LAN SUITE 2003

Manuál

Jeden server pro E-mail, Fax, Web, Proxy

s Firewallem a Antivirem

Srpen 2003

Obsah

Co je LAN SUITE?

LAN SUITE je bezpečný komunikační server určený pro operační systém Windows 98/ME/NT/2000/XP. Jednoduchá instalace a údržba předurčuje LAN SUITE jako ideální řešení pro střední a malé firmy.

Vestavěný SMTP/POP3 server díky integrované podpoře antivirového systému BitDefender™ (pouze v LAN SUITE Antivirus Edition) a anti-spam filtru zajišťuje bezpečnou a efektivní komunikaci elektronickou poštou. LAN SUITE navíc oproti obdobným systémům zajišťuje i příjem a odesílání faxů, a to i po ISDN.

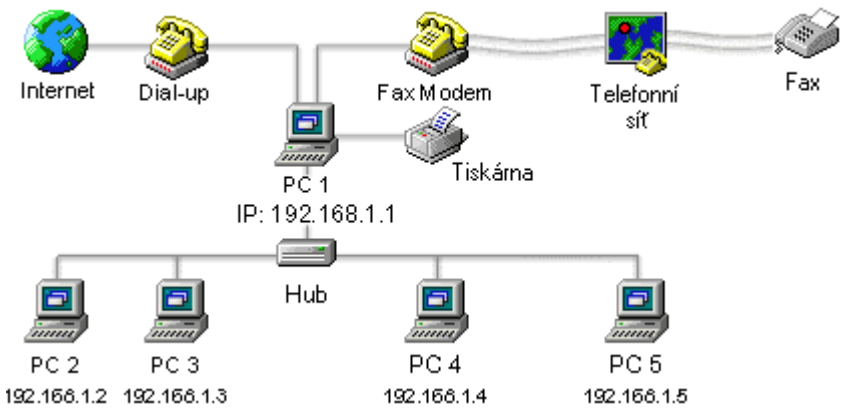
Svou poštu a faxy si mohou uživatelé číst nejen libovolným klientským programem podporujícím protokol POP3 (např. Outlook Express), ale díky webovému přístupu i browserem (např. Internet Explorer) odkudkoli z internetu nebo mobilního telefonu (WAP).

Samozřejmostí je sdílený přístup k internetu pro celou síť zabezpečený firewallem. Administrátor navíc může omezit přístup jednotlivých uživatelů na určité servery, a zvýšit tak efektivitu jejich práce s internetem.

Veškerou správu a konfiguraci LAN SUITE lze snadno provádět pomocí browseru (i přes internet). Instalace LAN SUITE nevyžaduje žádné speciální znalosti - je stejně jednoduchá jako instalace připojení k internetu na jednu stanici. Pomocí průvodce konfigurací nakonfigurujete LAN SUITE do 10 minut!

Jak LAN SUITE funguje?

Na následujícím schématu je znázorněna počítačová síť, která je připojena k internetu pomocí vytáčeného připojení (dial-up). LAN SUITE je provozována na počítači označeném PC1. Místo dial-up připojení může samozřejmě být i ISDN připojení nebo pevná linka apod.



Připojení k internetu i faxování může být realizováno i přes jediný modem. V tom případě jsou ale faxy odesílány a přijímány, pouze pokud není navázáno připojení k internetu. Optimálním řešením je použít dva modemy. Přijaté faxy jsou doručovány elektronicky, ale mohou být i automaticky tisknuty na tiskárně.

Nastavení protokolu TCP/IP

Pro provoz LAN SUITE je nutné mít v síti správně nakonfigurovaný protokol TCP/IP. Tento protokol se konfiguruje odlišně na počítači s LAN SUITE (serveru) a na ostatních počítačích v síti (stanicích např. s Internet Explorerem a Outlookem Express).

Pokud tento protokol není na počítačích nainstalován, je třeba ho tam přidat. To lze ve většině Windows učinit v nastavení sítě, které je dostupná tlačítkem Start a volbami Nastavení – Ovládací panely – Síť.

Upozornění: Dále popisované nastavení se týká připojení k internetu pomocí modemu (dial-up). Stejné nastavení se také použije i v případě asynchronní pevné linky realizované pomocí dvou modemů.

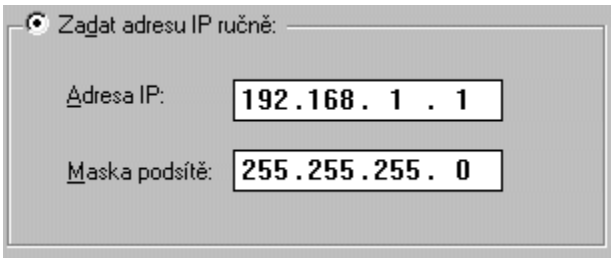
Nastavení TCP/IP na serveru

Konfiguraci protokolu TCP/IP na serveru lze rozdělit do dvou kroků. První se týká samotného připojení k internetu a zpravidla se provádí pomocí Telefonického připojení, které se nastaví podle údajů od poskytovatele připojení. Ve druhém kroku je třeba zajistit funkčnost TCP/IP spojení v rámci lokální sítě.

Následující konfiguraci TCP/IP proveďte POUZE u síťové karty, kterou je počítač připojen do lokální počítačové sítě (LAN). Nastavení se liší dle používaného operačního systému:

Windows 98

1) Start – Nastavení – Ovládací panely – Síť
2) Vyberte „TCP/IP ---> síťová karta“ a stiskněte Vlastnosti
3) Na záložce Adresa IP zvolte Zadat adresu IP ručně
4) Adresu IP zadejte 192.168.1.1 (doporučujeme)
5) Masku podsítě zadejte 255.255.255.0 (doporučujeme)
6) Potvrďte všechny dialogy OK a restartujte počítač.



Windows NT 4.0

1) Start – Nastavení – Ovládací panely – Síť
2) Vyberte záložku Protokoly
3) Klikněte na TCP/IP a zvolte Vlastnosti
4) Na záložce Adresa IP vyberte Zadat adresu IP ručně
5) Adresu IP zadejte 192.168.1.1 (doporučujeme)
6) Masku podsítě zadejte 255.255.255.0 (doporučujeme)
7) Potvrďte všechny dialogy OK a restartujte počítač.

Windows 2000/XP

1) Start – Nastavení – Síťová a telefonická připojení
2) Klikněte pravým tlačítkem na připojení, které chcete modifikovat a vyberte Vlastnosti
3) Vyberte Protokol sítě Internet (TCP/IP) a Vlastnosti
4) Vyberte Použít následující adresu IP
5) Adresu IP zadejte 192.168.1.1 (doporučujeme)
6) Masku podsítě zadejte 255.255.255.0 (doporučujeme)
7) Potvrďte všechny dialogy OK a restartujte počítač.

Nastavení TCP/IP na stanicích v síti

Protokol TCP/IP lze na stanicích nakonfigurovat obdobně jako na serveru. Je ale nutné dodržet pravidlo, že každý počítač musí mít jinou IP adresu. Doporučujeme zvyšovat postupně poslední číslo v adrese – např. 192.168.1.2, 192.168.1.3 atd. Maska podsítě je pro všechny počítače stejná, a to 255.255.255.0.

Pro některé aplikace (např. využívající služeb SOCKS serveru) je rovněž nutné zadat adresu DNS serveru. Jako adresu DNS serveru zadejte IP adresu počítače s LAN SUITE (např. 192.168.1.1).

Kontrola funkčnosti protokolu TCP/IP

Po provedení konfigurace protokolu TCP/IP na serveru i na stanicích je vhodné zkontrolovat, zda vše funguje tak, jak má. Server i stanice musí být zapnuté.

Kontrola funkčnosti protokolu TCP/IP spočívá v provedení příkazu **ping** z různých stanic na server (a naopak). Spusťte z Windows na stanici **Příkazový řádek** a zadejte např. příkaz:

ping 192.168.1.1 (pokud je 192.168.1.1 IP adresa počítače s LAN SUITE)

Musíte dostat odpověď podobnou následující:

Odpověď od 192.168.1.1: bajty=32 čas<10ms TTL=128 – vše je v pořádku.

Pokud dostanete odpověď typu ***Vypršel časový limit žádosti.***, protokol TCP/IP není správně nakonfigurován!

Instalace LAN SUITE

LAN SUITE je vhodné instalovat na počítač s faxmodemem (či obdobným zařízením), připojený k internetu, který splňuje příslušné systémové požadavky.

1) Spusťte instalaci LAN SUITE (ze staženého souboru nebo z CD).
2) Postupujte podle pokynů průvodce a po zadání jména a společnosti zvolte cílový adresář a složku pro ikony.
3) Po potvrzení vyčkejte na dokončení instalace.

Základní okno programu

V okně spuštěného programu můžete sledovat činnost LAN SUITE, spravovat frontu zásilek, manuálně navazovat dial-up připojení a vybírat POP3 schránky.

Pozn. Při prvním spuštění LAN SUITE se automaticky spustí **Průvodce konfigurací**, který Vás provede úskalími základní konfigurace LAN SUITE. Čtěte pozorně všechny instrukce.

Manuální řízení navazování dial-up připojení

Telefonní spojení (dial-up) do internetu si standardně ovládá server automaticky podle nastavení na záložce **Připojení**. Pokud chcete řídit spojení ručně, můžete použít příkaz **Navazování telefonního spojení** z menu **Server**. Pak můžete nastavit volbu na **manuální** a tlačítkem **Spojení navázat** ručně navázat připojení k internetu.

Upozornění! V manuálním režimu server nijak nekontroluje délku a využití spojení (je ignorováno veškeré nastavení na kartě **Připojení**). Je tedy zcela na odpovědnosti uživatele, aby navázané spojení opět ukončil, případně volič přepnul zpět na automatický provoz.

Pozn. Pokud je volba typu spojení v poloze **automatické** a uživatel vydá tlačítkem povel, který je v rozporu s nastavením na kartě **Připojení**, volič se automaticky přepne do polohy **manuální**.

Nastavení voliče do polohy **manuální** se neukládá, po startu programu je volič vždy v poloze **automatické**.

Výběr POP3 schránek a odeslání e-mailů

Pomocí příkazu **Výběr POP3 a odeslání internetových zásilek** z menu **Server** přinutíte LAN SUITE okamžitě stáhnout z internetu obsah POP3 schránek definovaných na záložce **POP3** a odeslat e-maily čekající na odeslání. Lze použít i klávesovou zkratku **Ctrl+F10**.

Přerušení přenosu faxu

Příkaz **Přerušení přenosu faxu** (nebo **Ctrl+C**) přeruší probíhající odesílání faxu.

Statistika

Příkaz **Statistika** otevře okno, ve kterém se zobrazí statistické údaje o všech aktivitách serveru (odeslaných zásilkách, stránkách atd.).

Přehled odeslaných faxů

Příkaz **Přehled odeslaných faxů** otevře okno s výpisem informací o odeslaných faxech (kdo byl odesílatel, kdo adresát, kdy a na kolik pokusů).

Výpis aktivních spojení

Příkaz **Výpis aktivních spojení** nebo klávesový povel **Ctrl+F7** vypíše seznam všech aktuálně navázaných spojení. Seznam je zobrazen jako součást logu zobrazeného v pracovním okně.

Deaktivace/Aktivace zpracování front

Tento příkaz deaktivuje/aktivuje zpracování front. LAN SUITE stále přijímá zásilky, ukládá je do fronty, ale nedoručuje/doručuje je na určené místo (lokálním uživatelům nebo do internetu).

Deaktivace/Aktivace POP3 výběrů

Tento příkaz deaktivuje/aktivuje vybírání POP3 schránek definovaných na záložce **POP3**.

Správa fronty zásilek

Příkazem **Fronta zásilek** otevřete okno s přehledem zpráv (e-mailů a faxů), které se mají odeslat. Pod přehledem je skupina ovládacích tlačítek:

- Tlačítko **Odložit** – dočasně vyřadí označenou zprávu z dalšího zpracování, tj. LAN SUITE se ji nebude pokoušet odeslat.
- Tlačítko **Oživit** – zařadí zprávu, jejíž odeslání bylo předtím potlačeno, zpět do fronty k odeslání.
- Tlačítko **Vymazat** – vymaže označenou zprávu z fronty.
- Zobrazený obsah fronty lze obnovit pomocí tlačítka **Obnovit seznam**.

Pozn. Právě odesílané zásilky nejde ani odložit ani vymazat.

Konfigurace LAN SUITE

Konfiguraci LAN SUITE je možno provádět v zásadě dvěma způsoby:

- pomocí **Průvodce konfigurací** (krok za krokem),
- prostřednictvím **Konfigurace pro odborníky** (všechna nastavení na záložkách v jednom konfiguračním okně). Ta je v graficky jiné podobě dostupná i vzdáleně pomocí browseru.

Průvodce konfigurací

Při prvním spuštění LAN SUITE se automaticky spustí **Průvodce konfigurací**, který Vás provede úskalími základní konfigurace LAN SUITE. Čtěte pozorně všechny instrukce.

Průvodce konfigurací můžete kdykoliv spustit znovu z menu **Konfigurace – Průvodce konfigurací**.

Konfigurace pro odborníky

Okno s konfigurací pro odborníky, které je dostupné z menu **Konfigurace – Konfigurace pro odborníky**, se skládá z následujících záložek:

- **Uživatelé** – správa uživatelů a nastavení domény
- **Připojení** – volba způsobu připojení k internetu (dial-up/trvalé)

- **Firewall** – nastavení ochrany lokální sítě i počítače s LAN SUITE
- **SMTP** – nastavení parametrů (SSL) SMTP serveru
- **POP3** – definice pravidelně vybíraných POP3 schránek, nastavení (SSL) POP3 serveru
- **Anti-virus** – zapnutí a nastavení parametrů antivirové kontroly pošty
- **Fax –** nastavení odesílání a příjmu faxů
- **Proxy** – nastavení HTTP/FTP/SOCKS/Telnet a RealAudio proxy včetně autentifikace do proxy, povolení/zákazu přístupu přes proxy na zadané servery, mapovaných spojení a IP filtru
- **WWW** – konfigurace (SSL) WWW serveru, FastCGI, mapovaných aplikací a adresářových aliasů
- **SSL –** konfigurace SSL, generování žádostí a certifikátů (pro SSL SMTP/POP3/WWW server)
- **DHCP –** *Dynamic Host Configuration Protocol* umožňuje automatickou konfiguraci protokolu TCP/IP na stanicích v síti
- **LDAP -** *Lightweight Directory Access Protocol* slouží ke sdílení seznamu uživatelů LAN SUITE
- **Administrace –** konfigurace vzdálené správy pomocí browseru
- **Zprávy –** definice činností zaznamenávaných do log souborů
- **NT služba** (Win95/98/Me služba) – instalace LAN SUITE jako NT služby pro automatické spouštění po startu Windows

Parametry příkazové řádky

LAN SUITE lze spustit s následujícími parametry na příkazové řádce:

- **/CONFIG** – po spuštění LAN SUITE s tímto parametrem přejdete ihned do konfigurace pro odborníky. Po uložení konfigurace se LAN SUITE ukončí (např. C:\LANSUITE\LANSUITE.EXE /CONFIG).
- **/DBG:R** – po přidání tohoto parametru bude LAN SUITE do logu vypisovat podrobná hlášení o SMTP/POP3 procesech.
- **/EXIT** – běžící LAN SUITE můžete ukončit z příkazového řádku jejím opětovným spuštěním s tímto parametrem.

Uživatelé

Tato záložka slouží pro správu uživatelů, jejich práv, schránek a souvisejících parametrů.

Nastavení implicitní domény

Jako **implicitní doménu** zadejte Vaši registrovanou doménu (např. firma.cz). Pokud nemáte vlastní doménu nebo chcete LAN SUITE využívat jen pro faxování, nemusíte do tohoto pole nic zadávat.

Přidání nového uživatele

Po stisku tlačítka **Přidat** se zobrazí dialog pro založení nového uživatele. Pro každého uživatele můžete nadefinovat následující parametry:

- **Jméno uživatele** – unikátní jméno uživatele (název jeho schránky). E-mailová adresa uživatele je pak tvořena z jeho jména a implicitní domény (např. jmeno@firma.cz). Pokud potřebuje daný uživatel odesílat e-maily i pod jinou e-mailovou adresou, je třeba mu jí nadefinovat v řádku **Aliasy**.
- **Heslo** – v heslu se nerozlišuje velikost písmen a není povolena diakritika.
- **Plné jméno** – slouží pro snadnější identifikaci uživatele (např. v seznamech).
- **Aliasy** – každý uživatel může mít současně několik e-mailových adres (aliasů). Pokud je jméno uživatele např. novak, může mít aliasy třeba: petr, obchod. V tom případě je mu možné posílat e-maily na následující adresy:

  novak@firma.cz, petr@firma.cz a obchod@firma.cz

  Jako alias lze zadat i celou e-mailovou adresu např. novak@seznam.cz. To umožní danému uživateli odesílat poštu skrz LAN SUITE i s touto adresou odesílatele (pokud si patřičně nastaví svůj klientský program).

