checkbox"/> Zapnut	<input type="checkbox"/> Zapnut
IP adresa servra <input type="text"/>	SMTP server <input type="text"/>
Cielovy port <input type="text" value="514"/>	Poslat mail na <input type="text"/>
Aktivovat zaznamenavanie sprav:	Navratova cesta <input type="text"/>
<input checked="" type="checkbox"/> Firewall zaznamy	<input type="checkbox"/> Overenie
<input checked="" type="checkbox"/> VPN zaznamy	Uzivatelске meno <input type="text"/>
<input checked="" type="checkbox"/> Zaznamy uzivatelskych pristupov	Heslo <input type="text"/>
<input checked="" type="checkbox"/> zaznamenavanie volania	
<input checked="" type="checkbox"/> WAN zaznamy	
<input checked="" type="checkbox"/> Router/DSL informacie	

Zaznamenavanie systemu:

Zapnut	Kliknite na "Enable" pre aktivovanie tejto funkcie.
IP adresa servra	IP adresa servra (alebo počítača v LAN), kde je spustená aplikácia Syslog (súčasť balíčka Router Tools).
Cielovy port	Pridelený port pre komunikáciu s aplikáciou Syslog.

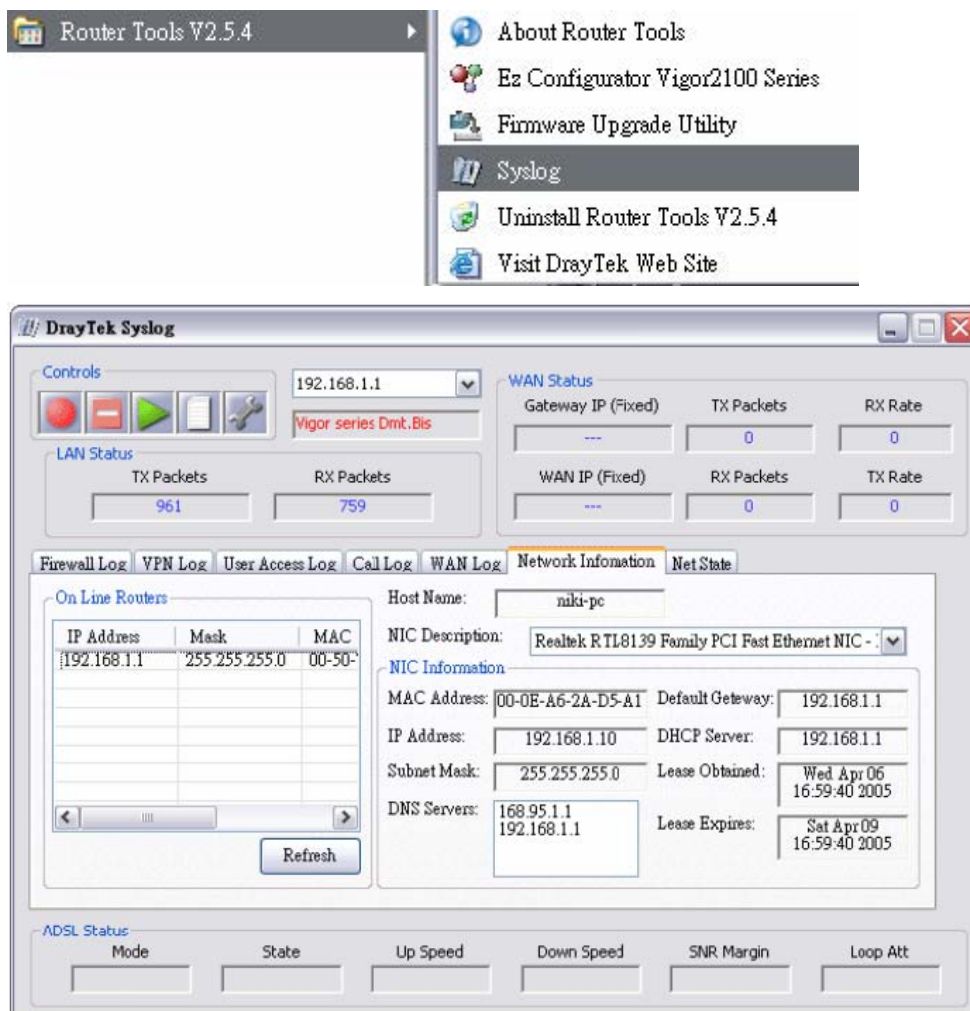
Upozornenie mailom:

Zapnut	Kliknite na "Enable" pre aktivovanie tejto funkcie.
SMTP Server	IP adresa SMTP servra.
Poslat mail na	Pridelenie mailovej adresy pre odosielanie smerom von.
Navratova cesta	Pridelenie cesty pre prijímanie mailu z vonku.

