Desktop jako na dlani

Jak bezpečně přistupovat na vzdálený počítač (CD)

PATRIK MALINA

Jistě tu situaci znáte: přicházíte domů a právě jste zjistili, že důležitou práci jste zapomněli na firemním počítači v kanceláři. Nebo obráceně? Přicházíte do práce a důležité dokumenty máte na domácím PC. Nebo potřebujete vzdáleně spustit aplikaci, „navštívit" pracovní plochu… Řešíte tyto potíže? Pak pokračujte následujícími odstavci!

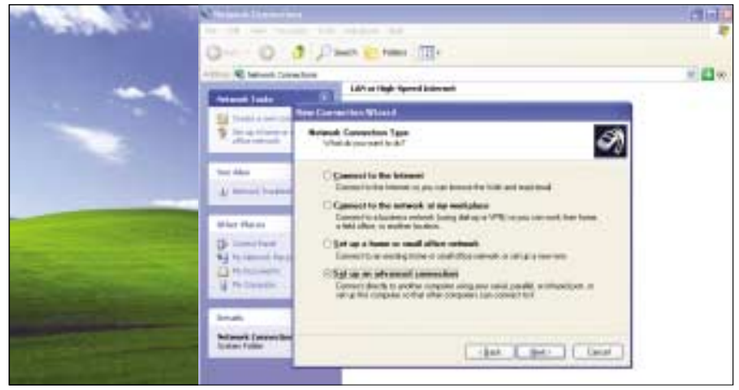
Vzdálený přístup k počítači prostřednictvím síťových cest není požadavek nijak nový ani nijak neobvyklý. Používání terminálů pro práci na vzdáleném, výkonném síťovém serveru je oblíbený model, jenž se prosadil dávno před nástupem počítačů třídy PC, a v různých podobách se stále vrací do módy. Navíc i dnes, kdy místo pracovních stanic dominují „písíčka", je pro administrátory často nezbytným nástrojem vzdálené zpřístupnění strojů jednotlivých uživatelů, neboť větší sítě často ani jinak spravovat nelze. Vývoj příslušného softwaru a operačních systémů však dnes již bez problémů dovoluje podobné formy vzdálené práce využívat i v případě malých domácích sítí a jste-li třeba často na cestách nebo potřebujete komunikovat na trase domov – zaměstnání, při troše trpělivosti se vám jistě vše podaří zprovoznit.

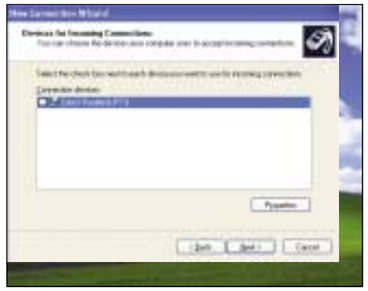
V následujících odstavcích se zaměříme jak na samotné přenesení rozhraní vzdáleného počítače, tak na další související přípravné kroky, bez nichž by často taková komunikace nebyla možná. Řekneme si, co je potřeba udělat pro dostatečnou míru zabezpečení, a také si vysvětlíme, jaké překážky na trase by vás mohly potkat. Než se do realizace některých scénářů pustíte, uvažte, že určité akce nelze realizovat bez asistence administrátorů firemních sítí, do nebo z nichž chcete komunikovat. Takže občas je potřeba kromě technologie též trocha diplomatického přístupu.