  Pokud má více uživatelů stejný alias (např. obchod), jsou e-maily zaslané na adresu obchod@firma.cz doručovány všem těmto uživatelům.
- **Doručujte tomuto uživateli faxy došlé na číslo (pouze CAPI)** – faxy došlé na zadané telefonní číslo budou doručovány přímo danému uživateli. Tato funkce je možná pouze po příjmu faxu CAPI (ISDN) zařízením, protože pouze v této situaci LAN SUITE zná číslo, na které fax došel.
- **Doručujte tomuto uživateli faxy s následujícími id. řetězci** – všechny příchozí faxy s identifikačním řetězcem odpovídajícím některému ze zadaných budou doručeny tomuto uživateli. Pro snadnější zadávání můžete použít tlačítka **Přidat**

fax. id řetězec ze seznamu přijatých faxů, které zobrazí id. řetězce všech v minulosti přijatých faxů.

- **Limit velikosti schránky** – omezuje maximální velikost schránky.

Práva uživatele

Práva uživatele se nastavují pomocí zaškrtávacích políček. Jejich význam je následující:

- **Uživatel je administrátor** – uživatel má právo spravovat LAN SUITE (lokálně i přes browser)
- **Uživatel smí posílat faxové zásilky** – uživatel má právo odesílat faxy
- **Uživatel smí používat proxy** – má význam pouze v případě, že je na záložce **Proxy** zaškrtnuta volba **Autentifikace požadována**. Pak se při použití browseru objeví přihlašovací okno, do kterého musí uživatel zadat své uživatelské jméno a heslo. Přístup do internetu mu bude povolen pouze tehdy, pokud má toto právo.
- **Uživatel smí posílat zásilky do internetu** – pokud toto právo uživatel nemá, může posílat zásilky pouze lokálně (v rámci LAN SUITE) a nikoliv i do internetu.
- **Uživateli se budou doručovat neroztříděné faxy** – faxy, které nemohou být doručeny konkrétnímu uživateli podle jejich id. řetězce, budou doručeny všem uživatelům s tímto oprávněním. (Pokud toto oprávnění nemá žádný uživatel, budou neroztříděné faxy doručovány všem uživatelům.)
- **Uživateli se budou doručovat neroztříděné zásilky** – e-maily stažené z POP3 schránky, které nemohou být doručeny konkrétnímu uživateli, budou doručeny všem uživatelům s tímto oprávněním. (Pokud toto oprávnění nemá žádný uživatel, budou neroztříděné zásilky doručovány všem uživatelům.)
- **Zahrnout uživatele do seznamu pro LDAP adresář** – uživatel s tímto oprávněním bude obsažen v LAN SUITE LDAP adresáři.

Smazání uživatele

Označte uživatele, kterého chcete odstranit, kliknutím na jeho jméno a stiskněte tlačítko **Vymazat**. Po potvrzení výmazu budete moci vymazat i celý obsah jeho schránky.

Změna vlastností uživatele

Pokud potřebujete upravit některou z vlastností uživatele nebo potřebujete změnit jeho práva, označte uživatele kliknutím na jeho jméno a stiskněte tlačítko **Vlastnosti**.

Import

Nové uživatele nemusíte zakládat pouze ručně, můžete je také naimportovat pomocí tlačítka **Import**. Po stisku tohoto tlačítka máte na výběr ze dvou možností:

- Importovat uživatele z textového souboru (CSV)
- Importovat uživatele Windows NT/2000/XP

Importovat uživatele z textového souboru (CSV)

Nejprve vyhledejte soubor, ze kterého budete chtít uživatele naimportovat. Před zahájením importu budete mít možnost vybrat a přiřadit, která textová pole uvedená v CSV souboru se budou importovat a jakým vlastnostem zakládaných uživatelů se načtené hodnoty přiřadí. Pomocí importu lze založit uživatele včetně všech jeho parametrů. Importovat lze následující hodnoty: Uživatelské jméno; Plné jméno; Aliasy; Uživatelská práva; Faxové identifikační řetězce; Limit velikosti schránky.

Uživatelská práva lze do CSV souboru promítnout pomocí hexadecimálních čísel. Různé kombinace uvedených práv docílíte výpočtem pomocí logického operátoru OR:

- 0000307D - uživatel je administrátor
- 00001074 - uživatel smí posílat faxové zásilky
- 0000105C - uživatel smí používat proxy
- 00003054 - uživatel smí posílat zásilky do internetu
- 00009054 - uživateli se budou doručovat neroztříděné faxy
- 000010D4 - uživateli se budou doručovat neroztříděné zásilky
- 80001054 - zahrnout uživatele do seznamu pro LDAP adresář

Příklady:

- 8000B0FD - uživatel je administrátor, budou se mu doručovat neroztříděné faxy i zásilky a bude zahrnut v seznamu pro LDAP adresář (maximální práva)
- 8000307C - uživatel smí posílat faxové zásilky, používat proxy, posílat zásilky do internetu a bude zahrnut v seznamu pro LDAP adresář (standardní práva)

Není ale třeba importovat uživatele ze souboru obsahujícího všechny možné hodnoty. V nejjednodušším případě stačí, aby soubor obsahoval sloupec s uživatelskými jmény. Novým uživatelům jsou pak nastavena standardní práva a ostatní vlastnosti nemají nadefinovány.

V průběhu importu budete postupně dotazováni na heslo pro právě zakládaného uživatele. Je možné zadávat hesla jednotlivě nebo v určité fázi importu zaškrtnout volbu **Použít toto heslo pro zbývající importované uživatele**.

Importovat uživatele Windows NT/2000/XP

Tato volba otevře okno se seznamem uživatelů definovaných **na tomto** počítači. Pro tuto funkci musí být LAN SUITE spuštěna na počítači s Windows NT/2000/XP.

V průběhu importu budete postupně dotazováni na heslo pro právě zakládaného uživatele. Je možné zadávat hesla jednotlivě nebo v určité fázi importu zaškrtnout volbu **Použít toto heslo pro zbývající importované uživatele**.

Uživatele nelze importovat z jiného počítače/serveru.

Export

Seznam uživatelů LAN SUITE můžete pomocí tlačítka **Export** uložit do CSV souboru. Před provedením exportu budete mít možnost zvolit, jaké vlastnosti uživatelů budou do souboru exportovány.

Exportovat lze následující hodnoty: Uživatelské jméno; Plné jméno; E-mail; Aliasy; Uživatelská práva; Faxové identifikační řetězce; Limit velikosti schránky.

Smazat zásilky čekající na doručení do plných schránek po X dnech

LAN SUITE umožňuje administrátorovi nastavit každému uživateli v jeho vlastnostech **Limit velikosti schránky**. Pokud e-mailem staženým z POP3 schránky nebo příchozím faxem uživatel překročí tento limit, jsou tyto zásilky uloženy do dočasného adresáře a uživateli je zaslána zpráva, že překročil nastavený limit velikosti schránky (Y MB).

Pokud uživatel včas neuvolní svojí schránku, **jsou čekající zásilky z dočasného adresáře po X dnech vymazány**.

Zásilky přicházející protokolem SMTP jsou při překročení limitu automaticky odmítány.

Vytvoření seznamu uživatelských stránek

Pro zjednodušení přístupu k HTML stránkám uživatelů v LAN SUITE, je možné vygenerovat stránku s jejich seznamem pomocí tlačítka **Vytvořit seznam uživ. stránek**.

Po stisku tlačítka máte možnost vybrat uživatele, jejichž stránky mají být zahrnuty do seznamu, a šablonu pro generování seznamu (standardně \users.tpl\users.htm).

Po potvrzení tlačítkem OK je seznam vygenerován v **Hlavním adresáři WWW serveru** (nastaveném na kartě WWW) a pojmenován **users.htm**. Seznam uživatelských stránek je pak dostupný na adrese http://server/users.

Šablonu pro generování seznamu uživatelských stránek (\users.tpl\users.htm) lze modifikovat při dodržení následujících podmínek:

- Šablona musí obsahovat „uživatelskou“ sekci začínající

  <!--TextToChangeStartUserLine-->

  a končící

  <!--TextToChangeEndUserLine-->

- Tato sekce musí obsahovat klíčová slova **UserName** a **UserDir**. LAN SUITE při generování nahradí tato klíčová slova jménem uživatele a odkazem na jeho HTML stránku.

  Např.: UserName

Když LAN SUITE generuje seznam uživatelských stránek, kopíruje také obsah adresáře se šablonou do **Hlavního adresáře WWW serveru**. Proto doporučujeme umístit modifikovanou šablonu ve zvláštním adresáři spolu s nutnými obrázky atd., aby nedocházelo ke kopírování zbytečných souborů.

Připojení

Na této záložce se nastavuje způsob, podmínky a frekvence navazování připojení k internetu.

Druh připojení

V této sekci nastavte, jak je LAN SUITE připojena k internetu. V principu jsou dvě možnosti:

- **Trvalé připojení** – tuto volbu použijte, nejen pokud je LAN SUITE připojena k internetu pevnou linkou, ale i pokud je připojena např. přes jiný počítač. Tato volba de facto znamená, že se LAN SUITE nebude o připojení starat a bude předpokládat, že je stále připojena.
- **Dial-up připojení** – pokud se k internetu připojujete vytáčenou linkou (pomocí analogového modemu, ISDN apod.) a chcete, aby LAN SUITE navazovala a ukončovala připojení, zvolte tuto možnost. Nezapomeňte pak nastavit parametry v sekci **Kdy navazovat dial-up spojení**.

Parametry dial-up připojení

Z nabídky **Jméno připojení** vyberte název telefonického připojení, které chcete používat (LAN SUITE přebírá všechny parametry daného připojení z Windows, neboli připojení musíte vytvořit nejprve ve Windows). Dále vyplňte položky **Uživatel** a **Heslo** (přihlašovací jméno a heslo pro připojení).

Sekundární připojení (VPN)

Tlačítkem **Po připojení** se otevře pomocný dialog. Jeho hlavní část tvoří sekce **Navázat sekundární připojení (připojení VPN)**. VPN (Virtual Private Network) je způsob, jak vytvořit pomocí technologie tunelování, případně šifrování a autentifikace, privátní spojení po veřejném médiu. Je tedy třeba vytvořit spojení pomocí VPN adaptéru ve Windows (konfiguruje se v Ovládacích panelech) na VPN bránu, která je na serveru této služby. Pokud se k internetu připojujete vytáčeným napojením pomocí modemu, je třeba provést vytáčení dvojí: jednou standardně modemem a po jeho navázání ještě “vytáčení" VPN adaptérem. Dialog určený ke konfiguraci tohoto druhého (sekundárního) připojení k VPN je přístupný až po nakonfigurování standardního vytáčení.

Pomocný dialog **Po připojení** navíc zatržením volby **Spustit ONCONN.BAT** umožňuje zvolit, zda se po navázání spojení má spustit soubor ONCONN.BAT (musí být umístěn v adresáři s LAN SUITE). V něm lze např. popsat úpravy routovací tabulky nebo jakékoliv jiné akce přístupné z dávkového souboru.

Kdy navazovat dial-up spojení

Připojit se trvale

Přepínačem **Trvale připojit** zajistíte trvalé napojení serveru k internetu. Zároveň se zpřístupní tlačítko **Časové omezení trvalého připojení**, které otevře tabulku umožňující stanovit týdenní rozvrh povolení nebo zákazu trvalého napojení. Tabulka je týdenní a je dělena po půlhodinách. Zelené políčko znamená, že spojení bude povoleno, červené políčko v danou půlhodinu spojení zakazuje.

Připojovat se periodicky

Přepínač **Připojovat každých** zaškrtněte, chcete-li se k internetu připojovat periodicky – pravidelně po určitých časových úsecích. Periodu v minutách zapište do pole vpravo od přepínače; nejkratší dobu spojení do pole **na X min**.

Při požadavku na periodické spojení se zpřístupní tlačítko **Časové omezení period. připojování**, které otevře tabulku umožňující stanovit týdenní rozvrh povolení napojení.

Připojovat se při požadavku na proxy

Pokud chcete, aby LAN SUITE navázala dial-up připojení při požadavku klientské stanice na proxy, SOCKS nebo DNS, zaškrtněte volbu **Při požadavku klienta na proxy**. Do pole **Rozpojit po X minutách bez požadavku** zadejte údaj v minutách, po kterých bude spojení ukončeno, nebude-li vznesen žádný další požadavek.

Tlačítko **Časové omezení připojení na požadavek** otevře tabulku týdenního rozvrhu navazování připojení při požadavku na proxy.

Připojovat se při zásilkách čekajících ve frontě

Připojení se naváže, čeká-li na odeslání:

- minimálně počet zásilek specifikovaný v poli **Čeká-li na odeslání nejméně X zásilek** nebo
- čeká-li i menší počet zásilek déle než stanovený počet minut. Tento časový údaj zapište do pole nebo **déle než X minut**.

Tlačítkem **Časové omezení připojení podle zásilek** otevřete tabulku pro týdenní rozvrh omezení připojování podle požadavků na práci se zásilkami.

Připojovat se při požadavku na výběr POP3 schránky

Připojení se naváže, pokud uplynul nastavený časový interval od minulého výběru některé POP3 schránky podle specifikace v kartě **POP3** a je tedy třeba provést nový výběr.

Tlačítkem **Časové omezení připojení pro POP3 výběry** otevřete tabulku pro týdenní rozvrh omezení připojování při POP3 výběru.

Kdy se má uvolnit TAPI zařízení pro odesílání faxů

Pokud je nastaveno stejné TAPI zařízení (obvykle stejný modem) pro připojování na internet i pro odesílání faxů, je možné nastavit za jakých okolností se má ukončit spojení na internet a tím umožnit odeslání faxů čekajících ve výstupní frontě.

TAPI zařízení se pro faxování uvolní:

- Ihned, pokud se ve výstupní frontě nahromadí nejméně tolik faxových zásilek, kolik uvedete do pole **Uvolnit TAPI zařízení, čeká-li na odeslání nejméně X fax. zásilek**.

- Po uplynutí časového intervalu uvedeného ve vstupním poli **…nebo déle než X minut**, i když je ve frontě menší počet zásilek (ale alespoň jedna).

Pokud dial-up a faxová část nepoužívají stejné TAPI zařízení (stejný faxmodem), je tato volba na konfigurační kartě neaktivní.

Firewall

Firewall chrání počítač s LAN SUITE a celou lokální síť před neoprávněnými spojeními a průniky. Firewall je přístupný a jeho funkcí lze využívat, pouze pokud je LAN SUITE provozována na Windows 2000/2003 a XP.

Charakteristika firewallu

Firewall chrání počítač s LAN SUITE a celou lokální síť před neoprávněnými spojeními. **Firewall je přístupný, pouze pokud je LAN SUITE provozována na Windows 2000/2003 a XP.** Konfigurace firewallu předpokládá existenci alespoň dvou síťových rozhraní:

- vnějšího pro připojení k internetu (modem, síťová karta k routeru apod.) a
- vnitřního pro připojení lokální sítě (obvykle síťová karta).

Firewall pracuje na principu paketového filtru a nastavuje se pomocí sad povolení spojení na jednotlivých síťových rozhraních. **Pokud tedy není nějaké spojení v nastavení firewallu explicitně povoleno, je zakázáno.**

Upozornění

Nevhodným nastavením pravidel práce firewallu lze znepřístupnit ostatní komunikační služby programu LAN SUITE nebo jiné síťové služby (např. sdílení)!

Konfigurace firewallu

Firewall se globálně zapíná či vypíná zaškrtnutím volby **Firewall**. I v případě, že je tato volba zaškrtnuta, je firewall aktivní pouze, pokud je spuštěna LAN SUITE (buď jako aplikace nebo jako služba).

Pro správnou funkci většiny sad povolení je nutné nejdříve definovat, které ze síťových rozhraní je lokální = určeno pro spojení s vnitřní sítí. Ostatní rozhraní se pak považují za spojení do internetu.

Při konfiguraci firewallu lze použít buď zjednodušené rozhraní a pomocí táhla nastavit určitou úroveň bezpečnosti (**Vysoká, Střední, Nízká**) nebo pravidla pro práci firewallu zadat

manuálně pomocí předdefinovaných a/nebo vlastních sad povolení (při úrovni bezpečnosti **Vlastní**).

