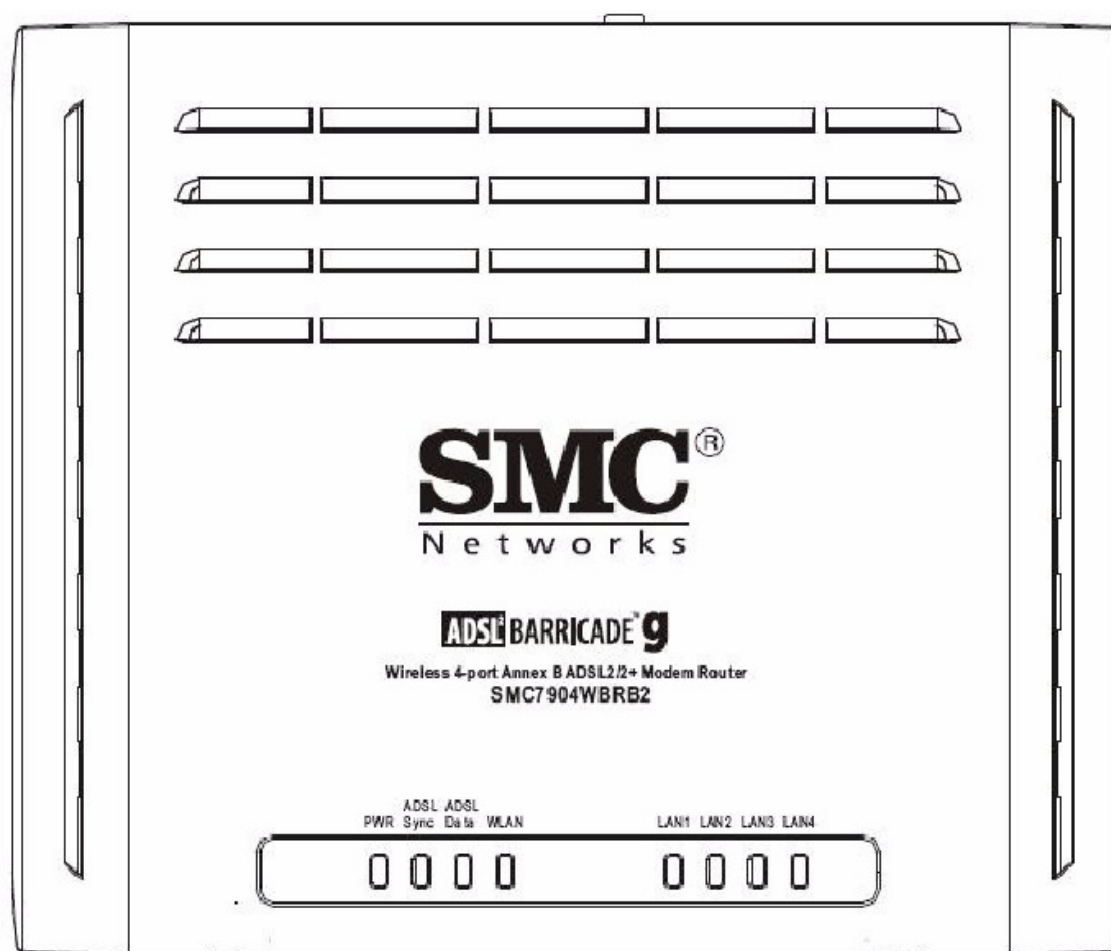


Vlastnosti a možnosti

- vestavěný ADSL/ADSL2+ modem s rychlostí až 24mbps
- lokální síťové připojení skrze 4x 10/100 Mbps Ethernetové porty
- 54mbps bezdrátový přístupový bod (standard 802.11g)
- odnímatelná anténa 2dBi s konektorem R/SMA
- protokoly WEP, WPA, WPA2 zabezpečují bezdrátovou komunikaci
- DHCP server pro automatické přidělování IP adres a DNS adres
- firewall třídy SPI (ochrana proti DoS)
- překlad adres (NAT) s podporou mapování portů pro možnost použití virtuálních serverů uvnitř sítě (webserver, FTP, P2P sítě)
- podpora průchodu VPN sítí (PPTP, L2TP, IPSec)
- rodičovská kontrola umožňuje omezit surfování po nechtěných stránkách
- vytváření filtračních pravidel na základě časového omezení
- automatické výstrahy skrze email při pokusu o napadení sítě
- podpora SNMP pro vzdálený management a monitoring
- podpora UPnP pro bezproblémový provoz P2P aplikací
- možnost nastavení statické routovací tabulky
- možnost nastavení Traffic managementu pro optimalizaci provozu realtime aplikací (telefonie, video)
- podpora VLAN, oddělení sítí připojených na jednotlivé porty.

Význam LED diod

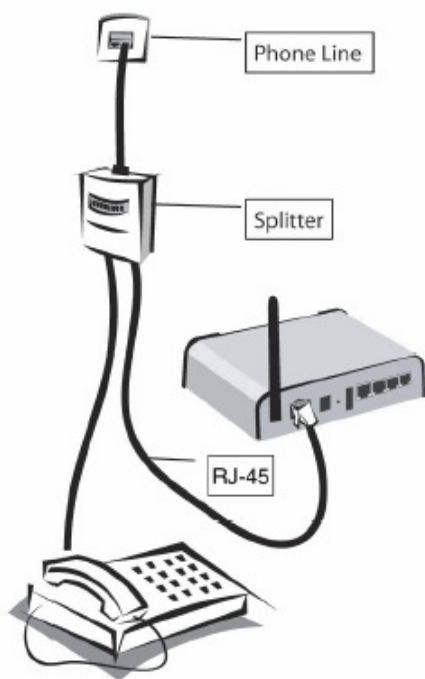


LED	Akce	Popis funkce
PWR	Svíí	Router je napájen z el. sítě, normální provoz
	Nesvíí	Router není napájen
ADSL Sync	Svíí	ADSL linka je spojena
	Bliká	ADSL linka se spojuje
	Nesvíí	ADSL linka není sestavena
ADSL Data	Bliká	přes ADSL procházejí data
	Nesvíí	Data neprocházejí
WLAN	Bliká	Bezdrátovou částí procházejí data
LAN1-4	Svíí	Port je zapojen
	Bliká	Portem procházejí data
	Nesvíí	Port není zapojen

Význam tlačítka Reset