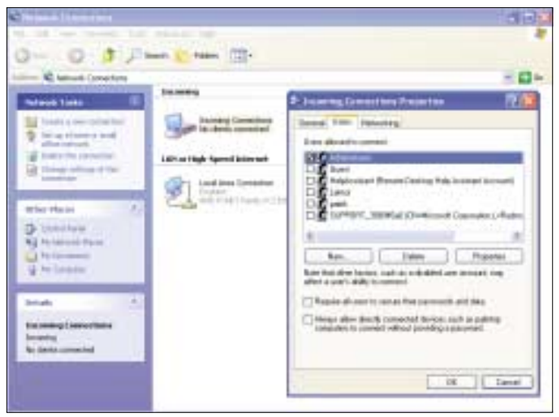
PRVNÍ FÁZE: budujeme bezpečný přístup

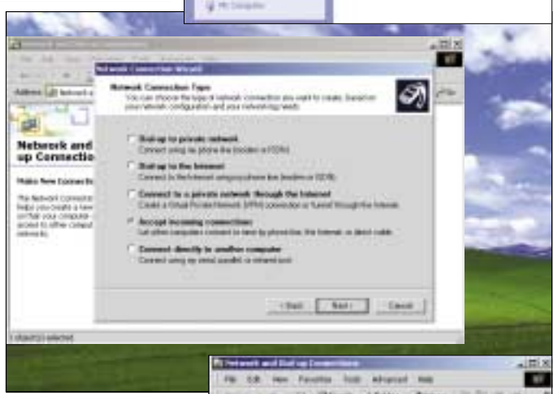
Vzdálený přístup a přenesení pracovního prostředí je možné realizovat podle řady scénářů v závislosti na tom, kde se nacházejí oba počítače – lokální, z nějž budete fyzicky komunikovat, a vzdálený (anglicky remote), k němuž se chcete připojit. V nejjednodušším případě jsou stroje umístěny ve stejné lokální síti (LAN), tedy uvnitř firmy či třeba v jediné domácnosti, a jejich propojení je provedeno přímo pomocí síťových karet a technologie Ethernet. Tato situace je sice nejsnazší, avšak ne zase tak častá: kdybych byl ve stejné domácnosti či kanceláři, asi bych si raději přímo sedl ke správnému stroji. Mnohem typičtější je tedy scénář, kdy propojení dvou PC realizujeme

„na dálku" přes rozlehlejší síť, kterou je typicky internet. A právě využití veřejné sítě s sebou přináší zásadní problém a riziko v podobě možnosti ohrožení komunikaci útočníkem zvenčí. Pokud se budete nedostatečně zabezpečeným kanálem připojovat ke vzdálenému počítači, mohl by si toho někdo „všimnout" a ve volné chvilce to zkusit tak jako vy s využitím znalostí, jež byly odposlechnuty. Pak by mohl takový útočník v případě úspěchu manipulovat se vzdáleným strojem stejně jako oprávněný uživatel. Naším úkolem je tedy v první řadě zajistit mezi lokálním a vzdáleným PC sestavení bezpečného kanálu, v jehož útrobách pak již s minimálním rizikem budete přenášet data pro vzdálenou práci.

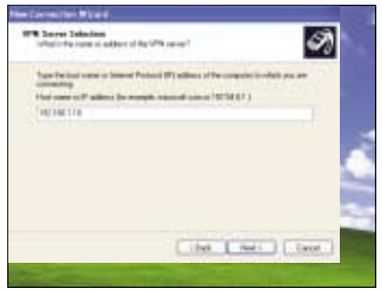








Protože v případě malých sítí či „domácího" nasazení nelze předpokládat, že byste využívali vyhrazených telefonních linek či jiných soukromých spojů, samozřejmou volbou pro požadované sestavení chráněného kanálu je využití technologie virtuálních privátních sítí. V této části si ukážeme, jak prakticky nastavit počítače na obou koncích pro sestavení VPN. Pokud vás zajímají podrobnosti o těchto technologiích, nahlédněte do rubriky Komunikace v tomto čísle, kde se podstatě VPN věnujeme více. Než se do vlastního nastavení pustíme, ještě jednou připomínáme, že

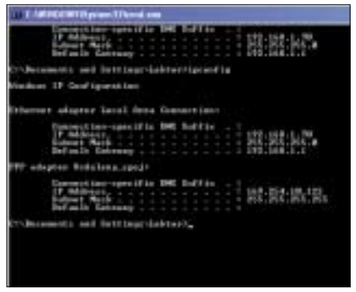


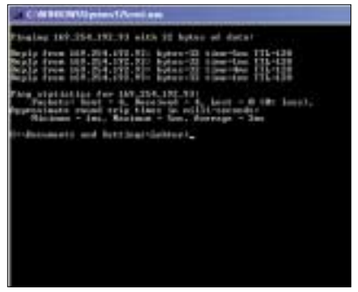
je potřeba mít vyřešenu otázku internetové konektivity – v opačném případě totiž nemáte, kudy byste VPN „protlačili“.

Naši práci začněme na počítači, jenž označujeme jako vzdálený: pokud vás to překvapuje, pak právě zde nadešla chvíle přehodnotit plány, neboť před samotným zprovozněním vzdáleného přístupu budete opravdu muset alespoň jednou váš cílový stroj nakonfigurovat. Naším prvním krokem tedy bude vytvořit z něj VPN server pro příchozí spojení. Ukázky jsou v tomto případě realizovány většinou v prostředí Windows XP se SP1, některé drobné odlišnosti pak ukážeme na Windows 2000 Professional.