Vlastnosti zmíněných bezpečnostních úrovní jsou popsány přímo v konfigurační kartě firewallu. Při vytváření vlastních sad povolení lze vytvářet vlastní povolení pomocí jednotlivých protokolů, směrů spojení, síťových rozhraní nebo IP adres a portů.

Nastavení vlastní úrovně bezpečnosti

Při nastavování vlastní úrovně bezpečnosti a zejména vlastních sad povolení je třeba vycházet z dobré znalosti vlastností IP spojení.

Při nastavení **Bezpečnosti** do polohy **Vlastní** se volí a upravují tzv. sady povolení. V pravé části karty je seznam aktuálních sad povolení. Tlačítky **Přidat sadu, Kopírovat sadu, Editovat sadu** a **Vymazat sadu** můžeme sady povolení přidávat, vytvářet jejich kopie pro další editaci, stávající sady editovat a sady mazat. Odškrtnutím čtverce u zvolené sady povolení je možné tuto sadu dočasně vyřadit z funkce.

Vlastní úroveň bezpečnosti obsahuje standardně po instalaci několik předdefinovaných sad povolení založených na střední úrovni bezpečnosti, které umožňují provoz a přístup k většině komunikačních služeb LAN SUITE jak z lokální sítě, tak z internetu. Pokud se kdykoli budete chtít vrátit k tomuto výchozímu nastavení, stiskněte tlačítko **Výchozí**.

Přidání sady povolení

Při přidávání sady povolení si můžeme vybrat, zda přidáváme sadu povolení předdefinovanou výrobcem (**Přidat vybrané předdefinované sady povolení**) nebo zda přidáme sadu vlastní (**Přidat novou sadu povolení**), kterou budeme dále editovat podle svých potřeb. Editovat lze i předdefinované sady, ale je třeba je následně ukládat pod novými názvy.

Předdefinované sady povolení lze přidávat i hromadně; k současnému označení více sad použijte levé tlačítko myši spolu s klávesou **Ctrl**.

Je třeba si uvědomit, že uživatelská pravidla jsou vždy povolující, tedy povolují další spojení, pokud tedy použijete jako základ své sady povolení některou sadu přednastavenou, budete stupeň bezpečnosti dalším přidáváním povolení vždy snižovat.

Příklad použití předdefinovaných sad povolení

Pokud chcete použít nastavení prostřednictvím úrovní bezpečnosti, ale potřebujete k němu přidat další povolení (např. povolit SMTP příjem při středním stupni bezpečnosti),

zvolte úroveň bezpečnosti **Vlastní**, přidejte přednastavenou sadu povolení pro zvolenou úroveň bezpečnosti a k ní přidejte další sadu(y) povolení podle aktuální potřeby. Např.:

- Povolení pro střední úroveň bezpečnosti,
- Povolení SMTP spojení z internetu na tento počítač.

Přidání nové (vlastní) sady povolení

Pokud při přidávání sady povolení zvolíte **Přidat novou sadu povolení**, otevře se Vám prázdné okno pro editaci sady povolení. **Jméno sady povolení** slouží k přehlednému pojmenování vytvářené sady a bude se následně zobrazovat v přehledu sad povolení.

Sadu povolení naplníte prostřednictvím tlačítek **Přidat, Editovat** a **Vymazat**, kterými přidáváte nebo modifikujete jednotlivá povolení obsažená v sadě.

Přidání / editace povolení

Konkrétní povolení přidáváme tlačítky **Přidat** nebo **Editovat** vždy do právě editované sady, která je určena svým jménem. Povolení se může týkat všech typů IP paketů nebo je možno zvolit z nabídky **IP protokol** určitý typ paketů: TCP, UDP, ICMP nebo „jiný“ (určený číslem protokolu). V závislosti na zvoleném protokolu je možné nastavit ještě další vlastnosti tohoto povolení: buď čísla povolených portů a druh paketu (pro TCP a UDP) nebo typ zpráv (pro ICMP).

Dále lze zvolit **Směr** paketů, a pokud definujete povolení pro určité konkrétní rozhraní (např. síťovou kartu), pak lze nastavit i další parametry:

- **Zdroj** – Jako zdroj lze nastavit libovolnou IP adresu s vyloučením konkrétních adres (tlačítkem **…**), jednotlivou IP adresu, IP adresu definovanou adresou a maskou podsítě, IP adresu z rozsahu určeného počáteční a koncovou IP adresou.
- **Cíl** – možnosti určení cíle jsou analogické s definicí **Zdroje**.

SMTP

Záložka SMTP slouží k nastavení odesílání zásilek pomocí SMTP protokolu. Pro příjem zásilek protokolem SMTP je třeba odpovídající dohoda s poskytovatelem připojení.

Příjem zásilek protokolem SMTP

SMTP protokol předpokládá, že daný SMTP server, na který doručuje zásilky, je vždy dostupný (tzn. je spuštěn a připojen k internetu). Jestliže nemáte trvalé připojení k internetu (např. používáte dial-up připojení), existují dvě možnosti řešení:

- Váš poskytovatel připojení může podporovat tzv. SMTP spooling – pokud není Váš SMTP server dostupný, může Váš poskytovatel dočasně uložit zásilky do fronty.
- Váš poskytovatel připojení nepodporuje SMTP spooling – zásilky jsou ukládány do POP3 schránky (zpravidla doménového koše), který Vám poskytovatel zřídil.

Nastavení protokolu SMTP

SMTP server můžete zapnout/vypnout zaškrtnutím stejnojmenné volby. Dále můžete specifikovat TCP/IP rozhraní, na kterém bude naslouchat. Standardně jsou zvolena **všechny,** ale můžete vybrat i konkrétní **IP adresu** ze seznamu. To může být vhodné jak z provozních, tak bezpečnostních důvodů (můžete specifikovat pouze vnitřní IP adresu, která umožní přístup k SMTP serveru pouze lokálním uživatelům).

LAN SUITE rovněž obsahuje i zabezpečený SSL SMTP server, který standardně pracuje na portu 2525.

Volba způsobu zpracování zásilek

Zásilky odesílat přes nadřízený SMTP server

Nejjednodušší způsob, jak odeslat zásilku do internetu, představuje přenesení problematiky vyhledání cíle pro zásilku a jejího doručení na jiný počítač v internetu, obvykle na SMTP server poskytovatele připojení. Stačí zaškrtnout volbu **Zásilky odesílat přes nadřízený SMTP server** a pro odesílání budete moci využívat externí počítač, který ví, kam poštu doručit. Musíte znát jeho adresu, buď v IP nebo symbolickém (doménovém) tvaru a zapsat ji do pole **Nadřízený SMTP server**.

Pozn. Možnost doručování přes nadřízený server doporučujeme využívat při dial-up napojení. Zásilky se maximální rychlostí přenesou k poskytovateli připojení, a teprve pak se vydají na „pomalou“ cestu internetem.

Přímé odesílání zásilek s využitím MX záznamů DNS

Pokud chcete zásilky odesílat přímo na cílové servery, můžete pro odesílání zásilek využít MX záznamy uložené v DNS, které mj. obsahují informace, kam se má pošta pro danou doménu doručovat. DNS požadavek posoudí a pokud přímo nenajde odpovídající MX záznam, postoupí jej „bližšímu“ DNS. To se opakuje, až je příslušný záznam nalezen a cílová adresa pro doručení sestavena.

Zkontrolujte, že **není** zatržena volba **Zásilky odesílat přes nadřízený SMTP server**, a klikněte na tlačítko **Nastavení odesílání pro odborníky** a vyplňte položky **DNS1** a **DNS2** (pokud existuje) podle údajů od poskytovatele připojení. Pokud tyto parametry nezadáte, LAN SUITE použije DNS zadané v konfiguraci protokolu TCP/IP ve Windows.

Pozn. Tento způsob doručování doporučujeme používat při trvalém připojení k internetu.

Vyžádání zásilek u nadřízeného SMTP serveru

Pokud SMTP server Vašeho poskytovatele podporuje tzv. SMTP spooling, můžete přijímat zásilky pomocí SMTP serveru, i když nemáte trvalé připojení k internetu.

Při příjmu zásilek vytáčenou linkou prostřednictvím SMTP může být po dohodě s poskytovatelem zapotřebí vyslat příkaz **ETRN** nebo **ATRN** k tomu, aby SMTP server poskytovatele začal vysílat zadržované zásilky pro „náš“ SMTP server.

V takovém případě po stisku tlačítka **Vyžádání zásilek u nadřízeného SMTP serveru** zaškrtněte přepínač **při navázání dial-up připojení**, zvolte jaký SMTP příkaz chcete pro vyžádání zásilek použít – **ETRN** nebo **ATRN** (včetně potřebných parametrů) a server specifikujte pomocí jeho adresy v poli **Nadřízený SMTP server** na kartě SMTP. LAN SUITE pak vyšle ETRN nebo ATRN příkaz při každém spuštění a při každém navázání dial-up připojení. Příkaz ETRN nebo ATRN lze také vysílat periodicky každých X minut.

SMTP RELAY

Funkce RELAY dovoluje SMTP serveru přijmout zásilku, jejíž adresát zde nemá schránku, a tuto zásilku je nutno odeslat dále jejímu adresátovi. Funkce je tedy nutná pro uživatele LAN SUITE, protože jejím prostřednictvím odesílají své zásilky z klientských SMTP/POP3 programů (např. Outlook Express) do LAN SUITE, který je po navázání dial-up napojení odešle do internetu.

Standardně je LAN SUITE nastavena tak, aby službu RELAY poskytovala pouze pro své uživatele (je zatržena volba **Služba SMTP RELAY pouze pro uživatele**). SMTP server pak testuje adresy odesílatelů; pokud odesílatel nemá v LAN SUITE účet (testuje se seznam uživatelských jmen včetně **aliasů** – viz Uživatelé), SMTP server požadovanou službu neposkytne – nedovolí zásilku odeslat.

Pokud zatrhnete i volbu **Ověřovat pomocí předcházejícího POP3 přístupu**, dovolí SMTP server odesílat zásilky pouze uživatelům, kteří se maximálně před 120 minutami úspěšně přihlásili do své POP3 schránky.

POZOR! – Pokud není zaškrtnuta ani jedna volba, SMTP server, obzvláště je-li připojen k internetu pevnou linkou, je zneužitelný pro šíření nevyžádaných (SPAM) zásilek!

Pokud chcete přístup k funkci SMTP RELAY navíc chránit speciálním IP filtrem, zaškrtněte volbu **Pro přístup k SMTP RELAY platí IP filtr** a po stisku tlačítka **SMTP relay IP filtr** nastavte povolené či zakázané IP adresy.

Např. přístup k SMTP RELAY pouze v rámci Vaší lokální sítě povolíte zpravidla zadáním IP adresy 192.168.1.1 a masky 255.255.255.0 (přístup bude povolen ze všech počítačů s IP adresou 192.168.1.x).

Nastavení odesílání pro odborníky

Nadřízený SMTP server vyžaduje autentizaci

Někteří poskytovatelé připojení vyžadují před odeslání e-mailu přes jejich SMTP server autentifikaci. Pokud to Váš poskytovatel požaduje, zaškrtněte volbu **Nadřízený SMTP server vyžaduje autentizaci**. Dále zvolte způsob autentifikace – **SMTP** nebo **POP3** (způsob Vám sdělí poskytovatel) a vyplňte **Jméno** a **Heslo**.

Privátní sítě a sítě WAN

Směrování poštovních zásilek podle seznamu použijete v případě, že se zásilky do vyjmenovaných domén mají posílat přímo na určité počítače, narozdíl od ostatních zásilek, které budou doručovány do internetu podle MX záznamů v DNS nebo prostřednictvím SMTP serveru poskytovatele. Jako příklad použití uveďme doručování zásilek SMTP protokolem v síti WAN a do internetu.

Při zaškrtnutí čtverce **Směrování podle seznamu** v dialogu **Nastavení odesílání pro odborníky** se zpřístupní tlačítko **Přednastavená směrování**. Jeho stiskem se otevře pomocný dialog. Do polí **Poštovní doména** a **Cílový počítač** zapište potřebné údaje a stiskněte tlačítko **Přidat**. Zadaná dvojice hodnot se zařadí do seznamu. Údaje v seznamu lze upravovat nebo mazat po nastavení ukazatele a stisku tlačítka **Vymazat/Editovat**.

Nastavení DNS

Vyplňte položky **DNS1** a **DNS2** (pokud existuje) podle údajů od poskytovatele připojení. Pokud tyto parametry nezadáte, LAN SUITE použije DNS zadané v konfiguraci protokolu TCP/IP ve Windows (viz výše Přímé odesílání zásilek s využitím MX záznamů DNS).

Pracovní intervaly

Nastavení pracovních intervalů pro SMTP server:

- **Doba mezi dvěma pokusy o odeslání zásilky** – pokud nemůže být zásilka odeslána (např. cílový SMTP server je mimo provoz), bude pokus o odeslání opakován po uplynutí zadané doby (v minutách).
- **Nedoručitelnou zásilku odložit po** – může se také stát, že se zásilku nezdaří doručit ani při dalších pokusech. Tento parametr udává interval v hodinách, po kterém je nedoručitelná zásilka definitivně odložena.

Max. počet současných SMTP vysílání

Hodnota položky **Max. počet současných SMTP vysílání** v okně **Nastavení odesílání pro odborníky** určuje, kolik může být zároveň navázáno SMTP spojení pro vysílání zásilek. To umožňuje regulovat zatížení komunikační linky.

Nastavení Anti-spam

Stiskem tlačítka **Anti-spam nastavení** se otevře dialog, ve kterém můžete potlačit příjem nežádoucích, zejména reklamních zásilek (tzv. spamů). Dialog má dvě okna:

Použít zvolené vyhledávací DNSBL služby k odmítnutí zásilek od spamovacích serverů

V okně je zobrazena „černá listina“ serverů, které se zabývají odhalováním serverů rozesílajících spamy. Seznam je sestaven za mezinárodní spolupráce poskytovatelů připojení. Pokud zaškrtnete čtverec před názvem položky, příjem zásilek ze spamového serveru bude službou posouzen a případně odmítnut. Některé servery poskytují své služby zdarma (FREE) a některé ne (PAY). Seznam si můžete sami upravit pomocí trojice tlačítek **Přidat službu**, **Editovat službu** a **Smazat službu**.

U každé služby můžete nastavit:

- **Jméno služby** – popisné jméno
- **Vyhledávací doména** – doména, kde je služba provozována
- **IP adresa vracená v případě nalezení v seznamu** – návratovou adresu definuje poskytovatel anti-apam služby. Je vrácena SMTP serveru v případě nalezení odesílacího serveru v databázi.
- **Text zamítnutí** – tento text je zaznamenán do log souboru v případě, že je příchozí zásilka spam.

Odmítnout zásilky od těchto serverů nebo odesílatelů

Pomocí tlačítek **Přidat**, **Editovat** a **Smazat** si můžete vytvořit seznam adres, ze kterých nebudete přijímat žádné zásilky. Lze zadat konkrétní e-mailovou adresu, adresu serveru nebo použít zástupné znaky * a ?. Seznam můžete také importovat i exportovat ve formě textového souboru, kde na každé řádce je jeden server nebo odesílatel.

POP3

POP3 server v LAN SUITE umožňuje jejím uživatelům pracovat s elektronickou poštou POP3 klientskými programy (např. Outlook Express). LAN SUITE lze také nakonfigurovat tak, aby automaticky stahovala poštu z POP3 schránek na internetu a doručovala ji do schránek uživatelů.

Zapnutí (SSL) POP3 serveru

POP3 server zapnete zaškrtnutím stejnojmenné volby. Dále můžete specifikovat TCP/IP rozhraní, na kterém bude POP3 server naslouchat. Standardně jsou zvolena **všechny,** ale můžete vybrat i konkrétní **IP adresu** ze seznamu. Standardní port pro POP3 server je 110, můžete ho ale v případě potřeby změnit (je ale pak nutné provést obdobnou změnu i v konfiguraci klientských programů).

LAN SUITE také obsahuje zabezpečený SSL POP3 server. Jeho konfigurace je shodná jako u standardního POP3 serveru. Standardně je spouštěn na portu 995.