Kliknite na OK pre uloženie nastavení.

Pre zobrazenie aplikácie Syslog, prosím vykonajte nasledovné:

- 1 Nastavte IP adresu vášho PC kde bude spustená aplikácia Syslog do poľa Server IP Address a aktivujte túto funkciu zaškrtnutím položky Enable
- 2 Nainštalujte utility Router Tools z priloženého CD. Po inštalácii, Kliknite v menu programov na **Router Tools>>Syslog**.
- 3 Na obrazovke Syslog, vyberte router ktorý chcete monitorovať. Nezabudnite že v **Network Information**, označte sieťový adaptér ktorý chcete monitorovať použitý pre spojenie s routrom. Inak nebude možné získať informácie z routra.



3.11.5 Čas a dátum

Umožňuje špecifikovať odkiaľ a ako sa majú získavať informácie o čase, pre systémový čas routra.

Sprava systému >> Cas a datum

Informacie o case

Aktualny systemovy cas 2000 Jan 1 Sat 0 : 9 : 7

Zistit cas

Cas a datum

☐ Pouzit cas z prehliadaca

☒ Pouzit klienta internetoveho casu

Casovy protokol

NTP (RFC-1305)

IP adresa servra

Casova zona

(GMT) Greenwich Mean Time : Dublin

Aktivovat prechod na letny cas

☐

Interval automatickeho
zistovania

30 sec

OK

Zrusit

Aktualny systemovy cas

Kliknite na Zistit cas pre získanie aktuálneho času.

Použitie času z prehliadaca	Označte túto možnosť, ak chcete aby router získal čas z hostiteľského PC a nastavil ho ako systémový čas routera.
Použitie klienta internetového času	Označte túto možnosť aby sa čas získaval z časových serverov v internete
Casový protokol	Vyberte časový protokol.
IP adresa servera	Zadajte IP adresu alebo DNS názov časového servera.
Casová zóna	Zadajte časovú zónu, v ktorej sa router nachádza
Aktivovať prechod na letný čas :	Označením aktivujete prechod na letný čas pri zmene času letného na zimný a opačne
Interval automatickeho zisťovania	Zadajte časový interval v ktorom sa bude aktualizovať čas z NTP servera.

Kliknite na **OK** pre uloženie týchto nastavení.

3.11.6 Správa systému

Tato stránka umožňuje spravovať nastavovanie spravovania prístupu, zoznam povolených prístupov, nastavenie portov, a SNMP nastavenie. Príklad ako spravovať kontrolu prístupu, číslo portu je použité na odosielanie/prijímanie SIP message pre zostavenie session. Prednastavená hodnota je 5060 a toto musí korešpondovať s registráciou ak uskutočňujete VoIP volania.