Konfiguraci zahájíme, jak jinak, pomocí ovládacího rozhraní *Network Connections* (Síťová připojení), kde si spustíme průvodce pro nové síťové připojení. Po uvítací obrazovce následuje rozhodovací bod: zde je potřeba vybrat volbu *Advanced Connection*. Na následující obrazovce pochopitelně volíme *Accept incoming connections* (přijmout příchozí spojení) a pokračujeme dalším oknem, v němž se operační systém pokusí zobrazit všechna zařízení, pomocí nichž je možné vzdáleně přistoupit. Protože konfigurujeme VPN a rozhraní jako telefonní modem či sériový kabel nás tedy nezajímají, beze změny pokračujte na další kartu a zaškrtněte volbu povolující příchozí VPN spojení. O obrazovku dále vám průvodce nabídne přehled existujících uživatelských účtů, z nichž můžete vybrat ty, jimž připojení virtuální sítě dovolíte. Následující okno je pak poměrně důležité: říkáte zde, které protokoly budou pro tunelování skrz navázané VPN spojení povoleny, což nemusíte měnit. Pokud ale chcete být důslední a postupovat opravdu co nejpřísněji, nechte jako platnou (zaškrtnutou) pouze volbu *TCP/IP*. Systém vám však bude sdělovat, že je nutno zastavit službu Server, jež se stará o sdílení složek a tiskáren – to však nemusí vždy dopadnout úplně nejlépe, takže to uvažte. Poté průvodce klidně ukončete. V okně síťových rozhraní vám přibude ikona pro příchozí spojení. Pokud na ní kliknete pravým tlačítkem a vyvoláte *Vlastnosti*, můžete i dodatečně některé parametry pro VPN změnit. Budete-li obdobná nastavení provádět ve Windows 2000 Professional, může průvodce vypadat mírně odlišně. Volbu pro příchozí spojení najdete přímo na rozhodovací obrazovce, zbytek je však prakticky shodný.

Přijímající počítač tedy máme připraven, přesuneme se na stroj, s nímž cestujeme a z nějž budeme spojení iniciovat. Opět použijeme průvodce novým síťovým připojením a tentokrát volíme položku *Connect to the network at my workplace* (tedy jako bychom se připojovali „do práce“). V dalším kroku samozřejmě volíme variantu *VPN*, o obrazovku dál přidělte novému spojení výstižné jméno (na funkci to nebude mít žádný vliv) a postupte do dalšího okna, kde budete zadávat veledůležitou adresu vzdáleného počítače v síti. Zde můžete narazit na potíže – pokud adresu neznáte, přejděte do následujícího odstavce, kde se problému věnujeme. A v závěrečném kroku průvodce nezapomeňte zatrhnout volbu, díky níž se nové připojení uloží jako zástupce na pracovní plochu, abyste je měli po ruce. Posléze již dojde k otevření samotného startovacího dialogu: stačí zadat přihlašovací jméno a heslo k účtu, jemuž jste na vzdáleném počítači povolili přístup, a spojení může být sestaveno. O tom, že spojení vzniklo, se můžete přesvědčit také v příkazové řádce, kde se po zadání příkazu *IPCONFIG* objeví hlášení, v němž bude figurovat PPP nebo WAN adaptér pod jménem, jež jste mu přidělili.





Co je vlastně výsledkem naší snahy? Sestavili jsme chráněný tunel mezi lokálním (odchozím) a vzdáleným (přijímacím) počítačem, a touto síťovou „rourou“ teď můžeme poměrně bezpečně zasílat data, pomocí nichž lze třeba vzdáleně onen stroj ovládat. Jednu věc však ještě potřebujeme ověřit: adresaci vzdáleného počítače v sestaveném tunelu a opravdovou prostupnost. Přejděme tedy opět na vzdálený (přijímající) stroj a pomocí stejného příkazu – IPCONFIG – se přesvědčme, že vše dopadlo dobře. Ve výpisu by se mělo objevit něco o PPP adaptéru RAS serveru a zároveň bude k dispozici přiřazená IP adresa. S její pomocí lze pak příkazem *PING* dokončit ověření průchodnosti spoje z protějšího počítače.