Pravidelné vybírání POP3 schránek

Do **Seznamu POP3 schránek, které mají být pravidelně vybírány** můžete tlačítkem **Přidat** snadno doplnit další schránku. Již zadané schránky můžete tlačítky vpravo **Editovat** nebo **Vymazat.**

Základní parametry pro výběr POP3 schránky

Při zadávání nové (editaci stávající) vybírané POP3 schránky je třeba zadat následující údaje (sdělí Vám je zpravidla poskytovatel připojení):

- **POP3 server** – adresa serveru na internetu s danou POP3 schránkou
- **Přihlašovací jméno** – jméno schránky (uživatelské jméno)
- **Heslo** – přihlašovací heslo

Použít APOP

Pokud nastavíte volbu **Použít APOP** na **Ano,** bude při přihlašování do POP3 schránky místo nezakódovaného hesla zaslán pouze jeho otisk v řetězci náhodných znaků, což zvyšuje bezpečnost. Záleží na poskytovateli schránky, zda tuto možnost podporuje. Standardně je tato volba nastavena na **Ne**.

Třídění přijatých zásilek

Pomocí volby **Přijaté zásilky doručit** můžete specifikovat, komu budou doručovány zásilky získané z dané POP3 schránky.

Pokud zvolíte možnost **podle adres v dopisu** budou zásilky automaticky doručovány uživatelům podle adresy (tj. bude se kontrolovat adresa adresáta proti uživatelskému jménu a doméně nastavené v LAN SUITE a následně proti nastaveným aliasům). Tak lze například nechat LAN SUITE automaticky doručovat poštu z tzv. doménového koše.

Druhou možností je doručování konkrétnímu uživateli bez ohledu na adresu v dopise. V tom případě zvolte ze seznamu **Přijaté zásilky doručit** konkrétního uživatele.

Interval výběru schránky

Časový interval kontaktování POP3 schránky s cílem vybrat její obsah nastavíte přepínačem **Kdy vybírat schránku**:

- **každých X minut** – schránka bude vybírána v pravidelných časových intervalech, vždy po uplynutí X minut
- **v určených časech** – schránka bude vybírána v určené hodiny a minuty; seznam časových údajů zapíšete do pole vedle sebe oddělíte čárkou, například 7:00, 9:00, 12:00, 13:00…atd.

Další omezení výběru POP3 schránek s ohledem na navazování připojení lze nastavit na záložce Připojení.

Ponechání zásilek na serveru

Standardně se zásilky vybrané z POP3 schránky ze serveru na internetu odstraňují. Pokud je chcete na serveru ještě nějakou dobu ponechat, můžete do pole **Ponechat vybrané zásilky na serveru po dobu X dní** zapsat počet dnů, kolik se má ve schránce na serveru uchovat originál zásilky, jejíž kopie již byla vložena do lokální schránky adresáta. Pokud zde zapíšete nulu, budou se zásilky z internetu adresátům do schránek přímo přesouvat aniž by vznikaly kopie.

Anti-virus

LAN SUITE 2003 Antivirus Edition obsahuje vestavěnou centrální antivirovou kontrolu všech zásilek pomocí systému BitDefender™, a to včetně jeho automatické aktualizace. Alternativně lze pro antivirovou kontrolu zásilek využít externí antivirový systém AVG firmy Grisoft.

Zapnutí antivirové kontroly

Vestavěnou antivirovou kontrolu (systémem BitDefender™) zapnete zaškrtnutím volby **Provádět kontrolu doručovaných zásilek antivirovým systémem 602Pro LAN SUITE** (tato volba je aktivní pouze v LAN SUITE 2003 Antivirus Edition). V případě, že je v příchozí nebo odchozí zásilce detekován vir, záleží na nastavení dalších voleb na kartě.

Poznámka: Pokud není pro danou situaci zaškrtnuta žádná z voleb (a antivirová kontrola je zapnuta), není zavirovaná zásilka doručena nikomu a je rovnou odstraněna (bez odeslání upozorňovacího e-mailu).

V případě nakažené příchozí zásilky

Chování LAN SUITE při nalezení viru v příchozí zásilce lze nastavit po stisknutí tlačítka **V případě nakažené příchozí zásilky:**

Zaslat adresátům

Pomocí této volby můžete specifikovat, co bude doručeno původním adresátům zavirované zásilky. Na výběr máte následující možnosti:

- **Vyrozumění o závadnosti zásilky** – pouze upozorňující e-mail, že jim odesílatel poslal zavirovanou zásilku
- **Vyrozumění s tělem dopisu původní zásilky** – obsahuje upozornění na přítomnost viru v původní zásilce a (pouze) text původní zásilky
- **Vyrozumění s připojenou původní zásilkou** – obsahuje upozornění na přítomnost viru v původní zásilce a celou původní zásilku – tedy včetně zavirovaných souborů!

Zaslat závadnou zásilku do speciální schránky

Informace o zavirované zásilce může být doručena také do speciální schránky, kterou vyberete ze seznamu vpravo. Je vhodné zvolit např. schránku, u které se předpokládá, že je pro tento účel vyčleněna a spravuje ji tedy uživatel dobře seznámený s antivirovou problematikou. Co bude do této schránky doručeno lze nastavit analogicky jako u původního adresáta:

- **Vyrozumění o závadnosti zásilky**
- **Vyrozumění s tělem dopisu původní zásilky**
- **Vyrozumění s připojenou původní zásilkou**

Zaslat administrátorům vyrozumění o závadné zásilce

Vyrozumění o zavirované zásilce může být také navíc doručeno uživatelům, kteří mají administrátorská práva (viz Uživatelé).

V případě nakažené odchozí zásilky

Chování LAN SUITE při nalezení viru v odchozí zásilce lze nastavit po stisknutí tlačítka **V případě nakažené odchozí zásilky**. Při zapnuté antivirové kontrole není zavirovaná zásilka nikdy odeslána bez ohledu na toto další nastavení!

Zaslat odesilateli

Pomocí této volby můžete specifikovat, co bude doručeno odesilateli zavirované zásilky (uživateli LAN SUITE). Na výběr máte následující možnosti:

- **Vyrozumění o závadnosti zásilky** – pouze upozorňující e-mail, že se pokusil odeslat zavirovanou zásilku
- **Vyrozumění s tělem dopisu původní zásilky** – obsahuje upozornění na přítomnost viru v původní zásilce a (pouze) text původní zásilky
- **Vyrozumění s připojenou původní zásilkou** – obsahuje upozornění na přítomnost viru v původní zásilce a celou původní zásilku – tedy včetně zavirovaných souborů!

Zaslat závadnou zásilku do speciální schránky

Informace o zavirované zásilce může být doručena také do speciální schránky, kterou vyberete ze seznamu vpravo. Je vhodné zvolit např. schránku, u které se předpokládá, že je pro tento účel vyčleněna a spravuje ji tedy uživatel dobře seznámený s antivirovou problematikou. Co bude do této schránky doručeno lze nastavit analogicky jako u odesilatele:

- **Vyrozumění o závadnosti zásilky**
- **Vyrozumění s tělem dopisu původní zásilky**
- **Vyrozumění s připojenou původní zásilkou**

Zaslat administrátorům vyrozumění o závadné zásilce

Vyrozumění o zavirované zásilce může být také navíc doručeno uživatelům, kteří mají administrátorská práva (viz Uživatelé).

Certifikace

Po zaškrtnutí volby **Certifikovat příchozí e-mailové zásilky** bude na konec všech přijímaných zásilek automaticky vkládán text, který zadáte do editačního pole **Certifikační text doplněný do příchozích zásilek**.

Analogicky bude po zaškrtnutí volby **Certifikovat odchozí e-mailové zásilky** na konec všech odchozích zásilek automaticky vkládán text, který zadáte do editačního pole **Certifikační text doplněný do odchozích zásilek**.

Aktualizace

LAN SUITE 2003 Antivirus Edition umožňuje provádět v pravidelných intervalech automatickou aktualizaci vestavěného antivirového systému BitDefender™. To lze nastavit pomocí volby **Provádět automatickou aktualizaci anti-viru každých** X **hodin**.

Pokud v okamžiku vypršení intervalu pro aktualizaci není navázáno dial-up připojení k internetu, provede LAN SUITE aktualizaci okamžitě po jeho dalším navázání.

V případě potřeby je možno provést aktualizaci okamžitě stiskem tlačítka **Provést aktualizaci**.

AVG

Pokud máte na stejném počítači s LAN SUITE nainstalován antivirový systém AVG (verze 6 nebo 7), můžete ho při dodržení licenčních podmínek využít ke kontrole přijímaných zásilek.

Antivirovou kontrolu zapnete zaškrtnutím volby **Provádět kontrolu doručovaných zásilek antivirovým systémem AVG** na záložce AVG. V případě, že je v příchozí nebo odchozí zásilce detekován vir, záleží na nastavení dalších voleb na kartě **Nastavení**.

Pozn. LAN SUITE nekontroluje ani neprovádí automatické aktualizace systému AVG.

Fax

Tato karta obsahuje ovládací prvky pro nastavení odesílání a příjmu faxů.

Faxy mohou být odesílány přes analogový faxmodem nebo ISDN zařízení, jehož ovladače CAPI podporují G3 fax.

Základní údaje

Na této záložce lze nastavit metodu faxování, pracovní intervaly a další pomocné parametry týkající se faxování.

Faxování povolíte zaškrtnutím volby **FAX server**. Následně budete mít možnost zvolit zařízení pro odesílání a příjem faxů:

- **TAPI zařízení** – analogový faxmodem
- **CAPI zařízení** – ISDN modem, ISDN karta

Identifikace faxu

Do pole **Identifikace faxu** zapište informaci, která bude moci být využita pro Vaši identifikaci jako odesílatele (zobrazí se na display přijímacího faxu, vytiskne do reportu apod.). Tato informace bude v úvodní části spojení předána protějšímu faxu a umožní mu Vaši identifikaci. Doporučujeme, aby součástí řetězce bylo Vaše vlastní faxové číslo.

Automatický tisk faxů

Pomocí volby **Tisknout přijaté faxy na zvolené tiskárně** můžete určit, zda se budou všechny přijaté faxy automaticky tisknout na zvolené tiskárně. Zvolit můžete libovolnou tiskárnu dostupnou z počítače s LAN SUITE (i síťovou).

Vkládat záhlaví do faxu

Pokud zaškrtnete tuto volbu, bude v záhlaví každého faxu, který odešlete, vložen text zadaný v řádku **Text přidaný do řádky v záhlaví**. Tento text může obsahovat např. název Vaší firmy apod.

Detekce OLE podpory

V sekci **OLE podpora** je uveden seznam typů souborů, pro které LAN SUITE nalezla na počítači OLE podporu. Soubory těchto typů lze odesílat jako faxy ve formě e-mailu s připojeným souborem. Pokud chcete seznam manuálně obnovit (např. po instalaci další aplikace), stiskněte tlačítko **Detekovat**.

Pracovní intervaly

V této sekci se nastavují intervaly pro časové řízení zpracování faxů:

- **Aktivace Fax serveru** – server bude aktivován po uplynutí daného počtu sekund a pokud ve frontě čekají na odeslání faxy, pokusí se jeden odeslat.

- **Odložení zásilky** – pokud se fax nepodařilo odeslat, bude se pokus o odeslání opakovat po nastaveném počtu minut.
- **Max. počet pokusů o odeslání** – tento parametr určuje maximální počet pokusů o odeslání faxu (v případě, že se jej nepodařilo napoprvé odeslat). První pokus v sobě zahrnuje čtyři vytočení cílového čísla, každý další pokus pak již jen dvě vytočení.

Záložka TAPI

V případě, že jste na záložce **Základní údaje** zvolili faxování pomocí **TAPI zařízení**, můžete na této záložce nastavit další parametry týkající se tohoto zařízení.

Všechna TAPI zařízení dostupná na daném počítači jsou zobrazena v **Seznamu TAPI zařízení**, ze kterého můžete jedno z nich zvolit. LAN SUITE podporuje pouze jedno TAPI zařízení pro odesílání i příjem faxů.

Vlastnosti TAPI zařízení

Pomocí tohoto tlačítka otevřete dialog operačního systému Windows, který slouží k nastavení předvoleb pro zvolené TAPI zařízení. Tento dialog je ve Windows rovněž dostupný přes Ovládací panely.

Vlastnosti vytáčení

Toto tlačítko otevře systémový dialog pro nastavení vlastností vytáčení (směrové číslo země, oblasti, přístup k vnější lince apod.). **Vlastnosti vytáčení** přímo ovlivňují sestavení vytáčeného čísla (např. zda se bude vytáčet nula pro přístup na státní linku).

Tento dialog je ve také Windows dostupný přes Ovládací panely.

Příkazy pro ovládání modemu

V sekci **Modemové příkazy pro 602Pro LAN SUITE** lze zadat tzv. „AT příkazy“ pro nastavení (**Konfigurace**) a reset (**Reset modemu**) Vašeho modemu. Ve většině případů postačí ponechat implicitní hodnoty.

Odpovídání na volání

Pomocí volby **Odpověď na volání** můžete nastavit, po kolika zvoněních zvedne LAN SUITE linku a odpoví na přicházející volání.

Nastavení sady ovládacích příkazů

Faxmodemy disponují několika sadami ovládacích příkazů své faxové části. Voličem **Sada ovládacích příkazů** lze tuto sadu zvolit přímo nebo její volbu ponechat na serveru prostřednictvím autodetekce:

- **Autodetekce** – LAN SUITE se pokusí zjistit, jakou sadu ovládacích příkazů faxmodem podporuje a tu bude používat.

Pokud autodetekce nefunguje, zkuste nastavit sadu ovládacích příkazů manuálně:

- **Class 1** – nejstarší sada příkazů, většinu operací spojených s faxováním provádí počítač. Doporučujeme vyzkoušet v případě problémů s autodetekcí. Class 1 a Class 2 jsou podporovány modemy založenými na chipsetu Rockwell.
- **Class 2** – aktualizovaná verze, nikdy nebyla zcela standardizována. Modem přebírá celou řadu operací spojených s faxováním. Tato sada příkazů je typická pro modemy ZyXEL.
- **Class 2.0** – nejnovější verze, je plně standardizována, ale zatím není příliš rozšířena. Podporují ji novější modemy ZyXEL a US Robotics.

Omezení rychlosti vysílání a příjmu

Pomocí voličů **Omezení rychlosti vysílání** a **Omezení rychlosti příjmu** můžete manuálně snížit rychlost vysílání resp. příjmu faxů, a tím se přizpůsobit kvalitě telefonní linky. Rychlost může být **NEOMEZENÁ** nebo **2400-12000 bit/s**.

Záložka CAPI

V případě, že jste na záložce **Základní údaje** zvolili faxování pomocí **CAPI zařízení**, můžete na této záložce nastavit další parametry týkající se tohoto zařízení.

Všechna CAPI zařízení dostupná na daném počítači jsou zobrazena v **Seznamu CAPI zařízení**, ze kterého můžete jedno z nich zvolit. LAN SUITE podporuje pouze jedno CAPI zařízení pro odesílání i příjem faxů.

Vlastnosti vytáčení

Toto tlačítko otevře systémový dialog pro nastavení vlastností vytáčení (směrové číslo země, oblasti, přístup k vnější lince apod.). **Vlastnosti vytáčení** přímo ovlivňují sestavení vytáčeného čísla (např. zda se bude vytáčet nula pro přístup na státní linku).

Tento dialog je ve také Windows dostupný přes Ovládací panely.

Referenční telefonní číslo

Do řádku **Referenční telefonní číslo (MSN)** zadejte, na kterém telefonním čísle bude CAPI zařízení faxy přijímat (jedna ISDN linka totiž podporuje více telefonních čísel). Pokud žádné referenční číslo nezadáte, bude LAN SUITE obsluhovat všechna čísla na ISDN lince.

Proxy

Proxy server v LAN SUITE přijímá požadavky od klientských počítačů ze sítě a sám je vyřizuje na internetu. Získané odpovědi na požadavky (typicky HTML stránky) pak vrací příslušným klientským počítačům. Proxy pracují vždy na konkrétním komunikačním protokolu. Klientský program proto musí podporovat komunikaci prostřednictvím proxy (nebo SOCKS).

Proxy a bezpečnost připojení k internetu

Proxy server plní dvě funkce:

- Proxy – zprostředkovává přístup do internetu stanicím v síti pro následující aplikační protokoly (HTTP, HTTPS, HTTP-FTP).
- Zabezpečení – veškerá komunikace lokální sítě s internetem se odehrává přes jedinou IP adresu (přes počítač s LAN SUITE). Tak je možno kontrolovat všechny požadavky na komunikaci protokoly HTTP, HTTPS, HTTP-FTP.