Sprava systemu >> Spravovanie

Spravca systému

<h5>Riadenie prístupu</h5> <p> <input type="checkbox"/> Aktivovať upgrade firmveru na diaľku(FTP) <input type="checkbox"/> Povolit spravovanie z internetu <input checked="" type="checkbox"/> Zakázať ping z internetu </p> <hr/> <h5>Zoznam povolených prístupov</h5> <table border="1"> <thead> <tr> <th>Zoznam</th> <th>IP</th> <th>Maska podsiete</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>2</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>3</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>	Zoznam	IP	Maska podsiete	1	<input type="text"/>	<input type="text"/>	2	<input type="text"/>	<input type="text"/>	3	<input type="text"/>	<input type="text"/>	<h5>Nastavenie manažmentu portov</h5> <p> <input type="radio"/> Prednastavené porty (Telnet: 23, HTTP: 80, HTTPS: 443, FTP: 21) <input checked="" type="radio"/> Užívateľom definované porty </p> <table> <tr> <td>Telnet Port</td> <td><input type="text" value="23"/></td> </tr> <tr> <td>HTTP Port</td> <td><input type="text" value="80"/></td> </tr> <tr> <td>HTTPS Port</td> <td><input type="text" value="443"/></td> </tr> <tr> <td>FTP Port</td> <td><input type="text" value="21"/></td> </tr> </table> <hr/> <h5>SNMP nastavenie</h5> <p> <input type="checkbox"/> Aktivovať SNMP Agent </p> <table> <tr> <td>Get Community</td> <td><input type="text" value="public"/></td> </tr> <tr> <td>Set Community</td> <td><input type="text" value="private"/></td> </tr> <tr> <td>Manager Host IP</td> <td><input type="text"/></td> </tr> <tr> <td>Trap Community</td> <td><input type="text" value="public"/></td> </tr> <tr> <td>Notification Host IP</td> <td><input type="text"/></td> </tr> <tr> <td>Trap Timeout</td> <td><input type="text" value="10"/> sec.</td> </tr> </table>	Telnet Port	<input type="text" value="23"/>	HTTP Port	<input type="text" value="80"/>	HTTPS Port	<input type="text" value="443"/>	FTP Port	<input type="text" value="21"/>	Get Community	<input type="text" value="public"/>	Set Community	<input type="text" value="private"/>	Manager Host IP	<input type="text"/>	Trap Community	<input type="text" value="public"/>	Notification Host IP	<input type="text"/>	Trap Timeout	<input type="text" value="10"/> sec.
Zoznam	IP	Maska podsiete																															
1	<input type="text"/>	<input type="text"/>																															
2	<input type="text"/>	<input type="text"/>																															
3	<input type="text"/>	<input type="text"/>																															
Telnet Port	<input type="text" value="23"/>																																
HTTP Port	<input type="text" value="80"/>																																
HTTPS Port	<input type="text" value="443"/>																																
FTP Port	<input type="text" value="21"/>																																
Get Community	<input type="text" value="public"/>																																
Set Community	<input type="text" value="private"/>																																
Manager Host IP	<input type="text"/>																																
Trap Community	<input type="text" value="public"/>																																
Notification Host IP	<input type="text"/>																																
Trap Timeout	<input type="text" value="10"/> sec.																																

OK

Aktivovať upgrade firmveru na diaľku (FTP) Označte toto políčko pre povolenie možnosti vzdialene upgradovať firmvér v zariadení cez FTP (používa sa firmvér s príponou .all)

Povolit spravovanie z internetu Označte toto políčko pre povolenie prihlásenie administrátora z internetu
Štandardne nie je povolené.

Zakázať ping z internetu Označte toto políčko pre odmietnutie všetkých PING paketov z internetu. Pre zvýšenie

bezpečnosti je táto funkcia štandardne aktivovaná.

Zoznam povolených prístupov Môžete tu špecifikovať že systémový správca sa môže pripojiť k routru zo špecifickej IP adresy alebo siete, definovanej v zozname. Maxim sú 3 IP/sieťové masky. Ak v zozname nie je definovaná žiadna IP adresa a maska je prístup povolený z akejkoľvek IP adresy, ak je táto funkcia aktivovaná

Zoznam IP Indikuje IP adresu ktorá má povolený prístup k routru.
Maska podsiete Reprezentuje masku podsiete povolenú pre prihlásenie sa k routru.

Nastavenie manazmentu portov:

Prednastavene porty Označiť pre použitie štandardných portov pre Telnet a http servre.

Uzivatelom definovane porty Označiť pre špecifikovanie čísiel portov užívateľom .

SNMP nastavenie:

Aktivovať SNMP Agent Označiť pre aktivovanie tejto funkcie.

Get Community nastaviť meno pre získanie community zadaním správneho popisu. Default nastavenie je public.

Set Community nastaviť community zadaním správneho mena. The default setting is private.

Manager Host IP Nastaviť jedného hostiteľa pre spravovanie a vykonávanie SNMP funkcie. Prosim zadajte IP adresu hostiteľa.

Trap Community Nastavte trap community zadaním správneho mena. Default nastavenie je public.

Notification Host IP Nastaviť IP adresu hostiteľa ktorý bude prijímať trap community.

Trap Timeout Default nastavenie je 10 seconds.

3.11.7 Reštartovanie systému

WEB konfigurátor môže byť použitý pre reštartovanie Vášho routra. Kliknite na **Restartovanie systemu** v **Sprave systemu** pre otvorenie nasledovnej stránky.

Sprava systemu >> Restartovanie systemu

Restartovanie systemu

Chcete reštartovať router ?

- ☒ Použiť aktuálnu konfiguráciu
☐ Použiť štandardnú výrobnú konfiguráciu

OK

Ak chcete reštartovať router použitím aktuálnej konfigurácie, označte **Použiť aktuálnu konfiguráciu** a kliknite **OK**. Pre resetovanie routra do výrobného nastavenia označte **Použiť štandardnú výrobnú konfiguráciu** a kliknite OK. Router bude asi za 5 sekúnd reštartovaný.