Máme za sebou tedy první fázi: bezpečné spojení. Pokud se vám operace nepodařila, v následujícím odstavci bude řeč o nejčastějších problémech. Je-li vše funkční, můžete poté pokračovat další částí – samotným přenosem vzdáleného ovládání.

DRUHÁ FÁZE: prošlapáváme trasu

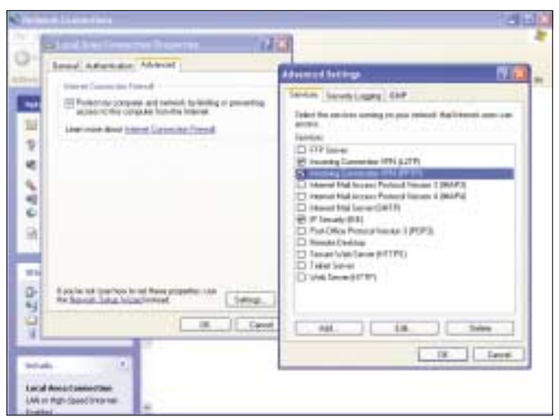
Bohužel zdaleka ne vždy probíhá „propojovací“ akce tak hladce, jako jsme naznačili v předchozím odstavci. V bezprostředně následujících řádcích si řekneme o typických úskalích a jejich možných řešeních.

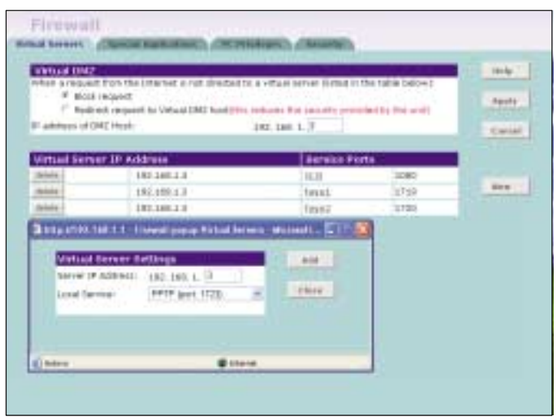
Při sestavování ochranného síťového tunelu můžete v první řadě narazit na problém, že oba počítače nemusí být přes internetovou globální síť tak snadno viditelní. Pokud jste byli pozorní, jistě vám neušlo, že jsme v průvodci pro odchozí VPN linku zadávali konkrétní IP adresu cílového (přijímacího) počítače. Nezbytnou podmínkou pro celou operaci je to, že ona cílová adresa bude v internetu ze zdrojového počítače přímo viditelná, čemuž v praxi může stát v cestě řada překážek.

První problém s adresací představují samotní poskytovatelé internetové konektivity (ISP). Pokud jste na cestách a přijímacím (vzdáleným) počítačem je vaše PC doma, můžete mít potíže díky tzv. dynamicky přidělované adrese. ISP vám totiž z různých důvodů může přidělovat IP adresu pomocí služby DHCP, a to při každém připojení internetu jinou, což samozřejmě iniciaci spojení z notebooku na cestách dosti ztěžuje. Řešením je dnes již nepříliš nákladná varianta – požádat ISP o přidělení adresy statické tak, abyste se zvenčí na váš cílový počítač „trefili“.

Dalším problémem může být, rovněž u poskytovatele internetu, nasazení služby NAT (tzv. překladu síťových adres). Z různých důvodů může docházet k tomu, že adresa vašeho počítače na internetovém rozhraní (směrem k ISP) nebude stejná jako ve veřejném internetu. Toto maskování má své důvody a k jeho překlenutí potřebujete od ISP zaručit dvě věci: že vám přidělí statickou IP adresu (tu skutečnou, úplně veřejnou) a že překlad adres (NAT) bude provádět v poměru 1 : 1, tedy že se vždy přes úplně veřejnou adresu trefíte po překladu na váš domácí počítač. Ani to už není požadavek nijak výjimečný a drahý. Samozřejmě to připadá v úvahu u služeb jako ADSL, kabelová televize či „bezdrát“, v případě dial-upu s ničím podobným moc nepočítejte…