  Pokud chcete zvýšit úroveň zabezpečení, musíte zvolit zabezpečení nezávislé na aplikačních protokolech. LAN SUITE obsahuje také SOCKS server. SOCKS server zapíná/vypíná softwarový IP filtr. Pokud není zapnuta HTTP proxy ani SOCKS proxy, všechna nastavení na kartě **IP filtr** jsou ignorována a IP filtr je nefunkční. SOCKS server také využijí některé aplikace, které pro svou činnost potřebují komunikovat s internetem (ICQ, některé FTP klientské programy apod.).

Nastavení HTTP, HTTPS, HTTP-FTP proxy

Tuto proxy zapnete zaškrtnutím volby **HTTP/HTTPS/HTTP-FTP proxy**. Tím je proxy připravena poskytovat služby internetovým prohlížečům (např. Internet Explorer). Standardní port pro tuto proxy je 80.

Po zaškrtnutí volby **Pro HTTP proxy použít jiný port než pro WWW server** máte možnost do vstupního pole zadat číslo portu, který bude použit pro HTTP proxy nezávisle na nastavení WWW serveru (např. 3128).

Pozn. Pokud hodláte na počítači s LAN SUITE provozovat jiný WWW server, než je v ní obsažen, budete muset tuto volbu zaškrtnout a zadat jiný port (např. 8080) nebo změnit hodnotu **WWW port** na kartě **WWW**.

Autentifikace do proxy

Při zaškrtnutí volby **Autentifikace požadována** se bude pro přístup k službě HTTP proxy vyžadovat autentifikace uživatele (přihlášení přes jméno a heslo). Zda bude moci daný uživatel služby HTTP proxy využít (tzn. prohlížet si stránky na internetu) ovlivníte zaškrtnutím práva **Uživatel smí používat proxy** ve vlastnostech daného uživatele (viz Uživatelé).

Nastavení pro odborníky

Stiskem tlačítka **HTTP proxy nastavení pro odborníky** se otevře pomocný dialog pro upřesnění požadavků na HTTP proxy.

Parametry interní vyrovnávací paměti cache lze zadat po zaškrtnutí volby **Lokální proxy cache**. Ta slouží k dočasnému ukládání dat stahovaných z internetu (prohlížených stránek, obrázků atd.) a pokud je požaduje jiný uživatel, nemusí se znovu stahovat nebo kvůli nim navazovat dial-up spojení. Tím se zvyšuje rychlost a zároveň snižují náklady na připojení.

Nastavit lze následující parametry a volby:

- **Adresář s cache** – zadejte přístupovou cestu k adresáři, kde má být vyrovnávací paměť vytvořena (kam mají být data dočasně ukládána).
- **Perioda úklidu cache** – časový interval v minutách, po kterém bude obsah vyrovnávací paměti testován a uvolněn vymazáním souborů s prošlou expirační dobou.
- **Max. velikost cache** – fyzická velikost prostoru na disku vyhrazeného pro cache (zadávaná v kilobajtech).
- **Expirační doba souborů** – doba v hodinách, po které budou soubory uložené ve vyrovnávací paměti vymazány.
- **Vyžadovat informace o souborech** – některé WWW a FTP servery nesdělují klientským programům velikost souborů a další informace. Pak se může stát, že v cache zůstane nekompletní soubor. Pokud zaškrtnete tuto volbu, nebudou se soubory bez připojených informací do cache ukládat.
- **Skripty (CGI, ASP) vždy provádět** – proxy se pokusí podle URL zjistit, zda je daná HTML stránka produktem CGI skriptu a pokud je, neuloží ji do cache, aby se

při příštím pokusu o stažení znovu aktivoval CGI skript a neposlala se tedy stránka uložená v cache paměti.

- **Povolit řízení cache HTTP příkazy** – vysílající WWW server může vložit do hlaviček přenášených informací příkazy specifikující, jakým způsobem má být s příslušnou stránkou nakládáno. Obvykle se browseru a proxy přikazuje, aby stránka nebyla vkládána do cache nebo se vymezuje její časová platnost. Pokud volbu nezaškrtnete, proxy (a cache) tyto příkazy ignoruje.

Do vstupního pole **Nadřízený proxy/cache server** můžete napsat adresu jiného počítače, disponujícího proxy pro HTTP a FTP, kterou budete chtít využívat. Typickým příkladem využití je proxy server poskytovatele připojení k internetu. Tak lze také zvýšit efektivitu připojení k internetu.

SOCKS proxy

Zaškrtnutím této volby zapnete SOCKS server (verze 4 a 5) a zároveň IP filtr na „síťové“ úrovni. SOCKS proxy využijí internetové aplikace jako např. ICQ a některé FTP klientské programy.

Pokud je **SOCKS proxy** spuštěna, mohly by aplikace (typicky internetové prohlížeče) obcházet **autentifikaci do proxy**. Proto pokud používáte autentifikaci do proxy a máte zapnutou SOCKS proxy, měli byste zaškrtnout také volbu **Nedovolit HTTP ani FTP spojení přes SOCKS proxy**.

FTP server proxy

FTP server proxy pro použití z FTP klientů poslouchá na portu FTP (21) a pracuje podobně jako protokol FTP.

Tento proxy server lze použít „přímo“ z každého FTP klienta tak, že se místo cílového FTP serveru zadá adresa proxy a místo jména uživatele user@host:port (jménouživatele@adresaFTPserveru:port). Většina FTP klientských programů však tento proxy server podporuje přímo, obvykle pod názvem firewall bez logování uživatelů (bez password módu).

Zaškrtnutím přepínače **FTP server proxy** se povolí vyrovnávací paměť (cache) pro FTP klientské programy pracující na portu FTP, tedy 21 (např. pro WS-FTP, CuteFTP apod.)

Pozn. Pokud potřebujete na počítači s LAN SUITE provozovat jiný FTP server, změňte hodnotu **FTP proxy port** (např. na 8021).

Telnet a RealAudio proxy

Zaškrtnutím volby **TELNET server proxy** zpřístupníte proxy pro Telnet. Princip práce spočívá v tom, že se programem Telnet nejprve spojíte na adresu počítače s proxy, kde se objeví výzva k zadání adresy a případně portu cílového počítače, kam se chcete ve skutečnosti spojit. Po zadání tohoto údaje dojde ke spojení s cílovým počítačem a vše probíhá standardním způsobem.

Volbou **RealAudio proxy** zpřístupníte službu RealAudio proxy. Firma RealNetworks (http://www.real.com) vytvořila softwarovou podporu pro přenos multimediálních dat (rozhlas, video…) po internetu. Aby bylo možné používat tuto službu i v lokálních sítích napojených na internet pouze prostřednictvím proxy, obsahuje LAN SUITE i RealAudio proxy postavenou na SDK firmy RealNetworks. Pro použití této proxy je nutné mít RealAudio Player verze 3 nebo vyšší, kde je podpora této proxy implementována.

DNS proxy

Pokud je zaškrtnuta tato volba, LAN SUITE zprostředkovává služby DNS serveru ostatním počítačům v síti tak, že zajišťuje překlad adres pomocí DNS serveru poskytovatele připojení. Fungující DNS je nutné pro provoz aplikací přes SOCKS proxy.

Potlačením zaškrtnutí volby **DNS proxy** se uvolní port tohoto počítače pro příjem DNS požadavků, což může být nutné, pokud má na tomto počítači pracovat jiný DNS server.

Zakázání navazování dial-up spojení kvůli DNS

Pokud jste připojeni k internetu pomocí dial-up, máte možnost zaškrtnout volbu **Nenavazovat dial-up spojení kvůli DNS**, což může být výhodné s ohledem na poplatky za připojení (DNS požadavky totiž často generují i aplikace, které jinak s internetem vůbec komunikovat nepotřebují).

Nastavení portů pro služby proxy

Všechny služby proxy můžete provozovat na jiných něž standardních portech zapsáním hodnoty portu do příslušného okénka.

Tlačítkem **Nastavit implicitní porty** naplníte všechna vstupní pole proxy portů implicitními hodnotami.

Proxy – Přístup na servery

Na této záložce můžete zakázat či povolit přístup ke konkrétním serverům na internetu uživatelům využívajícím služby proxy, SOCKS nebo DNS. K dispozici jsou dva režimy – zákaz přístupu a povolení přístupu.

Omezení pro uživatele se specifikují s využitím jejich IP adres a masek. To postačuje k nastavení omezení přístupu na danou URL jak pro jeden počítač tak pro podsíť.

Pokud potřebujete specifikovat celou síť, napište do polí **Vstupní adresa** a **Vstupní maska** hodnoty 0.0.0.0

Pokud chcete omezení nastavit pro konkrétní počítač nebo skupinu počítačů (podsíť), zapište do polí specifickou IP adresu a masku (princip je obdobný jako u vstupních parametrů IP filtru).

Narozdíl od IP filtru se servery, ke kterým chcete omezit/povolit přístup, definují jménem nebo částí jména obsahující zástupné znaky * a ?. Hvězdička přitom značí skupinu libovolných přípustných znaků, otazník zastupuje jeden libovolný přípustný znak.

Zadávání zakázaných/povolených serverů

Ke vkládání serverů s omezeným přístupem využijte vstupní pole **Vstupní IP adresa**, **Vstupní maska** a **URL nebo adresa**. Stiskem tlačítka **Přidat** údaje vložíte do seznamu. V něm je můžete později tlačítkem **Vymazat/Editovat** upravit nebo zrušit. Seznam omezení můžete také importovat nebo exportovat ve formě textového souboru (jedna adresa na jednom řádku), a tak ho přenášet nebo zálohovat.

Zda se bude jednat o seznam serverů, na něž je přístup zakázán, nebo naopak o seznam serverů, pouze na které lze přistupovat, určíte volbou v horní části okna:

- **Zakázat přístup na následující URL …**
- **Povolit přístup pouze na následující URL …**

Příklady omezení přístupu k serverům

.porno.*	omezuje přístup k serverům, jejichž název domény začíná znaky „porno“ pro všechny služby (HTTP, HTTPS, FTP)
*.obchod.??	zakazuje přístup k doméně obchod se všemi dvojznakovými kombinacemi domény (konkrétně může jít o adresy www.obchod.cz, trafika.obchod.sk – ale nikoliv www.obchod.com) pro všechny služby (HTTP, HTTPS, FTP).
www.sex.com	zamezuje přístup k jedinému serveru na dané adrese.

Proxy – Mapovaná spojení

Funkce „mapovaná spojení“ představuje alternativu pro napojení stanice privátní sítě k internetu. Je vhodná pro použití z aplikací, které nepodporují SOCKS ani proxy a spojují se na konkrétních portech pouze s jedním počítačem v internetu (např. připojení k serveru s diskusními příspěvky – news). Mapované spojení lze provádět protokolem TCP nebo UDP.

Princip fungování

Klientský program na stanici v privátní síti potřebuje navázat TCP/IP spojení s konkrétním počítačem v internetu. Místo adresy tohoto počítače se v klientském programu zadá adresa serveru s LAN SUITE, ve kterém se v záložce **Mapovaná spojení** určí, že pokud se na daný port připojí tato stanice, mají se všechny pakety posílat na určitý počítač v internetu. Tím se vytvoří virtuální spojení mezi počítači prostřednictvím počítače s LAN SUITE. Jedná se tedy o jakýsi přesměrovávač, jehož prostřednictvím se mohou po TCP/IP spojit dva počítače.

Výhody

Klientský program nemusí podporovat žádný typ firewallu, SOCKS nebo proxy.

Nevýhoda (vlastnost)

Stanice se takto může připojit pouze na jediný počítač v internetu, resp. na ty počítače, které jsou konkrétně nakonfigurovány v LAN SUITE.

Nastavení

Na záložce **Mapovaná spojení** je nutné nastavit:

- **Protokol** – jakým protokolem se má spojení realizovat (**TCP** nebo **UDP, UDP1, UDP2**). Typy UDP protokolů jsou vysvětleny níže.
- Ve sloupci **Spojení z** nastavte, který počítač se bude připojovat (pole **IP adresa** a **IP maska**).

  IP adresa – adresa počítače/počítačů, které budou moci používat dané mapované spojení. **Např.** Pro jeden konkrétní počítač zadejte jeho IP adresu, pro celou síť zadejte IP adresu počítače s LAN SUITE a změňte poslední číslici na 0 (typicky 192.168.1.0). Pro všechny počítače lze zadat 0.0.0.0.

IP maska – maska podsítě. **Např.** Pro jeden konkrétní počítač zadejte 255.255.255.255, pro celou síť pak 255.255.255.0. Pro všechny počítače lze zadat 0.0.0.0.

- Ve dvojici polí **Na tento počítač** zadejte, přes který port počítače bude navazován kontakt se serverem (pole **IP adresa** a **Port**).

  IP adresa – doporučujeme ponechat nastavení pro všechny. Konkrétní IP adresu zadejte, pouze pokud požadujete vyšší míru bezpečnosti.

  Port – pokud přijde požadavek na zadaný port, LAN SUITE ho přesměruje na cílovou adresu. Každé číslo portu můžete použít pouze jednou (ve dvojici s danou IP adresu). Zároveň nemůžete používat obsazené porty (např. 21, 80, 1080, 25, 110), pokud je neuvolníte např. vypnutím příslušných služeb v LAN SUITE.
- Ve dvojici polí **Mapovat na** se nastavuje, na který počítač se má toto spojení směřovat (pole **Cílová adresa** a **Port**).

  Zdrojový počítač s maskou a IP adresa počítače se serverem musí být uvedeny číselnou IP adresou; adresa a port cílového počítače mohou být uvedeny i symbolicky.

Nezapomeňte po zadání všech parametrů stisknout tlačítko **Přidat** a na závěr **Uložit** konfiguraci.

Poznámka 1

Formát tabulky tedy umožňuje i takové nastavení, kdy se přes jeden port počítače se serverem může současně spojovat více počítačů na několik různých cílových počítačů, protože definujeme, který zdrojový počítač (síť) se má spojovat na který cílový počítač.

Poznámka 2

Pokud chcete, aby mapované spojení pracovalo současně na všech IP adresách tohoto počítače, zadejte adresu jako 0.0.0.0 .

Nastavení pro protokol UDP

Pro spojení v internetu se používají v zásadě dva protokoly: TCP a UDP. Mapovaná spojení pomocí UDP nemají jednoznačné řešení – proto jsou podporovány tyto varianty mapování :

- **multiuser (UDP)** – tato varianta je nejkomfortnější, protože umožňuje provoz UDP protokolu současně z více stanic či aplikací, předpokládá však, že server z internetu

odpovídá volajícímu počítači UDP spojením na stejný port, ze kterého původní volání přišlo (tedy nikoliv na jeden pevně určený port).

- **one-way (UDP1)** – pokud není třeba, aby server v internetu navazoval zpětné UDP spojení, lze použít tuto variantu, která dovoluje navazovat stanicím v síti UDP spojení směrem do internetu – spojení zpět možné není.
- **single user through fixed port (UDP2)** – tato varianta mapovaného UDP spojení umožňuje UDP komunikaci pouze jedné stanici v síti, která z pevného portu volá server v internetu opět na stejný pevně stanovený port. Server v internetu pak může odpovídat zpět na tento daný port mapovaný na stanici v uzavřené síti. Tato varianta je vhodná pro servery, které zpětné UDP spojení navazují na pevně stanovaný port bez ohledu na to, ze kterého portu původní volání přišlo.

Příklady použití

SMTP/POP3 (přímý přístup k POP3 schránce)

Pokud potřebuje některý uživatel přistupovat přímo ke své POP3 schránce v internetu a chce i přímo odesílat e-maily (nechce z nějakého důvodu využívat služeb LAN SUITE), je třeba pro něj nastavit dvě mapovaná spojení:

TCP	192.168.1.0 / 255.255.255.0	192.168.1.1:2020	pop3.isp.cz:110
TCP	192.168.1.0 / 255.255.255.0	192.168.1.1:2021	smtp.isp.cz:25

V tomto případě je nutné patřičně upravit konfiguraci klientských programů (např. Outlook Express) tak, že jako SMTP a POP3 server zadáte IP adresu 192.168.1.1 a porty upřesníte na 2020 pro POP3 a 2021 pro SMTP.

Výsledkem výše popsaného nastavení je, že všichni uživatelé z lokální sítě mohou, pakliže mají správně nakonfigurované své klientské programy, přímo přistupovat k uvedenému SMTP a POP3 serveru.

Pozn. Pro zachování bezpečnosti je vhodné v sekci **Na tento počítač** zvolit pouze lokální **IP adresu** (např. 192.168.1.1). Pokud potřebujete vytvořit obdobná mapovaná spojení na více cílových serverů, nezapomeňte, že je třeba v sekci **Na tento počítač** použít **různá** čísla portů.