- na zadním panelu routeru naleznete tlačítko **Reset**. Při jeho stisknutí provedete restart zařízení (stejně jako při vypnutí a zapnutí napájení).
- Pokud tlačítko při zapnutém zařízení podržíte déle než 5 sekund provedete reset zařízení do továrního nastavení. Všechny LED diody na horním panelu probliknou. Všechna vaše nastavení v routeru budou ztracena a heslo do routeru bude nastaveno na **smcadmin**.

Instalace



Zapojení:

- zapojte jednotlivé počítače pomocí ethernetových kabelů (jeden z kabelů je přiložen v balení) do portů označených jako LAN1 – LAN4
- do portu označeného jako ADSL připojte kabel a propojte jej do splitteru do portu označeného jako DSL.
- splitter zapojte mezi telefonní zásuvku a telefonní přístroj. Zásuvku připojte do portu LINE a telefon do portu PHONE.
- zapojte router do elektrické sítě a zapněte vypínač na zadní straně

Konfigurace IP adres:

- nastavte počítače tak, aby získaly adresu IP ze serveru DHCP. *(podrobnosti níže v Příloze 1)*

Konfigurace routeru:

- spustíte prohlížeč internetu (Internet Explorer, Firefox, Opera)
- zkontrolujte zda není v prohlížeči nastavená proxy: *(Internet Explorer -> Nástroje -> Možnosti internetu -> záložka Připojení -> tlačítko Nastavení místní sítě -> zrušit případné zaškrtnutí u položky Server proxy)*
- do adresního řádku napište: <http://192.168.2.1>
- do přihlašovací obrazovky zadejte heslo. Heslo nenakonfigurovaného routeru je: **smcadmin**. Doporučujeme heslo co nejdříve změnit v ovládacím rozhraní routeru.
- při prvním spuštění routeru je nutné zadat zemi v níž je router provozován, kvůli různým omezením sítí standartu 802.11b/g (bezdrátové sítě)