3.11.8 Upgrade firmveru

Pred upgradovaním firmvéru routra, je potrebné nainštalovať Router Tools. **Firmware Upgrade Utility** je súčasť tohto balíčka.

Stiahnite si najnovší firmver zo stránky výrobcu alebo distribútora (www.attel.sk) alebo z FTP stránky..

Kliknite na **Sprava systemu >> Upgrade firmveru** pre spustenie Firmware Upgrade Utility.

Upgrade firmveru

Aktualna verzia firmware : 2.6.2.1_RC3

Upgrade firmveru:

- 1. Kliknite "OK" a nastartuje sa TFTP server.
- 2. Otvorte Firmware Upgrade Utility alebo iny 3-party TFTP client software.
- 3. Skontrolujte ze je spravne menu subouru.
- 4. Kliknite na "Upgrade" v aplikacii Firmware Upgrade Utility a zacne sa upgrade.
- 5. Po uspesnom uprade firmveru, sa TFTP server automaticky ukonci.

Chcete upgradovat firmvare ?

OK

Kliknite na OK a zobrazí sa nasledovná stránka

Sprava systemu >> Upgrade firmveru



TFTP server je aktivovany. Prosim spustite sofver Firmware Upgrade Utility na upgradovanie routra. Tento server sa ukonci sam po upgrade firmware.

3.12. Diagnostické nástroje

Diagnosticke nástroje

- WAN pripojenie
- Dial-out spustaci mechanizmus
- Routovacia tabulka
- ARP Cache tabulka
- DHCP tabulka
- NAT tabulka spojeni
- Ping diagnostika
- Monitor prietoku dat
- Sledovanie trasy paketu

Diagnosticke nástroje užitočný spôsob ako **zobraziť** alebo **diagnostikovať** stav routra.

3.12.1 WAN pripojenie

Kliknite na **Diagnosticke nástroje** a kliknite na **WAN pripojenie** pre otvorenie tejto stránky.

Diagnosticke nástroje >> WAN pripojenie

PPPoE/PPPoA diagnostika

| [Obnovit](#) |

Mod/Stav širokopásmového prístupu	---
Internetový prístup	>> Vytocit PPPoE/PPPoA
WAN IP Adresa	---
Rozpojit spojenie	>> Rozpojit PPPoE/PPPoA

Obnovit	Pre získanie posledných informácií, kliknite sem a stránka sa znovunačíta.
Mod/Stav Širokopásmového prístupu	Zobrazí stav a mód širokopásmového prístupu. Ak je širokopásmové pripojenie aktívne zobrazí Internetový prístup je aktívny. Keď nie je tak sa zobrazí “---”.
WAN IP adresa	WAN IP adresa pre aktívne spojenie.
Rozpojit spojenie	Kliknúť sem na vytvorenie alebo zrušenie spojenia PPPoE alebo PPPoA

3.12.2 Dial-out spúšťací mechanizmus

Kliknite na **Diagnosticke nástroje** a Dial-out spustací mechanizmus pre otvorenie nasledovnej stránky. Internetové spojenie (PPPoE, PPPoA) je spúšťané paketom z konkrétnej IP adresy v sieti, ak nie je nastavená funkcia „Vždy pripojený“.

Diagnosticke nástroje >> Dial-out spustací mechanizmus

Paket ktorý spôsobil vytocenie pripojenia na internet

| [Obnovit](#) |

HEX format:

```
00 50 7F D8 ED F0-00 12 F0 A0 E6 DB-08 00

45 00 00 3B 54 32 00 00-7F 11 E2 BF C0 A8 01 0A
C3 0C 80 01 04 06 00 35-00 27 C1 CD 03 35 01 00
00 01 00 00 00 00 00 00-03 77 77 77 06 6B 6F 76
61 63 69 02 73 6B 00 00-01 00 01 00 01 0C 80 09
66 84 00 00 00 00 00 00-00 00 00 00 00 80 B1
```

Dekodovaný paket:

```
192.168.1.10,1030 -> 195.12.128.1, domain
Pr udp HLen 20 TLen 59
```

HEX format	Zobrazuje zdrojový paket v HEX kóde
Dekodovaný paket	Zobrazuje zdrojovú IP (lokalnú), cieľovú IP (vzdialenú) adresu, protokola dĺžku paketu.
Obnoviť	kliknite pre znovunačítanie (obnovenie) stránky.

3.12.3 Routovacia tabuľka

Kliknite na **Diagnosticke nástroje** a kliknite na **Routovacia tabuľka** pre otvorenie nasledovnej stránky.