News (diskusní skupiny)

Následující příklad definuje, že všechny počítače z jedné podsítě budou přes jakoukoliv IP adresu počítače s LAN SUITE serverem spojeny s konkrétním NEWS serverem v internetu.

TCP 192.168.1.0 / 255.255.255.0 0.0.0.0:119 news_srv.x.cz:news

Time protokol

Následující příklad definuje, že všechny počítače z jedné podsítě budou přes jakoukoliv IP adresu počítače s LAN SUITE serverem spojeny s konkrétním TIME serverem v internetu.

UDP 192.168.1.0 / 255.255.255.0 0.0.0.0:time tock.usno.navy.mil:time

Proxy – IP filtr

Pomocí IP filtru můžete definovat, která spojení prostřednictvím proxy a SOCKS se mohou navazovat.

Kdo a kam má nebo nemá povolen přístup

Pomocí IP filtru můžete definovat, která spojení prostřednictvím proxy a SOCKS se mohou navazovat. Speciální IP filtry, které se nastavují na příslušných záložkách v konfiguraci, mohou dále omezovat přístup k WWW serveru, funkci SMTP RELAY a vzdálené administraci.

V sekci uprostřed karty vytvoříte seznam sítí a stanic, jimž (a na něž) je povolen nebo zakázán přístup. Jednotlivé položky se vkládají zápisem do čtveřice vstupních polí a stiskem tlačítka **Přidat**. Do polí **Vstupní IP adresa** a **Vstupní maska** zapište adresu a masku počítače nebo sítě, který požadavek vyslal. Do polí **Cílová IP adresa** a **Cílová maska** pak adresu a masku počítače, kam požadavek míří. Ke každé položce IP filtru je třeba definovat, zda znamená zákaz nebo povolení. K tomu je vlevo pod seznamem volič s dvojicí semaforů – červená znamená (podle očekávání) zákaz přístupu, zelená přístup povoluje.

Zopakování základních pojmů

Počítačová síť je definována IP adresou a maskou. IP adresa definuje hodnotu adres v síti, maska velikost sítě, tj. max. počet IP adres v dané síti. Pomocí bitové operace AND je pak možné např. zjistit, zda určitá konkrétní IP adresa patří do určité sítě.

Příklady masek :

255.255.255.255 … jednotlivec; počítač s výše danou IP adresou,

255.255.255.0 … všechny počítače dané sítě typu C (tj. prakticky 254 počítačů),

255.255.255.224 … podsíť s 32 adresami (tj. prakticky 30 počítačů),

0.0.0.0 … maska zahrnující všechny IP adresy, tedy celý internet.

Princip činnosti IP filtru

Pomocí IP filtru se tedy ověřuje, zda je povoleno navázat určité spojení mezi dvěma počítači v internetu. Vezme se tedy IP adresa počítače, který chce spojení navázat (KDO_IP) a adresa počítače kam se chce spojit (KAM_IP) a **postupně se procházejí položky IP filtru ve směru shora dolů** a hledá se, zda je dané spojení některou z položek zakázané (= záporný výsledek IP filtru) nebo zda je dané spojení povolené (= kladný výsledek IP filtru). Pokud se nenašla žádná odpovídající položka, je výsledek IP filtru též záporný. To umožňuje provést např. takové nastavení, které lokálním uživatelům zpřístupňuje celý internet a přitom nejprve specifikovat jednotlivé počítače nebo sítě, kam přístup povolen není. Pokud je výsledek IP filtru kladný, může se dané spojení začít navazovat.

Zda se tedy daná položka IP filtru na dané spojení vztahuje, se zjišťuje podle následujících pravidel:

VSTUPNI_IP AND VSTUPNI_MASKA = KDO_IP AND VSTUPNI_MASKA

VYSTUPNI_IP AND VYSTUPNI_MASKA = KAM_IP AND VYSTUPNI_MASKA

Pokud potřebujete změnit pořadí položek v seznamu, označte ji a stiskněte **Ctrl + šipka nahoru** nebo **Ctrl + šipka dolů**. Pokud chcete určitou položku seznamu zrušit, nastavte na ni ukazatel a stiskněte tlačítko **Vymazat**. Položku pod ukazatelem můžete také editovat, protože její obsah se přenese do editačních okének.

Upozornění

Při použití dvoustupňové cache nelze v IP filtru používat omezení cílovou IP maskou, protože proxy server v tomto případě nezjišťuje IP adresu cílového počítače. Pro omezení přístupu pouze k některým počítačům můžete použít filtr zakázaných URL (viz **Přístup na servery**).

Příklady nastavení IP filtru

Příklad 1

Chcete nastavit IP filtr tak, aby:

- tři zaměstnanci s IP adresami 192.168.1.25, 192.168.1.35 a 192.168.1.38 neměli přístup do internetu,
- všichni ostatní mohli do internetu,
- uživatelé z internetu měli přístup pouze k počítači s IP adresou 192.168.1.1.

Řešení:

semafor	Vstupní adr.	Vstupní maska	Cílová adr.	Cílová maska
červená	192.168.1.25	255.255.255.255	0.0.0.0	0.0.0.0
červená	192.168.1.35	255.255.255.255	0.0.0.0	0.0.0.0
červená	192.168.1.38	255.255.255.255	0.0.0.0	0.0.0.0
zelená	192.168.1.0	255.255.255.0	0.0.0.0	0.0.0.0
zelená	0.0.0.0	0.0.0.0	192.168.1.1	255.255.255.255

Pozn. Kdyby bylo čtvrté pravidlo zařazeno jako první, nebylo by již možné omezit požadované tři uživatele.

Příklad 2

Všichni uživatelé sítě 192.168.1.0 mají mít možnost komunikovat s libovolným počítačem internetu. Přitom z internetu nemá být tato síť dosažitelná. Adresy nastavte na hodnoty:

semafor	Vstupní adr.	Vstupní maska	Cílová adr.	Cílová maska
zelená	192.168.1.0	255.255.255.0	0.0.0.0	0.0.0.0

Příklad 3

Je třeba zajistit, aby všichni uživatelé lokální sítě s adresami 192.168.1.0 (s max. 255 počítači) mohli kamkoliv do internetu, kromě serveru 194.196.5.193. Ostatní uživatelé z internetu nebudou mít povoleno žádné spojení.

semafor	Vstupní adr.	Vstupní maska	Cílová adr.	Cílová maska
červená	192.168.1.0	255.255.255.0	194.196.5.193	255.255.255.255
zelená	192.168.1.0	255.255.255.0	0.0.0.0	0.0.0.0

Příklad 4

Je zapotřebí potlačit funkci IP filtru; spojení tedy bude možné mezi libovolnými počítači. Adresy nastavte v tomto případě na hodnoty:

semafor	Vstupní adr.	Vstupní maska	Cílová adr.	Cílová maska
zelená	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Příklad 5

Budete chtít povolit komunikaci pouze uživateli s IP 192.168.1.2. Adresy nastavte takto:

Semafor	Vstupní adr.	Vstupní maska	Cílová adr.	Cílová maska
Zelená	192.168.1.2	255.255.255.255	0.0.0.0	0.0.0.0

WWW

LAN SUITE obsahuje také WWW a SSL WWW server. Parametry těchto serverů se nastavují na této záložce.

Konfigurace WWW serveru

Zaškrtnutím volby **WWW server** (resp. **SSL WWW server**) zapnete příslušný web server.

Dále můžete specifikovat TCP/IP rozhraní, na kterém bude provozován. Standardně jsou zvolena **všechny,** ale můžete vybrat i konkrétní **IP adresu** ze seznamu. To může být vhodné jak z provozních, tak bezpečnostních důvodů (můžete specifikovat pouze vnitřní IP adresu, která umožní přístup k WWW serveru pouze lokálním uživatelům).

Pozn. Standardní **WWW port** je 80, ale můžete ho změnit, pokud na stejném počítači hodláte provozovat jiný web server. V tom případě nastavte **WWW port** např. na hodnotu 8080.

Nastavení adresářů a dalších parametrů WWW serveru

Pro provoz WWW serveru je třeba nastavit následující parametry:

- **Hlavní adresář WWW serveru** – umístění hlavního („root“) adresáře web serveru
- **Jméno souboru s indexem** – jméno souboru, který je standardně zobrazen při přístupu k web serveru (složce na web serveru). Obvykle index.htm. Lze zadat i více názvů oddělených mezerou.
- **Adresář se skripty** – soubory v tomto adresáři budou považovány za CGI skripty (spustitelné aplikace)
- **Systémové proměnné pro skripty** – například cesty, které využívají jen spuštěné CGI skripty
- **Uživatelský adresář** – do tohoto pole se zadává cesta k adresáři, ve kterém se generují uživatelské adresáře a stránky (viz Uživatelé).
- **Procházení adresářů** – tento přepínač zapíná vypisování obsahu adresářů, které neobsahují soubor s indexem. To lze využít např. pro snadné zveřejňování souborů.

Stejné parametry se nastavují i pro SSL WWW server. Hodnota **SSL WWW port** je standardně 443.

Použití uživatelských adresářů

Každý uživatel může mít na WWW serveru či SSL WWW serveru svůj uživatelský adresář, kde může prezentovat své informace. Od běžných adresářů na WWW serveru se uživatelské adresáře liší tím, že bez ohledu na jejich fyzické umístění na disku jsou přístupné přes http://server/~jménouživatele, kde „server“ je jméno nebo IP adresa počítače, na kterém je spuštěna LAN SUITE.

Uživatel může modifikovat své stránky těmito způsoby:

- **Kopírováním souborů** na disk do příslušného adresáře za předpokladu, že má tento disk přístupný.
- Může provádět update stránek **protokolem HTTP** např. z prostředí Netscape Navigator po přihlášení odpovídajícím jménem a heslem. Jako cílový adresář je třeba zadat ~jménouživatele/názevadresáře.
- **Protokolem FTP** - uživatel, který není administrátor se přihlásí protokolem FTP k počítači s LAN SUITE, a tím se dostane přímo do svého uživatelského adresáře a může poslat potřebné soubory. Uživatelé s právem administrátora se po přihlášení k FTP serveru na tomto počítači dostanou do hlavního adresáře WWW serveru. Do uživatelských adresářů se dostanou pouze v případě, že je shodně nakonfigurován hlavní adresář pro WWW a uživatelský adresář (standardní nastavení).

Filtrace přístupu k WWW serveru

Přístup k (SSL) WWW serveru můžete omezit i pomocí speciálního IP filtru. Můžete tak specifikovat, ze kterých počítačů je možno na daný web server přistupovat.

Pod sloupcem vstupních polí je zaškrtávací přepínač **Pro přístup k WWW serveru platí IP filtr** (resp. **Pro přístup k SSL WWW serveru platí IP filtr**). Zaškrtnutím přepínače aktivujete pro daný server speciální IP filtr, který lze nastavit po stisku tlačítka **WWW & SSL WWW server IP filtr**.

WWW – FastCGI aplikace

FastCGI aplikace je program, který běží na kterémkoliv počítači přístupném po TCP/IP a je schopen zpracovávat požadavky vyslané z browseru prostřednictvím WWW serveru.

Pro použití FastCGI aplikace je třeba ji zaregistrovat a definovat následující hodnoty:

- **Jméno FastCGI aplikace** – jméno aplikace pod kterým bude uvedena v seznamu.
- **Role** – FastCGI aplikace může obsluhovat více druhů požadavků, může tedy mít více tzv. rolí. Zde uvedeme o kterou roli se jedná. Pokud nemáte speciálně

naprogramovanou aplikaci, je role = 1 (FastCGI aplikace vrací HTML stránku odpovídající dané cestě). Implicitně jsou předdefinované tyto role:

1 responder

2 authorizer

3 filter.

- **URL** – umístění (cesta), kterou uživatel specifikuje ve WWW prohlížeči pro volání této FastCGI aplikace.
- **Spojení (adresa:port)** – je třeba specifikovat počítač a číslo portu, na kterém běží aktuální FastCGI aplikace ve formě host:port. Pokud je aplikace na lokálním počítači, stačí uvést pouze <číslo portu> nebo localhost:<číslo portu>.
- **Cesta k výkonnému souboru** – pokud je výkonný soubor FastCGI aplikace na tomto počítači, může WWW server při svém spuštění tento soubor spustit, aby byl připraven pro zpracování požadavku.
- **Pracovní proměnné** – FastCGI aplikace dostává od WWW serveru kompletní informace o navázaném spojení a typu serveru. Pro práci konkrétního FastCGI skriptu může být potřeba předat mu další vstupní údaje. Zde uveďte jejich výčet ve formátu: *jméno_proměnné=hodnota*. Jednotlivé proměnné oddělte středníkem.

Po vyplnění všech potřebných hodnot stiskněte tlačítko **Přidat**.

Bližší informace o FastCGI najdete na WWW stránce: http://www.fastcgi.com.

WWW – Mapované aplikace

Mapované aplikace umožňují provozování WWW serveru s dynamicky generovaným obsahem stránek – např. pomocí PHP skriptů. Použitím Mapované aplikace lze zajistit, že každá požadovaná stránka s danou extenzí (např. .php) je nejprve zpracována výkonnou aplikací, a teprve výsledek je odeslán na klientský počítač.

Pro použití Mapované aplikace je třeba ji zaregistrovat a definovat následující hodnoty:

- **Jméno aplikace** – jméno aplikace pod kterým bude uvedena v seznamu.
- **URL extenze** – extenze stránek, které mají být zpracovávány výkonnou aplikací (např. .php – extenzi je třeba uvést s tečkou na začátku).
- **Cesta k výkonnému souboru** – kompletní cesta k výkonnému souboru aplikace, který bude zpracovávat stránky s odpovídající extenzí (např. C:\PHP\php.exe).
- **Pracovní proměnné** – Mapovaná aplikace dostává od WWW serveru kompletní informace o navázaném spojení a typu serveru. Pro práci konkrétní Mapované

aplikace může být potřeba předat jí další vstupní údaje. Zde uveďte jejich výčet ve formátu: *jméno_proměnné=hodnota*. Jednotlivé proměnné oddělte středníkem.

Po vyplnění všech potřebných hodnot stiskněte tlačítko **Přidat**.

Příklad

Při požadavku na stránku cenik.php server nejprve spustí příkaz:

„C:\PHP\php.exe C:\LANSUITE\DOCS\cenik.php“ a zpět na klientský počítač odešle až výsledek.

WWW – Aliasy

Pomocí aliasů lze definovat virtuální adresáře, virtuální názvy pro výkonné aplikace i pro konkrétní stránky, a ty pak používat při provozování WWW serveru. Alias slouží nejen ke zkrácení cesty v URL, umožňuje také zveřejňovat nebo spouštět soubory umístěné mimo kořenový nebo skriptový adresář WWW serveru.

Pro použití Aliasu je třeba ho zaregistrovat a definovat následující hodnoty:

- **Alias** – název aliasu, pod kterým bude volán v URL.
- **Cesta** – kompletní cesta do adresáře nebo k výkonnému souboru aplikace, jíž alias v URL zastupuje.
- **Pracovní proměnné** – Alias dostává od WWW serveru kompletní informace o navázaném spojení a typu serveru. Pro práci konkrétního Aliasu může být potřeba předat mu další vstupní údaje. Zde uveďte jejich výčet ve formátu: *jméno_proměnné=hodnota*. Jednotlivé proměnné oddělte středníkem.

Po vyplnění všech potřebných hodnot stiskněte tlačítko **Přidat**.

Virtuální adresář

Pro vytvoření virtuálního adresáře stačí zadat jeho **alias** (např. dokumentace) a do řádky **cesta** skutečnou cestu do tohoto adresáře na disku (např. C:\materialy\dokumentace).

Ve výše uvedeném příkladu bude WWW server při volání URL http://server/dokumentace/navod.htm hledat stránku v adresáři „C:\materialy\dokumentace“ namísto standardního „C:\LANSUITE\DOCS\dokumentace“.

Virtuální stránka

Pro vytvoření virtuální stránky stačí zadat její **alias** (např. manual) a do řádky **cesta** skutečnou cestu k této stránce na disku (např. C:\materialy\dokumentace\manual.htm).

Ve výše uvedeném příkladu vrátí WWW server při volání URL http://server/manual přímo stránku „C:\materialy\dokumentace\manual.htm“.

Virtuální skript

Pomocí aliasu lze také zkrátit i zápis URL pro dynamicky generované stránky. Jako **alias** lze zadat např. cgi a jako **cestu** např. c:\LANSUITE\cgi-bin\602cgi8.exe.

Pak lze místo URL http://server/cgi-bin/602cgi8.exe/edock_db/eDock/login.www psát např. http://server/cgi/edock_db/eDock/login.www.