Konfigurace ADSL linky

- ve webovém rozhraní po přihlášení klikněte na položku Advanced Setup. Objeví se obrazovka s menu v pravém sloupci. V menu vyberte položku WAN. Klikněte na položku ATM PVC a poté v levé hlavní části obrazovky na rádek označený jako VC1.
- pro linku připojenou k síti Telefónica O2 zadejte tyto údaje:
 - **Protocol** : PPPoE
 - **VPI/VCI**: 8/48
 - **Encapsulation**: LLC
 - zadejte také uživatelské heslo (username) a 2x heslo (Password a confirm password), které vám poskytne Váš ISP. Ostatní položky neměňte.
- pro linku připojenou k síti Českého Telecomu, která je založena před 31.3. 2005 nebo pro linku některých alternativních operátorů (AVONET) zadejte tyto údaje:
 - **Protocol** : PPPoA
 - **VPI/VCI**: 8/48
 - **Encapsulation**: VC MUX
 - zadejte také uživatelské heslo (username) a 2x heslo (Password a confirm password), které vám poskytne Váš ISP. Ostatní položky neměňte.

ATM Interface

	ATM1
Protocol	PPPoE
VPI/VCI	8 / 48
Encapsulation	LLC
QoS Class	UBR
PCR/SCR/MBS	4000 / 4000 / 10
IP assigned by ISP	Yes
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Connect Type	Always Connected
Idle Time (Minute)	5
Username	
Password	
Confirm Password	
MTU	1492

Popis ovládacího menu:

v následujících odstavcích Vám popíšeme jednotlivé části konfiguračního menu, které uvidíte po přihlášení a kliknutí na položku **Advanced Settings**.

System (Systémová Nastavení)

Tato stránka obsahuje všechny konfigurační nástroje pro Barricade, jako např. časové pásmo, nastavení hesla a vzdálená správa.

Time Zone – nastavení časové zóny a serverů pro synchronizaci času routeru.

Password Settings – nastavení hesla pro přístup do routeru a času po jehož uplynutí bude přihlášení ukončeno.

Remote Management – nastavení vzdáleného přístupu do ovládání routeru.

Enabled – zapíná nebo vypíná vzdálený přístup k routeru z Internetu

Host Address – IP adresa z níž je povolen přístup k routeru. Pokud vyplníte 0.0.0.0 bude přístupný z jakéhokoliv počítače

Port Number – nastavíte požadovaný port pro vzdálený přístup. Standardní nastavení je 8080

WAN

Slouží k zadání informací o způsobu připojení Vašeho routeru k Internetu. Pro korektní informace kontaktujte svého ISP.

ATM PVC – definuje virtuální okruhy, kterých router umí až 8. Obvykle využijete pouze VC1, kde vyplníte údaje svého ISP. (viz výše)

Clone MAC Address – položku využijete v případě, že ISP omezuje připojení na konkrétně definovanou MAC adresu. Obvykle není potřeba nastavení měnit.

DNS – slouží k zadání DNS serverů. Pro správné údaje kontaktujte svého ISP. Obvykle je možné ponechat defaultní nastavení 0.0.0.0

LAN (Nastavení LAN)

LAN IP - Router Barricade musí mít IP adresu pro lokální síť. Tu přidělíte v položce „**IP address**“ (standardně 192.168.2.1)

DHCP Server - Můžete povolit nebo zakázat serveru DHCP dynamicky přidělit IP adresy Vaším klientským PC.

Lease Time = na jak dlouho bude adresa přidělena. Doporučujeme nastavit Forever (napořád)

IP Address Pool – rozsah přidělovaných IP adres DHCP serverem.