Další překážkou na cestě může být firemní síť. Už jsme v našich scénářích naznačili, že typickým cílem – vzdáleným počítačem – může být naše pracovní PC v kanceláři či jinde na pracovišti. Takový stroj samozřejmě není přímo „vystrčen“ do internetu, tedy pokud administrátor není blázen, a vy budete potřebovat jeho pomoc. V zásadě jsou zde dvě možná řešení. První vyžaduje, aby vám administrátor na hranicích firemní sítě (firewallu) otevřel příslušná „dvířka“ pro cestu dovnitř – při konzultaci uvádějte, že potřebujete prostoupit pomocí protokolu PPTP, což by mu mělo postačovat. Ovšem přichází jiný problém: firemní sítě, stejně jako ISP, často využívají službu NAT, takže stejně nebudete moci přímo zacílit na IP adresu vašeho firemního desktopu. Řešením je tedy varianta druhá, a to využití nějakého firemního RAS či VPN serveru, což je pravděpodobně možné. Ovšem pozor, zde dochází ke změně celého scénáře! Přijímacím počítačem pro tunel už nebude váš vzdálený stroj, ale jiný firemní server, jehož parametry vám





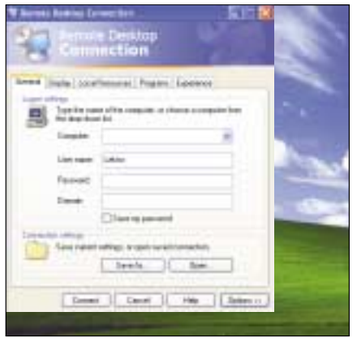
správce sdělí. Zcela tak odpadá nutnost konfigurovat výše popsané příchozí spojení na vzdáleném počítači, neboť to administrátor udělá za vás na VPN serveru a pustí vás rovnou do firemní sítě. Cesta pro další kroky pak již bude volná.

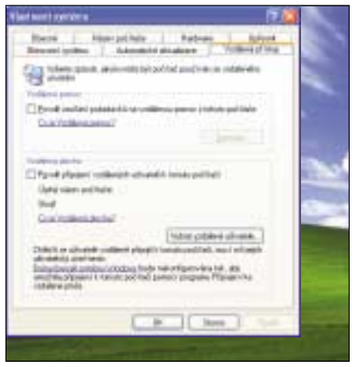
Ještě dobrodružnější situace nastane, pokud se podobně jako firemní firewall chová nějaké zařízení ve vaší domácí síti. Typicky takto pracuje třeba pokročilý ADSL modem či domácí hardwarový router/firewall. Ten právě realizuje službu NAT i ochranu před příchozí komunikací a pokud jej nenastavíte, bude vaší snahu přistoupit na domácí PC odněkud zvenčí považovat za neoprávněnou. Problém vyřešíte tím, že váš vnitřní počítač šetrně vystavíte z domácí sítě do internetu, k čemuž se většinou používá funkce s názvem Virtual DMZ, Server publishing či podobné. Příslušné nastavení pak musí říkat, že dovnitř propouštíte protokol PPTP, jehož pomocí se tunelované spojení realizuje, a že má být přesměrováno na určitou vnitřní, ukrytou IP adresu. A teď otázka: jakou cílovou adresu zadáte na straně VPN klienta (odchozího spojení) na počítači mimo domov, z nějž budete přistupovat vzdáleně? Správně, tu, kterou jste si podle výše uvedených instrukcí domluvili se svým ISP!

Na závěr uveďme, že úplně stejnou překážkou může být také samotný firewall v operačním systému Windows, jenž dokáže příchozímu spojení zabránit. Proto je potřeba jej nakonfigurovat stejně jako domácí hardwarový router/firewall pro příjem spojení PPTP. Pokud však nebudete provádět žádné vlastní zásahy, po spuštění služby příjmu příchozích spojení by si měl Windows firewall příslušné porty připravit a otevřít sám, jak je patrné z obrázku na předchozí straně.

TŘETÍ FÁZE: přenášíme pracovní plochu

Možná si říkáte, že jsme toho pro bezpečnost už udělali dost a je načase se opravdu vzdáleně připojit. Pokud máte cestu pomocí VPN sestavenou, můžeme opravdu přistoupit k ovládnutí plochy vzdáleného počítače. Ukážeme si několik cest a také několikeré softwarové vybavení, které je k dispozici. Každá z naznačených cest má své výhody i nevýhody, takže nezbývá než si poté vybrat. Nezapomeňte také, že otázku vzdáleného přístupu, tedy vlastně terminálového spojení, musíte vyřešit opět na obou stranách spojení – na počítači „mimo domov a kancelář", tedy na terminálovém klientu, a na počítači vzdáleném, jenž bude plochu předávat a jemuž budeme jinak říkat terminálový server.