SSL

Vrstva SSL (Secure Sockets Layer) řeší zabezpečení přenášených dat mezi klientem a serverem a je vložena mezi aplikační protokol a protokol TCP. Přenášená data se pak tedy např. mezi WWW serverem a browserem přenášejí kódovaně pomocí šifrování veřejným a soukromým klíčem. Klíče mohou navíc obsahovat autentifikační informaci od certifikační autority.

Každý server, který komunikuje pomocí SSL má pár klíčů: **veřejný** a **soukromý**.

- **Soukromý klíč** server používá pro zašifrování dat.
- **Veřejný klíč** (certifikát) používají klienti pro dekódování dat. Certifikační autorita (CA) obvykle podepisuje veřejný klíč, aby si klienti mohli být jisti, že komunikují se správným serverem. Nejjednodušší konfigurace SSL spočívá v použití tzv. self-signed certifikátu, kdy server funguje zároveň jako certifikační autorita.

Záložka SSL má dvě podzáložky, na kterých se nastavují hodnoty a parametry používané pro SSL SMTP, SSL POP3 a SSL WWW servery:

Základní údaje

Pokud chcete umožnit uživatelům komunikovat zabezpečeně se SMTP, POP3 nebo WWW serverem, musíte nejprve vytvořit výše zmíněný pár klíčů (soukromý a veřejný).

Vyplňte správně údaje v sekci **SSL informace**:

- **Organizace** – zde napište jméno Vaší firmy
- **Jméno serveru** – zadejte doménové jméno (popř. IP adresu) počítače, na kterém provozujete LAN SUITE (např. www.parler.cz nebo 192.168.1.1).
- **Kontaktní e-mail –** zadejte e-mailovou adresu např. administrátora LAN SUITE
- **Země** – vyberte **Česká republika**

- **Délka klíče** – pro zvýšení bezpečnosti nastavte na **1024 bits** (delší klíč zvyšuje bezpečnost, ale šifrování pak více zatěžuje procesor).

Nyní máte dvě možnosti, jak pokračovat. Záleží na tom, k jakým účelům budete zabezpečení pomocí SSL využívat.

- Pokud budete zabezpečení pomocí SSL využívat pouze „interně“ (např. jen v rámci firmy), můžete si vygenerovat tzv. Self-signed certifikát pomocí volby **Vytvořit a současně podepsat certifikát**.
- Jestliže však chcete Váš web server provozovat „veřejně“ (např. provozovat na něm zabezpečeně elektronický obchod), budete potřebovat certifikát podepsaný nějakou veřejnou certifikační autoritou (např. I.CA, Thawte, apod.).

Jak si „Vytvořit a současně podepsat certifikát“

Pomocí tohoto postupu si zcela ZDARMA vygenerujete a podepíšete certifikát, který Vám umožní využívat zabezpečení pomocí SSL.

Tato metoda je vhodná pouze pro interní využití, neboť vůbec nezaručuje autenticitu serveru, se kterým klient komunikuje. Bezpečnost ale zůstává zachována.

Klikněte na tlačítko **Vytvořit a současně podepsat certifikát**. Vyčkejte dokončení generování klíčů a potvrďte **OK**. Nyní můžete na příslušných konfiguračních kartách zapnout jednotlivě **SSL SMTP server, SSL POP3 server** a **SSL WWW server.**

Provedená nastavení na závěr uložte tlačítkem **Uložit** a restartujte LAN SUITE.

Pozn. Soukromý i veřejný klíč jsou uloženy v souboru SERVER.PEM v adresáři s LAN SUITE. Veřejný klíč je rovněž uložen v souboru SERVER.CRT, který se nachází v hlavním adresáři WWW serveru a který můžete použít pro instalaci certifikátu serveru do seznamu CA do prohlížečů na počítačích uživatelů.

Jak získat certifikát podepsaný certifikační autoritou

Certifikát podepsaný certifikační autoritou využijete, pokud hodláte na svém web serveru provozovat např. elektronický obchod a chcete chránit data, která Vám zákazníci poskytují apod. **Za ověření certifikátu si certifikační autority účtují poplatek.**

Certifikát podepsaný certifikační autoritou zaručuje kromě bezpečnosti i autenticitu serveru, se kterým klient komunikuje. Např. zákazník si tedy může ověřit, že komunikuje opravdu se serverem obchodníka.

Nejprve klikněte na **Vytvořit žádost o podepsání certifikátu (CSR)**. Pomocí volby **Uložit jako** si žádost uložte na bezpečné místo! Potom si žádost příslušným tlačítkem

Zkopírujte do schránky. Žádost o certifikát dopravte k certifikační autoritě. Zpravidla pomocí formuláře na webových stránkách certifikační autority (např. I.CA, Thawte, apod.).

Kliknutím na **OK** uzavřete okno se žádostí. Po obdržení podepsaného certifikátu stiskněte tlačítko **Vložit podepsaný certifikát**. Certifikát vložte do okna nebo jej načtěte ze souboru pomocí tlačítka **Načíst X.509 certifikát ze souboru**. Klikněte na **Uložit certifikát pro 602Pro LAN SUITE**. Nyní můžete na příslušných konfiguračních kartách zapnout jednotlivě **SSL SMTP server**, **SSL POP3 server** a **SSL WWW server**.

Provedená nastavení na závěr uložte tlačítkem **Uložit** a restartujte LAN SUITE.

Pozn. Soukromý klíč vytvořený při generování žádosti o certifikát je uložen v souboru PRIVKEY.PEM. Následně je soukromý i veřejný klíč uložen v souboru SERVER.PEM v adresáři s LAN SUITE. Veřejný klíč je rovněž uložen v souboru SERVER.CRT, který se nachází v hlavním adresáři WWW serveru a který můžete použít pro instalaci certifikátu serveru do seznamu CA do prohlížečů na počítačích uživatelů.

Pro pokročilé

Tyto volby není pro zabezpečení SSL při běžném provozu nijak modifikovat. Slouží pouze pro případné upřesnění konfigurace SSL.

- Volba **Verifikace klientů pomocí certifikátů** zapíná ověřování certifikátů certifikačních autorit klienta (v opačném případě si pouze klient ověřuje certifikát serveru). Další dva přepínače se zpřístupní jen při zaškrtnutí této volby.
- Po aktivaci volby **Vyžadovat certifikát** bude ověření certifikátu klienta považováno za nutnou podmínku k další komunikaci.
- Při zaškrtnutí volby **Verifikovat pouze jednou** bude WWW server akceptovat pouze certifikáty potvrzené přímo certifikační autoritou (nikoliv „podautoritami“).
- Volbou **Nepoužívat žádné certifikáty** zabráníte používání certifikátů pro autentifikaci serveru i klientů.
- Do pole **Certifikátový soubor serveru** se zapisuje přístupová cesta k certifikátovému souboru obsahujícímu privátní i veřejný klíč certifikovaný certifikační autoritou.
- Pokud certifikátový soubor neobsahuje privátní klíč, zapište do pole **Soubor s RSA klíčem** přístupovou cestu k souboru, který tento klíč obsahuje.
- Do pole **Adresář se soubory CA** zapište přístupovou cestu k adresáři se soubory obsahujícími veřejné klíče jednotlivých certifikačních autorit.

- Pokud je k dispozici pouze jediný veřejný klíč certifikační autority, je možné ho specifikovat pomocí pole **Soubor s databází CA**.

Pro komunikaci WWW serveru a prohlížeče se používají různé šifrovací metody. Pomocí sady voleb **Povolené šifrovací metody** specifikujte ty metody, které bude WWW server akceptovat.

Další volby

- **Používat pouze SSL v.2** – LAN SUITE bude s klienty komunikovat pouze pomocí SSL verze 2
- **Používat pouze SSL v.3** – LAN SUITE bude s klienty komunikovat pouze pomocí SSL verze 3
- **Nevytvářet dočasný RSA klíč** – aktivací přepínače bude zakázáno vytváření dočasného RSA klíče pro dosažení vyšší bezpečnosti kódování
- **Kompatibilita s chybami implementací SSL** – ve starších browserech byly chyby implementace SSL. Zaškrtnutím přepínače bude nastaven takový provoz SSL kódování, který umožní tyto chyby eliminovat.

DHCP

Dynamic Host Configuration Protocol (DHCP) poskytuje mechanizmus, pomocí kterého mohou počítače s protokolem TCP/IP automaticky obdržet ze serveru konfigurační parametry – typicky IP adresu, masku podsítě, DNS, jméno domény a další.

Dynamické přidělování přináší kromě zjednodušení administrace IP adres na síti výhodu také v tom, že je potřeba jen tolik IP adres, kolik je skutečně zapnutých počítačů. Protokol DHCP používá protokol UDP, a to na portu 67 a 68.

DHCP je otevřený standard vytvořený Dynamic Host Configuration working group (DHC WG) z Internet Engineering task Force (IETF). Plný popis DHCP je možné najít především v RFC 2131 a dále také v RFC 1531, 1541, 1534, 2132.

Konfigurace

Zapnutí DHCP serveru

Nejprve zaškrtněte volbu **DHPC Server** v levém rohu okna. Dále se ujistěte, že je pro v položce **IP adresa DHCP serveru** zvolena VNITŘNÍ IP adresa (typicky 192.168.x.x).

Nastavení rozmezí IP adres

Nyní musíte definovat **Počáteční IP adresu** a **Koncovou IP adresu**. Doporučujeme použít IP adresy třídy C – typu 192.168.x.x. Nastavte tedy Vaši **Počáteční IP adresu** např. na 192.168.1.10 a **Koncovou IP adresu** na 192.168.1.100 (tím získáte prostor pro 90 počítačů v síti). Jestliže jste zadali adresy klikněte na tlačítko **Přidat**. Pokud chcete označené rozmezí odstranit stiskněte tlačítko **Vymazat**.

Tím, že jste definovali rozsah od 192.168.1.10, jste navíc získali 9 IP adres pro počítače, které nebudou DHCP Server využívat (192.168.1.1 až 192.168.1.9).

Samozřejmě můžete také definovat několik různých nepřekrývajících se rozmezí.

Parametry DHCP

LAN SUITE podporuje velké množství DHCP parametrů a nastavení, ale Vám stačí nastavit pouze dva z nich. Jsou to :

- **1 subnet-mask** - nastavte na hodnotu 255.255.255.0
- **6 domain-name-servers** – zadejte IP adresu počítače s LAN SUITE (např. 192.168.1.1)

Nezapomeňte po vybrání příslušného **DHCP parametru** a zadání jeho hodnoty stisknout tlačítko **Přidat**. Libovolný parametr můžete samozřejmě odstranit pomocí tlačítka **Vymazat**.

Další informace o DHCP, jeho parametrech a hodnotách můžete získat na serveru www.dhcp.org.

LDAP

LDAP (Lightweight Directory Access Protocol) slouží ke sdílení seznamu uživatelů LAN SUITE a jejich e-mailových adres.

Zpřístupnění služby LDAP

Pokud chcete adresářovou službu LDAP zpřístupnit, nejprve na kartě LDAP zaškrtněte volbu **LDAP adresář**.

IP adresy

Pokud je počítač s běžícím programem LAN SUITE Vaší branou do internetu a máte na něm dva síťové adaptéry, pak máte několik možností nastavení voliče **IP adresa**. Můžete:

- vybrat interní IP adresu – informace o uživatelích budou k dispozici jen interně uživatelům stejné sítě

- vybrat IP adresu vnější sítě – informace budou k dispozici jen v této externí síti (někde na internetu, nikoliv ve Vaší lokální síti LAN)
- vybrat položku všechny – informace o uživatelích budou k dispozici jak všem uživatelům internetu, tak ve Vaší lokální síti.

Port

Implicitním portem, na kterém „naslouchá“ služba LDAP je **389**. Pokud tuto hodnotu změníte, bude muset každý klientský program navazující s Vámi LDAP kontakt mít ve své konfiguraci provedenou stejnou změnu.

Jméno administrátora a heslo

Do položky **Administrátor** a **Heslo** zadejte jméno a heslo pro správu Vašeho LDAP serveru pomocí externích programů (zpravidla se nepoužívá, ale toto je třeba vyplnit).

Báze

Do pole **Báze** zadejte výchozí bod pro LDAP server. Doporučujeme zadat alespoň zemi (např. c=CZ).

Konfigurace Outlook Express jako LDAP klient

Zvolte v menu **Nástroje** – **Účty** a po stisku tlačítka **Přidat** vyberte **Adresářová služba**. Do položky **Adresářový server Internetu (LDAP)** zadejte IP adresu počítače s LAN SUITE. Doporučujeme nekontrolovat adresy pomocí adresářové služby.

Na závěr vyberte právě zadanou adresářovou službu a v jejích vlastnostech na záložce **Upřesnit** zadejte jako **Výchozí bod hledání** c=CZ.

Nyní můžete vyhledávat pomocí této služby e-mailové adresy volbou „Najít osoby“ buď v programu Outlook Express nebo přímo z Windows přes menu Start-Najít-Osoby.

Administrace

Kromě přímé administrace na konzoli je možné LAN SUITE spravovat vzdáleně pomocí browseru, a to jak z počítače na lokální síti tak z internetu.

Pokud chcete zabezpečit přístup do konfigurace z menu v okně LAN SUITE, zaškrtněte volbu **Omezit přístup ke konfiguraci přímo z programu pouze na administrátory**. Pak bude při každém pokusu o vstup do Konfigurace pro odborníky i do Průvodce konfigurací vyžadováno zadání jména a hesla uživatele s administrátorskými právy.

Vzdálená administrace pomocí browseru

Parametry související se správou LAN SUITE se nastavují na záložce **Administrace**. Vzdálenou administraci pomocí browseru povolíte zaškrtnutím volby **Povolit dálkové ovládání pomocí browseru**. Vzdálená administrace je pak dostupná na adrese http://adresaserveru/admin.

V sekci **Přihlášení ke vzdálenému ovládání** můžete upřesnit míru zabezpečení vzdálené administrace:

- **žádné – volný vstup** – do vzdálené administrace bude mít přístup kdokoliv!
- **vyžadováno přihlášení uživatele** – pro vstup bude třeba zadat uživatelské jméno a heslo libovolného uživatele LAN SUITE
- **přístup pouze pro administrátory** – vstup do vzdálené administrace budou mít pouze uživatelé LAN SUITE s právy administrátora (***doporučujeme***).

Bez ohledu na výše zmíněné nastavení, mohou pouze administrátoři pomocí vzdálené administrace přistupovat na „záložku“ **Uživatelé**.

Použití zvláštního portu nebo SSL

Implicitně je vzdálené ovládání a administrace součástí web serveru (je spuštěno na stejném portu a nachází se ve virtuálním adresáři /ADMIN). Z bezpečnostních důvodů je možné vzdálené ovládání a administraci přesunout na jiný port a případně vyžadovat použití zabezpečeného protokolu HTTPS.

Po zaškrtnutí volby **Použít zvláštní port pro vzdálené ovládání** zadejte číslo portu, na kterém chcete vzdálené ovládání provozovat (např. 8081).

Pokud požadujete, aby se ke vzdálenému ovládání dalo připojit pouze pomocí zabezpečeného protokolu HTTPS, zaškrtněte i volbu **Použít SSL protokol**.

Poznámka: Na jakou adresu je třeba se připojit pro přístup k vzdálené administraci ukazuje dynamicky text psaný kurzívou umístěný pod těmito volbami.

Update obsahu WWW serveru pomocí FTP

Stránky jsou na WWW serveru uloženy v adresářích definovaných na záložce **WWW** v konfiguraci LAN SUITE. Jejich aktualizaci lze provádět nejen přímou prací se soubory na disku (standardně v podadresáři **DOCS**), ale i vzdáleně pomocí protokolů HTTP a FTP.

Aktualizaci obsahu WWW serveru pomocí protokolu FTP povolíte zaškrtnutím volby **Povolit FTP update WWW serveru na portu X** (standardně 21). Toto nastavení neovlivní možnost provádět update stránek pomocí protokolu HTTP.

Pozn. Pokud potřebujete na počítači s LAN SUITE provozovat jiný FTP server, změňte hodnotu portu (např. na 8021).

Je několik způsobů, jak obsah WWW serveru aktualizovat

- HTML stránky lze do LAN SUITE poslat jakýmkoliv FTP klientským programem.
- Používáte-li prohlížeč Microsoft Internet Explorer, pak můžete použít Web Publishing Wizard (standardně ve Windows98, MSIE 4.0 a vyšší, FrontPage) – stránky se pošlou pomocí protokolu FTP.
- Používáte-li prohlížeč Netscape Navigator, pak využijte jeho HTML editor (Netscape Composer) a pomocí ikonky Publish proveďte aktualizaci stránek – protokolem HTTP PUT.