VLAN Binding – zde můžete ke každému jednotlivému LAN portu přidělit rozdílnou VLAN (definovanou v LAN -> VLAN). Nastavení umožní provozovat více nezávislých sítí na jedné ADSL lince.

>> **VLAN** – definujete jednotlivé VLAN, které poté můžete přidělit jednotlivým LAN portům

WIRELESS (Nastavení bezdrátového přístupového bodu)

Položka slouží ke konfiguraci bezdrátového připojení. Výběrem **Enable** bezdrátové rozhraní zapnete a volbou **Disable** vysílání vypnete.

Channel and SSID – **SSID** – nastavení jména sítě

SSID Broadcast – vypnutí nebo zapnutí šíření jména sítě. Pro větší bezpečnost doporučujeme vypnout (Disable)

Wireless Mode – zvolte parametr rychlosti síťového rozhraní. Doporučujeme volbu Mixed

Channel – zvolte kanál na kterém bude vysílat vestavěný bezdrátový přístupový bod.

Access Control – na základě MAC adresy bezdrátových síťových karet můžete filtrovat přístup k bezdrátové části Vašeho routeru.

Enable MAC filtering – zapnete nebo vypnete filtraci.

Access Rule for registered MAC address – zvolte zda seznamu adres níže povolíte (**Allow**) nebo naopak zakážete(**Deny**) přístup.

MAC Filtering table – do seznamu zadejte seznam MAC adres. Tlačítkem „Add currently associated MAC stations“ automaticky vyplníte právě přihlášené síťové karty.

Security – zvolíte protokol zabezpečení bezdrátového rozhraní.

No WEP, No WPA – šifrování vypnuto. Z bezpečnostních důvodů nedoporučujeme.

WEP only – použijte nastavení šifrování 64bit nebo 128bit WEP. Doporučujeme použít pouze pokud v bezdrátové síti jsou zařízení, které nepodporují modernější WPA.

WPA only – nejbezpečnější šifrování, doporučeno.

WEP – nejprve vyberte ve **WEP mode** úroveň šifrování (doporučujeme 128-bit), poté do políček **Key1** až **Key4** zadejte šifrovací klíč. Stačí vyplnit pouze jedno políčko. Stejný klíč zadejte i v nastavení Vaší síťové karty.

WPA – ve volbě WPA mode zadejte typ šifrování (doporučujeme WPA/WPA2 Mixed mode). Pak vyplňte položku Pre-shared Key heslem. Stejně heslo vyplňte také v nastavení Vaší síťové karty.

802.1x – zabezpečení, využitelné v podnikových sítích, které používají RADIUS server pro autorizaci uživatelů pro přístup k bezdrátové síti. Pro správnou funkčnost vyberte položku 802.1x ve volbě **Authentication** u nastavení šifrování **WPA**

WDS – Wireless Distribution System. Umožňuje spojit Přístupové body s podporou WDS do širší sítě a zvýšit tak jejich dosah.

Enable or disable WDS feature – zapne nebo vypne WDS

AP MAC address table – zadejte MAC adresu přístupových bodů, které chcete přidat do systému WDS.

NAT (Nastavení NAT – překladu adres)

Network Address Translation (NAT) umožňuje více uživatelům z Vaší lokální sítě připojení na Internet přes jedinou veřejnou IP adresu nebo více veřejných IP adres. NAT může také zabránit hackerským útokům mapováním lokálních adres na veřejné adresy pro klíčové služby jako WWW nebo FTP.

Address Mapping

Network Address Translation (NAT) umožňuje IP adresy používané v soukromé lokální síti mapovat na jednu nebo víc adres používaných ve veřejném, globálním Internetu. Tato charakteristika limituje počet veřejných IP adres požadovaných od ISP a taky udržuje soukromí a bezpečnost lokální sítě. Povolujeme

mapování jedné nebo víc než jedné veřejné IP adresy na skupinu lokálních adres. Využijte v případě, že máte od Vašeho ISP více veřejných IP adres.