Aktualna routovacia tabulka

[Obnovit](#)

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
*          0.0.0.0/          0.0.0.0 via 195.72.7.1, IF3
C~        192.168.1.0/    255.255.255.0 is directly connected, IF0
```

Obnovit' kliknite pre znovunačítanie (obnovenie) stránky.

3.12.4 ARP Cache tabulka

Kliknite na **Diagnosticke nstroje** a kliknite na **ARP Cache tabulka** pre zobrazenie obsahu ARP cache (Address Resolution Protocol) uloženej v routri. Tabuľka zobrazuje mapovanie medzi ethernet hardware adresou (MAC Address) a IP adresou

Diagnosticke nastroje >> Zobrazit ARP Cache tabulku

Ethernet ARP Cache tabulka

[Vymazat](#) | [Obnovit](#)

IP Address	MAC Address
192.168.1.10	00-12-F0-A0-E6-DB

Obnovit' kliknite pre znovunačítanie (obnovenie) stránky.
Vymazat' Kliknite pre vymazanie celej tabulky

3.12.5 DHCP tabuľka

Umožní zobrazit' informácie o pridelených IP adresách DHCP servrom. Tieto informácie sú dôležité pri diagnostike sieťových problémov, ako napr. konflikt IP adries.

Kliknite na **Diagnosticke nstroje** a kliknite na **DHCP tabulka** pre otvorenie nasledovnej stránky.

Diagnosticke nastroje >> DHCP tabulka

Tabulka IP adries pridelenych DHCP

| [Obnovit](#) |

DHCP server: Running				
Index	IP Address	MAC Address	Leased Time	HOST ID
1	192.168.1.1	00-50-7F-D8-ED-F0	ROUTER IP	
2	192.168.1.10	00-12-F0-A0-E6-DB	0:02:40.470	toshiba_pc

Index	Zobrazuje cislo pripojenia.
IP Address	Zobrazuje IP adresu pridelenu týmto routrom pre konkrétne PC.
MAC Address	Zobrazuje MAC adresu pre konkrétne PC pre ktoré bola pomocou DHCP pridelená IP adresa
Leased Time	Zobrazuje prenájatý čas platnosti pridelenej IP adresy pre PC.
HOST ID	Zobrazuje hostiteľské ID meno konkrétneho PC.
Obnovit	kliknite pre znovunačítanie (obnovenie) stránky.

3.12.6 NAT tabuľka spojení (sessions)

Kliknite na **Diagnosticke nstroje** a kliknite na **NAT tabulka spojeni** pre otvorenie nasledovnej stránky.

Diagnosticke nastroje >> NAT tabulka spojeni

Tabulka aktivnych NAT spojeni

| [Obnovit](#) |

Private IP :Port	#Pseudo Port	Peer IP :Port	Ifno	Status
------------------	--------------	---------------	------	--------

Private IP:Port	Zobrazuje zdrojovú IP adresu a port pre lokálne PC.
#Pseudo Port	Zobrazuje dočasný port routra použitý pre NAT.
Peer IP:Port	Zobrazuje cieľovú IP adresu a port vzdialeného hostiteľa.
Ifno	Zobrazuje preddefinované číslo pre rozdielne rozhranie.

0: LAN

1~2: ISDN (nepoužíte v toto modeli)

3: WAN

4 a viac: VPN

Status

Stavové hodnoty sú definované nasledovne:

0: iný TCP stav

1: TCP fin incoming

2: TCP fin out

3: TCP fin closing

4: TCP syn

5: TCP syn,ack

6: TCP ack

Obnovit

kliknite pre znovunačítanie (obnovenie) stránky.

3.12.7 Ping Diagnostika

Nasledovná funkcia umožňuje zadať do poľa IP adresa, IP adresu na ktorú sa vykona funkcia PING a tak je možnú overiť či je daná adresa IP dostupná. PO zadaní IP adresy stlačte Spustiť a po pár sekundách sa zobrazí výsledok.

Vymazať

Umožní vymazať obsah okna s výsledkom PINGU

Diagnosticke nástroje >> Ping diagnostika

Ping diagnostika

Ping na: Host / IP

IP adresa:

Spustiť

Výsledok

vymazať

3.12.8 Monitor prietoku dát

Táto funkcia umožňuje diagnostikovať prietok dát ktorý využívajú jednotlivé lokálne počítače, pričom zobrazí ich IP adresu a počet session (spojení)

Sledovanie trasy paketu

Host / IP adresa:	<input type="text"/>	<input type="button" value="Spustiť"/>
Výsledok	<div> Vymazať </div> <div><div></div></div>	