Windows a Vzdálená plocha

Jste-li uživateli operačního systému Windows, může vám k rychlému zpřístupnění vzdáleného počítače posloužit přímo dostupná komponenta s názvem **Remote Desktop Connection**. Jde o klientskou aplikaci, s jejíž pomocí můžete využít libovolný terminálový server na platformě Windows – typickým „cílem" tak mohou být právě Windows XP, jež nabízejí serverovou část pod názvem **Remote Desktop**. Klientská aplikace je ve Windows XP umístěna přímo v části *Programy-Příslušenství-Komunikace* a při jejím spuštění máte k dispozici okno pro zadání základních přihlašovacích údajů. Do pole *Computer/Počítač* zadáváte IP adresu nebo jméno cílového (vzdáleného) stroje, na jehož plochu se chcete připojit, čímž jasně říkáte, kdo je příjemcem spojení. Zde nezapomeňte na velmi důležitou věc: pokud jste před tímto krokem realizovali výše popsané VPN spojení, je v tuto chvíli nutné zadat IP adresu, jež platí uvnitř sestaveného privátního tunelu! Vzpomeňte si: najdete ji po úspěšném VPN spojení třeba pomocí příkazu IPCONFIG, spuštěném na vzdáleném počítači – jenže to asi stěží uděláte, když bude skutečně vzdálený! Samozřejmě existuje cesta: klepněte v panelu vedle hodin na ikonu aktivního VPN spojení a v okně vlastností, jež se zobrazí, přejděte na kartu *Details*, kde potřebné adresy najdete. Z dalších údajů budete muset určitě vložit jméno uživatele a heslo a všimněte si také, že celou konfiguraci lze pro usnadnění uložit a umístit jako pojmenovaného zástupce třeba na pracovní plochu.

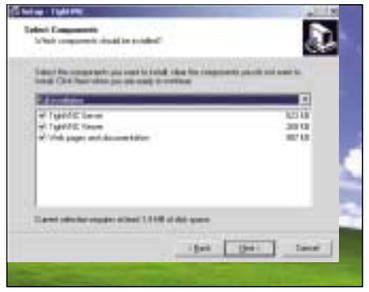
Tímto jsme vyřešili problém na straně klienta, ovšem zbývá nám serverová strana. Je-li vzdálený počítač vybaven Windows XP, je cesta opět poměrně snadná. K dispozici je totiž zmíněný zabudovaný terminálový server s názvem Remote Desktop (Vzdálená plocha) a stačí jej tedy pouze rozeběhnout a nastavit. K tomu přejděte na vzdáleném počítači na ikonu *Tento počítač* a pomocí pravého tlačítka myši vyberte volbu *Vlastnosti/Properties*. Na kartě *Remote/Vzdálený přístup* pak přejděte do spodní poloviny, kde je potřeba server povolit zatržením jediné položky. Pokračujte pomocí tlačítka *Vybrat vzdálené uživatele* a do otevřeného okna poté přidejte seznam uživatelských účtů, jimž chcete použití vzdálené plochy povolit. Pozor, je potřeba to opravdu udělat – to, že jste dříve někomu povolili sestavení a příjem VPN spojení, ještě neznamená, že má povolenu funkci Vzdálené plochy!

Ačkoliv je výše popsané řešení dostupné a elegantní, chybí mu některé možnosti. Klient sice funguje prakticky na všech Windows od verze 95, ale server je jenom ve Windows XP, což je problém. Dále vám může chybět interaktivní spolupráce s uživatelem, jenž na vzdáleném počítači pracuje – Remote Desktop pracuje výlučně, takže buď jste připojeni lokálně, nebo vzdáleně. Jinak jde o velmi dobré řešení.