Virtual Server (Virtuální Server)

Můžete nakonfigurovat Barricade jako virtuální server, takže vzdálení uživatelé přistupující na služby jako Web nebo FTP na Vaší lokální síti přes veřejné IP adresy mohou být automaticky přesměrováni na lokální servery nastavené se soukromými IP adresami. Jinými slovy, v závislosti na požadované službě (TCP/UDP číslo portu), Barricade přesměruje vnější požadavek na službu na příslušný server (umístěný na jiném vnitřní IP adrese). Tento nástroj může podporovat jak rozsah portů a vícenásobné porty, tak i jejich kombinace.

LAN IP address – IP adresa počítače ve vnitřní síti na kterém běží daná služba nebo server.

Protocol Type – volba protokolu který daná služba vyžaduje. (obvykle TCP)

LAN port – port ve vnitřní síti na kterém služba běží (např: WWW = 80, FTP = 21).

Public Port – port, který je vidět „zvenčí“. Může ale nemusí být shodný s LAN port. To umožní mít ve vnitřní síti více např. WWW serverů.

Enable – po zaškrtnutí začne pravidlo fungovat. Nezapomeňte zmáčknout tlačítko Add

Special Applications (Speciální Aplikace)

Některé aplikace vyžadují násobné připojení, jako např. hraní přes Internet, video konference, Internetové telefonování a jiné. Tyto aplikace nemohou pracovat, pokud Network Address Translation (NAT) je povolena. Pokud potřebujete spustit aplikace, které vyžadují násobné připojení, určete port normálně sdružený s aplikací v poli "Trigger Port", zvolte typ protokolu jako TCP nebo UDP, pak vložte veřejné porty sdružené se spouštěcím portem (trigger port) pro jejich otevření pro příchozí spojení. V položce „Popular Applications“ najdete připraveno nastavení pro několik nejoblíbenějších aplikací.

NAT Mapping Table (tabulka NAT spojení)

V tabulce naleznete seznam aktuálních spojení, které jsou právě v routeru aktivní. Počet spojení by neměl být větší než přibližně 3000. Pokud máte příliš velký počet těchto spojení, zkontrolujte programy ve vnitřní síti.

ROUTING

Položka slouží ke konfiguraci Statických routovacích tabulek v případě, že v síti máte více než jeden router. Také zde můžete nastavit protokol RIP. Doporučujeme nechat nastavení na výchozích hodnotách.

FIREWALL (Bezpečnostní Nastavení)

Barricade poskytuje rozšířenou ochranu firewallem omezením parametrů připojení pro snížení rizika útoku hackerů, a obranu proti široké škále běžných útoků. Avšak pro aplikace, které vyžadují neomezený přístup k Internetu, můžete nastavit určitého klienta/server jako demilitarizovanou zónu (DMZ).

Parental Control – umožňuje nastavit, které služby nebo protokoly mají být blokovány pro konkrétní uživatele sítě na základě zadaných pravidel.

MAC Filter – seznam MAC adres zařízení (počítačů) které mají zakázán nebo naopak povolen přístup do vaší vnitřní sítě.

Website Blocking – seznam domén nebo klíčových slov v názvu domény ke kterým bude zakázán přístup. Např: sex = bude zakázán přístup ke všem doménám, které mají ve svém názvu „sex“ (sex.com, ale i sussex.com.uk apod.)

Advanced – umožňuje zapnout pokročilý firewall a nastavit detaily, kam mají být zasílány upozornění o možném útoku na Vaši síť

DMZ – Demilitarizovaná zóna – pokud některé aplikace, které ve Vaší síti provozujete vyžadují neomezený přístup k internetu, zařaďte počítač do DMZ.

SNMP

SNMP (Simple Network Management Protocol) slouží k ovládání a kontrole stavu routeru. V položce SNMP operation mode zvolte pro které rozhraní chcete SNMP používat. Pokud SNMP nepoužíváte doporučujeme jej nastavit na: Disabled

Community - nastavte hesla a přístupové údaje pro externí programy s podporou SMTP, které mohou router ovládat

Trap – Nastavte server, kam bude automaticky router zasílat informace o svém stavu.