VNC a TightVNC

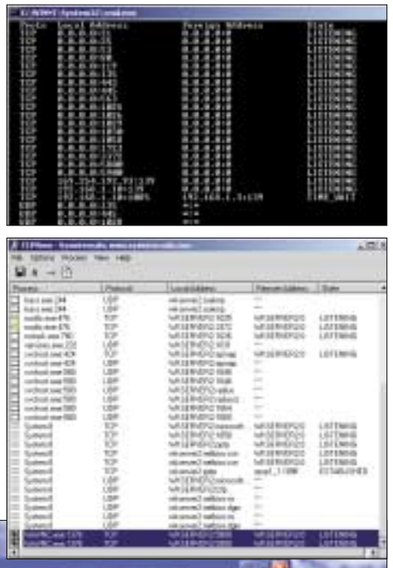
Abychom se vyhnuli některým omezením předchozího řešení, sáhneme po osvědčeném a prověřeném softwaru. Produkty s výše uvedenými názvy se vyznačují tím, že dostatečná kvalita se zde spojuje s příjemnou cenou – vše je zdarma. Přesto jde o velmi populární a dobře propracovaný způsob, jak vzdáleně přistoupit k počítači.

Pro praktické nasazení použijeme variantu TightVNC, jež představuje mírně vylepšenou a průběžně udržovanou variantu původního VNC a jejíž instalaci najdete na NA NAŠEM CD či na internetových stránkách *www.tightvnc.com*. Pro umístění serverové části jsme si vybrali úmyslně Windows 2000 Professional, jež jednoduchým terminálovým serverem nedisponují. Po spuštění instalačního souboru nejdříve musíte provést výběr z komponent – na straně serveru samozřejmě postačí nainstalovat odpovídající část, případně též dokumentaci. Dalším krokem při instalaci je volba, zda se TightVNC server bude chovat jako služba systému Windows. Je to výhodná volba, neboť pak poběží „na pozadí" a nebude se muset starat o její ruční spouštění. Zvolíte-li též automatický start pomocí dalšího zatržítka, dojde po dokončení instalace k bezprostřednímu spuštění a „vyskočí" na vás okno, že nemáte nastaveno přístupové heslo, přičemž konfigurační rozhraní se otevře vzápětí. O tom, že služba opravdu běží a naslouchá na síti, se můžete přesvědčit několika způsoby. Zkuste třeba spustit příkazovou řádku a zadejte příkaz *NETSTAT -an*, kde ve výpisu ve druhém sloupci zjistíte, že „cosi" naslouchá (Listening) na portu 5800 a 5900. Ke stejné kontrole můžete použít kupříkladu nástroj TCPView, který najdete na NA NAŠEM CD nebo na stránkách *www.sysinternals.com/ntw2k/source/tcpview.shtml*. Vyznačuje se pěkným grafickým rozhraním a navíc vám ukáže i běžící službu včetně ikony.



Je-li v provozu server na vzdáleném počítači, můžeme přistoupit ke konfiguraci klientské části. Ze stejného instalačního souboru, jenž byl už jednou použit, můžete tentokrát nainstalovat klientský prohlížeč. Po spuštění této aplikace stačí pouze zadat cílovou IP adresu, případně též číslo portu (je-li výchozí, nemusíte to dělat). V následujícím dialogu budete požádáni o heslo. Poté již uvidíte v okně vzdálenou plochu systému a můžete začít inspekci či akci.

TightVNC nabízí řadu zajímavých možností. Bližším průzkumem zjistíte, že lze pomocí dvou hesel odlišit, zda při vzdáleném přístupu pouze nakukujete nebo můžete s plochou pracovat. Z této informace snadno odvodíte, že aktivní může být zároveň lokální uživatel na vzdáleném počítači i vy jako klient VNC, a to zároveň a na téže ploše, což se může hodit. Lze rovněž definovat chování při odpojení vzdáleného klienta, takže vzdálený počítač se může z bezpečnostních důvodů zamknout. Navíc může probíhat více vzdálených relací zároveň a některé z vás třeba potěší, že není ani potřeba spouštět klientskou aplikaci, neboť její úkol dokáže obstarat speciální aplet v jazyce JAVA, spuštěný ve webovém prohlížeči.



Závěrem

Pokud jsme vás v předchozích odstavcích přesvědčili, že používat vzdálené připojení a ovládání počítače není zase až tak obtížné, jsme tomu velmi rádi. A pokud máte po prvním přečtení pocit, že to není úplně prosté, nebojte se začíst ještě jednou a více experimentovat, neboť úspěchy se jistě dostaví. V každém případě věřte, že práce se vzdálenou plochou je dnes samozřejmostí a příslušné aplikace patří k běžné výbavě. 5 0118/OK ❑