UPnP

Zapnutí UPnP umožní operačním systémům a programům s jeho podporou (Windows XP, Me, Vista) automaticky konfigurovat router aby mohly být využívány pokročilé funkce některých programů pro přenos dat (P2P sítě, Instant messaging (ICQ, MSN)). Vzhledem k tomu, že je to možné bezpečnostní riziko, doporučujeme při zapnutí této vlastnosti mít zapnut i firewall v PC.

QoS

Sekce QoS je vhodným nástrojem, jak zajistit, aby některé aplikace (jako třeba telefonování přes internet) nebo počítače měly vždy zabezpečený přístup k WAN lince.

Na úvodní stránce můžete jedné ze sedmi skupin (EF je nejvyšší priorita, BE nejnižší) přidělit minimální hodnotu v procentech. Tato hodnota pak bude použita pouze pro provoz, který bude patřit k této skupině. (obvykle toto doporučujeme pouze pro skupinu EF). Zaškrtnutím políčka **Allow More** umožníte aby provoz spadající do dané třídy využíval více než definované procenta. Zrušit zaškrtnutí je vhodné pouze u málo upřednostňovaných tříd. (BE)

Traffic Mapping – je možné si nadefinovat jednotlivé typy provozu nebo počítače, které budou mít větší nebo menší prioritu při přístupu k Internetu. Standardně je předpřipraveno pravidlo pro prioritizaci provozu internetové telefonie. Můžete si přidat vlastní pravidla.

Traffic Statistics – Zobrazuje statistiku dat pro jednotlivé druhy provozu. Můžete vidět statistiku maximálně za posledních 12 hodin. Zobrazeny jsou data pro průměrné využití jednotlivých pravidel a počty zahozených paketů.

ADSL

Nastavení ADSL protokolu a diagnostika ADSL linky

Parameters – Nastavení Operačního módu ADSL linky. Doporučené nastavení: **Automatic**

Status – kontrola a diagnostika ADSL linky

DDNS

Dynamický DNS poskytuje uživatelům na Internetu způsob, jak spojit jejich název(y) domén(y) s počítači nebo servery. DDNS umožňuje Vašemu názvu domény sledovat Vaší IP adresu automaticky změnou DNS záznamů, když se změní Vaše IP adresa. Tuto službu využijete v případě, že máte od svého ISP dynamicky přidělovanou adresu, ale přesto chcete provozovat služby jako www server nebo FTP server.

TOOLS

Ping Utility – umožňuje poslat příkaz ping na počítač ve vnitřní síti a ověřit tak, zda je zapnut. Je možné poslat ping in na počítače ve vnější síti

TraceRoute Utility – dovoluje pomocí příkazu TraceRoute ověřit síťovou cestu k jinému počítači ve vnitřní síti nebo v Internetu

Configuration Tools – můžete zálohovat konfiguraci Vašeho routeru nebo jej nastavit do továrního nastavení (Reset to default settings)

Firmware upgrade – dovoluje provést upgrade na aktuální verzi firmware.

Reboot – provede restart routeru v případě, že router projevuje nestandardní chování. Nastavení routeru nebude ovlivněno.

STATUS

Obrazovku Status můžete použít pro zobrazení stavu připojení WAN/LAN rozhraní, čísel verzí firmware a hardware, jakýchkoliv nepovolených pokusů o přístup do Vaší sítě, stejně jako informací o všech DHCP klientech právě připojených do Vaší sítě

Příloha 1:

Konfigurace TCP/IP protokolu

Windows 2000/XP

- zvolte Start -> Nastavení -> Ovládací panely -> Síťová připojení
- poklikejte na ikonku síťové karty, která je připojena do router (typicky má název Připojení k místní síti)
- stiskněte tlačítko Vlastnosti
- na následující kartě najděte položku Protokol sítě TCP/IP. Označte ji, ujistěte se, zda je zaškrtnuta a klikněte na tlačítko Vlastnosti níže.
- Vyberte volbu: Získat adresu IP ze serveru DHCP automaticky a níže také volbu Získat adresu serveru DNS automaticky.

Windows 98SE/ME

- zvolte Start -> Nastavení -> Ovládací panely -> Síť
- Na záložce konfigurace vyberte položku TCP/IP -> (název síťové karty)
- stiskněte tlačítko Vlastnosti
- na záložce IP adresa zvolte možnost: „Získat adresu IP automaticky“
- na záložce Brána zkontrolujte, zda je položka Brána prázdná, případně ji smažte. (označte ji myší a stiskněte tlačítko smazat)

Příloha 2:

Často kladené dotazy (FAQ):

1) Jak zajistím abych byl „Active user“ v programu Direct Connect ++

- zajistěte aby počítač, kde běží DC++ měl pevnou IP adresu (neměla by být přidělována z DHCP, jinak hrozí, že se adresa změní a nastavení nebude fungovat)
- v nastavení routeru najděte sekci Advanced settings -> NAT -> Virtual server
- do pole LAN IP address vyplňte IP adresu počítače
- Protocol Type = TCP&UDP
- LAN port a Public port = číslo portu na kterém DC++ běží (obvykle 3084)
- zaškrtněte políčko Enable a klikněte na Add

2) Jak nastavím, abych zvenčí měl přístup pro vzdálenou správu na více počítačích?

- na všechny počítače nainstalujte potřebný software (např: VNC)
- zajistěte aby počítače, kde běží VNC měly pevnou IP adresu (neměla by být přidělována z DHCP, jinak hrozí, že se adresa změní a nastavení nebude fungovat)
- v nastavení routeru najděte sekci Advanced settings -> NAT -> Virtual server
- do pole LAN IP address vyplňte IP adresu počítače
- Protocol Type = TCP
- LAN port a Public port = číslo portu na kterém VNC běží (obvykle 5900)
- zaškrtněte políčko Enable a klikněte na Add
- nastavení opakujte pro všechny IP adresy kde běží požadovaný software s tím, že pro každý další řádek použijete jiné číslo portu v kolonce „Public port“ (např 5901, 5902)
- pro každý počítač budete mít zvenčí specifický přístup, který bude odlišen číslem portu: (např: 123.123.123.123:5903)

3) Jak zajistím, aby jeden počítač měl přednost v přístupu k internetu před ostatními?

- Zjistěte si IP nebo MAC adresu preferovaného počítače
- V menu QoS se ujistěte, že hodnota „Enable or Disable QoS function“ je na Enable
- V menu QoS -> Traffic Mapping zmáčkněte tlačítko Add traffic clas
- Pojmenujte pravidlo (rule name) a zvolte Local Address (vyberte IP Range)
- Do polozky IP Range zadejte např.: 192.168.2.100 – 100 (bude preferován jeden počítač s toto IP adresou.)
- Remote Address ponechejte na (Any)
- Traffic Type – můžete ponechat Any pro jakýkoliv provoz nebo vyberte z menu.
- Map to Forwarding Group – zvolte AF4x nebo EF (čím blíže k EF tím větší priorita)
- Direct to VC – By routing
- Po takovém nastavení bude mít zadaný počítač preferovaný přístup k datům na Internetu.

4) Co je to MAC adresa?

- MAC (Medium Access Control) adresa je fyzická adresa každého síťového zařízení
- adresa je na světě jedinečná a žádná dvě zařízení nemají z výroby stejnou
- zjistit adresu je možné obvykle na obalu zařízení nebo je vytištěna na zařízení samotném.
- ve Windows zjistíte adresu takto:
- Win NT/2000/XP – spusťte Start -> Spustit -> napište příkaz cmd a klikněte na OK. Napište příkaz: „ipconfig –all“ (bez uvozovek). Ve výpisu uvidíte řádek: Fyzická adresa.
- má tvar obvykle podobný jako: 00-00-39-37-A5-A9 nebo 00:00:39:37:A5:A9