Kdo může stránky aktualizovat

Uživatel, který není administrátor, může aktualizovat pouze svoje osobní stránky. Uživatelé s právem administrátora se po přihlášení k FTP serveru na tomto počítači dostanou do hlavního adresáře WWW serveru. Do uživatelských adresářů se dostanou pouze v případě, že je shodně nakonfigurován hlavní adresář pro WWW a uživatelský adresář.

Další informace k problematice konfigurace WWW serveru a uživatelských stránek naleznete v kapitole **Uživatelé** a také **WWW**.

Další zabezpečení vzdálené administrace

Pro zvýšení bezpečnosti můžete přístup ke vzdálené administraci i FTP update obsahu WWW serveru omezit navíc pomocí speciálního IP filtru zaškrtnutím volby **Pro přístup k dálkovému ovládání a FTP update platí IP filtr**, který lze nastavit po stisku tlačítka **IP filtr dálkového ovládání a FTP update**.

Např. přístup ke vzdálené administraci a FTP update pouze v rámci Vaší lokální sítě povolíte zpravidla zadáním IP adresy 192.168.1.1 a masky 255.255.255.0 (přístup bude povolen ze všech počítačů s IP adresou 192.168.1.x).

Zprávy

Zprávy o činnosti serveru se standardně vypisují do okna serveru a mohou se zapisovat i do souboru na disk. LAN SUITE také umožňuje zaznamenávání činnosti serveru WWW, HTTP proxy a firewallu do souborů ve formátu W3C pro pozdější analýzu externími programy.

Zprávy o činnosti serveru se mimo souborů standardně vypisují do okna programu. Počet řádků, které se uchovávají v paměti (a jimiž lze v okně listovat) můžete nastavit v poli **Počet řádek terminálového bufferu**.

Zprávy o činnosti serveru se mohou také zapisovat do tzv. log souboru. Po zaškrtnutí volby **Zapisovat zprávy do souboru SDDMMRRI.LOG** se pro každý den generuje zvláštní soubor, kde *dd* je den, *mm* měsíc a *rr* poslední dvojčíslí letopočtu. Každý takový soubor se udržuje na disku po dobu stanovenou v poli **Soubory se zprávami mazat po X dnech**, a pak se vymaže.

Další statistický log soubor se automaticky vytváří pro poštovní a faxový provoz (soubor **LANSUITE.CSV**). Zaznamenávají se do něj hlavičky odesílaných a přijímaných zásilek (SMTP e-mailů a faxů). Tento soubor je ve formátu CSV a lze ho snadno načíst např. do tabulkového procesoru. Velikost tohoto souboru je omezena v poli **Max. velikost souboru se statistikou faxů v kB**. Po dosažení limitní hodnoty je CSV soubor automaticky zkrácen o 10 procent a logování pokračuje.

V sekci **Zapisovat zprávy od** můžete zaškrtnout, které zprávy se mají zapisovat do hlavního log souboru. Monitorovat lze činnost následujících částí LAN SUITE:

- **WWW/Proxy**
- **SOCKS serveru**
- **Navazování dial-up připojení**
- **SMTP serveru**
- **POP3 serveru/výběru POP3 schránek**
- **Vyřizování požadavků na DNS**
- **DHCP serveru**
- **LDAP adresáře**
- **Fax serveru**

W3C – rozšířený formát log souboru

Většina webových serverů volitelně umožňuje zaznamenávat svoji činnost podle standardu W3C.

Viz http://www.w3.org/Daemon/User/Config/Logging.html#common-logfile-format

LAN SUITE může zaznamenávat v tomto formátu průběh různých operací podle aktuálního nastavení voleb v sekci **Zprávy od HTTP proxy a WWW serveru ve formátu W3C** resp. **Zprávy od firewallu**. Logy jsou zaznamenávány do následujících souborů:

- W3CA.LOG – log WWW serveru
- W3CP.LOG – log HTTP proxy serveru
- W3CC.LOG – log HTTP proxy cache
- FW.LOG – log o činnosti firewallu

W3C logy jsou zaznamenávány ve formátu, který je čitelný pomocí externích aplikací. Proto má každý záznam hlavičku, která obsahuje mj. informaci o typu záznamu.

Pro analýzu těchto logů existuje řada komerčních i volně dostupných programů. Např.:

- http://kresch.com/resources/Freeware/Log_Analyzer/
- http://www.webattack.com/Freeware/webpublish/fwlogalyzer.shtml

NT služba

Tato záložka je dostupná pouze v případě, že je LAN SUITE provozována pod operačním systémem Windows NT/2000/XP, a umožňuje provoz LAN SUITE jako služby.

Úvodní text na záložce konstatuje, zda je v daném okamžiku LAN SUITE nainstalována jako služba či nikoli. Další prvky dialogu umožňují program jako službu instalovat nebo případně upravit některá nastavení služby:

- **Parametry příkazové řádky** – zde se vkládají parametry příkazové řádky, která bude použita při spuštění služby.
- **Způsob spouštění služby** – zde je možno nastavit, že se služba má spouštět automaticky při každém startu systému, nebo že ji bude ručně spouštět přímo uživatel z Ovládacích panelů ve Windows, nebo že se má služba dočasně deaktivovat.
- **Účet služby** – při startu služby se jí přiřadí účet, který určuje, jaká práva může služba využívat. Pokud bude LAN SUITE potřebovat např. přístup na disky na jiném počítači, můžete zde nastavit účet uživatele s právem přístupu na tyto disky.
- **Službu startovat až po označených službách** – někdy může být nutné zajistit, aby před startem LAN SUITE již pracovala nějaká jiná služba, případně více služeb. Zde ji můžete zaškrtnout a systém spustí LAN SUITE až po naběhnutí této označené služby (služeb).

Po nastavení údajů můžete LAN SUITE nainstalovat jako službu tlačítkem **Instalovat službu**. Pokud je služba již nainstalována, můžete ji po provedení změn rekonfigurovat tlačítkem **Reinstalovat službu**. Tlačítko **Zrušit službu** můžete použít k odinstalování služby.

Win9x/ME služba

Tato záložka je dostupná pouze v případě, že je LAN SUITE provozována pod operačním systémem Windows 9x/ME, a umožňuje provoz LAN SUITE jako služby resp. jen její automatické spuštění po startu Windows.

Úvodní text na záložce konstatuje, zda je v daném okamžiku LAN SUITE nainstalována jako služba či nikoli. Další prvky dialogu umožňují program jako službu instalovat nebo případně upravit některá nastavení služby:

Pojem služba má ve Windows 9x/ME podstatně menší význam než ve Windows NT. Jedná se pouze o automatické spuštění daného programu ihned po startu Windows s tím, že jeho ikona je skrytá v pravém spodním rohu obrazovky (SysTray). Dále už se program chová jako standardní aplikace Windows.

Do pole **Parametry příkazové řádky** můžete zapsat parametry příkazového řádku, které mají být použity při spuštění služby. LAN SUITE nastavíte jako službu tlačítkem **Instalovat službu**. Tlačítko **Zrušit službu** můžete použít k odinstalování služby.

Klientské programy

SendFax

Program SendFax je doplněk LAN SUITE, který Vám umožní ze stanic v síti odesílat faxy z libovolné aplikace ve Windows stejně snadno, jako když tisknete na tiskárnu.

Instalace

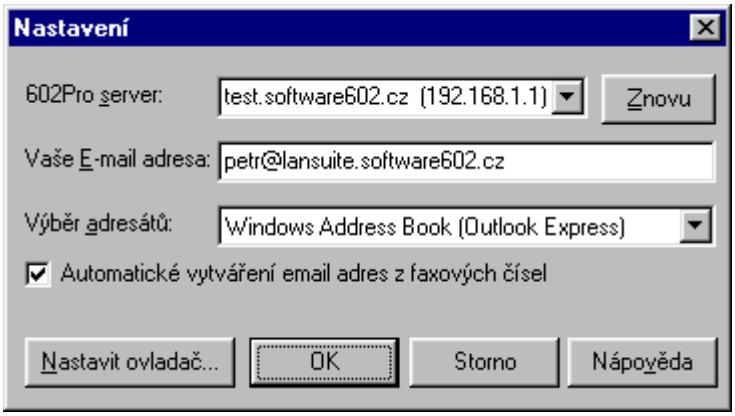
Tento program je třeba nainstalovat na všechny počítače, ze kterých budete chtít výše uvedeným způsobem faxovat.

1) Spusťte instalaci programu SendFax (ze staženého souboru nebo z CD).
2) Postupujte podle pokynů průvodce a po zadání jména a společnosti zvolte cílový adresář.
3) Po potvrzení vyčkejte na dokončení instalace.

Pozn. Faxy ale můžete odesílat i bez programu SendFax, a to přímo z programu pro práci s elektronickou poštou. Stačí odeslat e-mail (třeba i s připojenými soubory) na adresu číslo@fax. Obsah e-mailu i souborů LAN SUITE automaticky převede a odfaxuje na dané číslo (viz Fax).

Konfigurace

SendFax je třeba před prvním použitím nakonfigurovat. Po instalaci ho spusťte pomocí ikony na ploše. Nastavit lze tři (resp. čtyři) parametry:



- **602Pro Server** – adresa počítače, na němž běží LAN SUITE. Tuto adresu program vyhledá sám (hledá počítače s běžící LAN SUITE), uživatel ji může případně přepsat nebo si vybrat tu správnou z více nabízených.

- **Vaše e-mail adresa** –e-mailová adresa daného uživatele uvedená v konfiguraci LAN SUITE.
- **Seznamy** – program SendFax si neudržuje vlastní seznamy faxových adresátů. Ty je třeba udržovat v jednom z nabízených klientských programů – buď Outlook Express nebo Outlook 9x/2000/XP, případně Simple MAPI klient (např. Netscape Messenger).
- **Automatické vytváření e-mail adres z faxových čísel** – Pokud používáte Outlook Express, můžete si faxová čísla zapisovat přímo do příslušných položek v Kontaktech (fax do zaměstnání, fax domů), a ty pak využít při posílání faxových zásilek. Tuto funkci můžete zapnout zaškrtnutím políčka v konfiguračním dialogu programu SendFax.

Pozn. Do konfigurace programu SendFax se také dostanete po jeho spuštění s parametrem **/options** (např. M602SNDF.EXE /OPTIONS).

Nastavení vlastností ovladače Fax602

Další parametry lze nastavit v rámci vlastností ovladače **Fax602**. Ve Windows9x/ME tyto parametry nastavíte ve **Vlastnostech** tiskárny Fax602 v Ovládacích panelech. Ve Windows NT/2000 se tyto parametry nastavují až těsně před tiskem (volba **Vlastnosti** a **Upřesnit**).

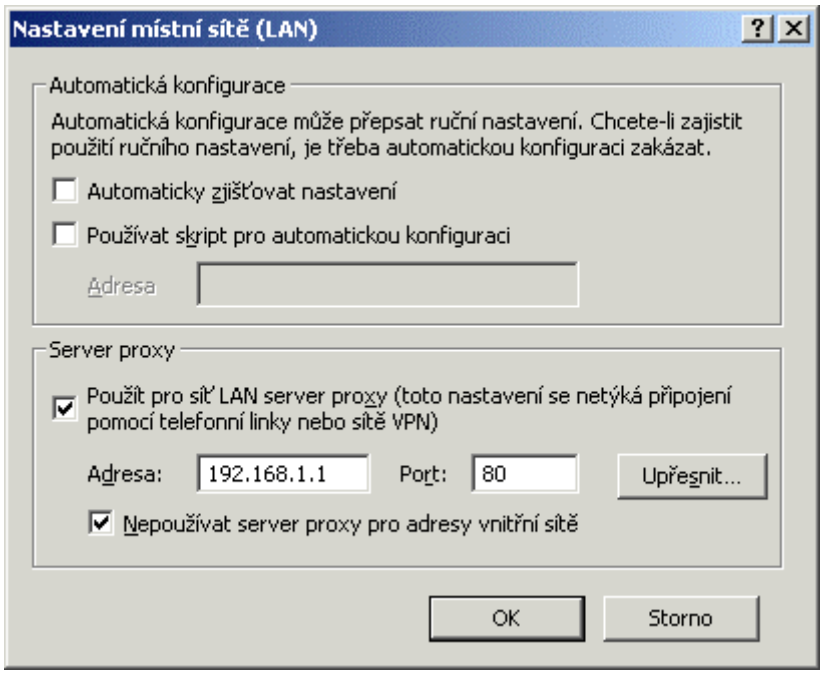
- můžete vyžadovat zachování délky stránky – fax vytiskne všechny strany stejně dlouhé i prázdným místem,
- můžete vyžadovat zobrazení náhledu faxu před odesláním,
- můžete specifikovat rozlišení (standardní 200x100 dpi nebo vysoké 200x200 dpi) a rozklad barev.

Internet Explorer

Postup nastavení programu Internet Explorer pro spolupráci s LAN SUITE.

1) Spusťte Internet Explorer.
2) V menu vyberte **Nástroje**, **Možnosti Internetu …**,
3) klikněte na záložku **Připojení**,
4) stiskněte **Nastavení místní sítě**,
5) zaškrtněte **Použít pro síť LAN server proxy** a vyplňte IP adresu počítače s LAN SUITE (např. 192.168.1.1) a port 80. Zaškrtněte také **Nepoužívat server proxy pro**

adresy vnitřní sítě. Ujistěte se, že nejsou zaškrtnuty žádné volby v sekci Automatická konfigurace.



6) Potvrzujte **OK**, dokud se nevrátíte na základní obrazovku browseru.

Obecný SMTP/POP3 poštovní klient

Pro práci s elektronickou poštou v rámci LAN SUITE můžete použít libovolný poštovní klientský program podporující protokol SMTP/POP3.

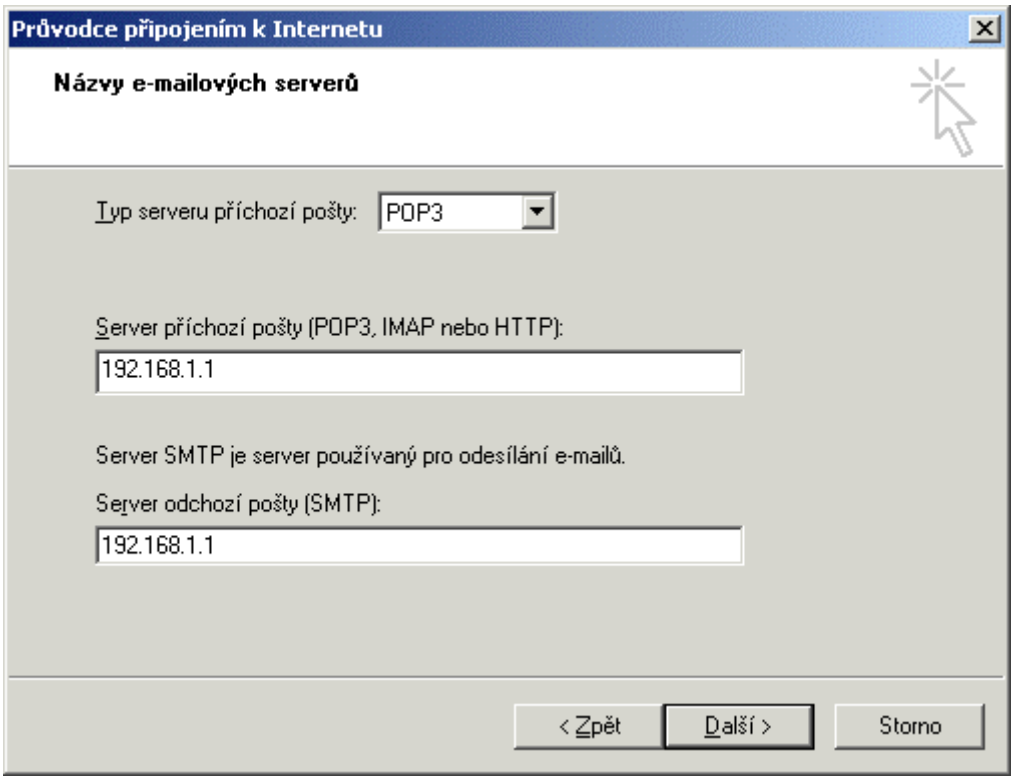
Pro odesílání pošty je třeba nastavit adresu SMTP serveru jako IP adresu počítače s LAN SUITE (např. 192.168.1.1) a zadat vlastní e-mailovou adresu uživatel@doména dle konfigurace LAN SUITE (např. karel4@firma.cz).

Pro příjem pošty je třeba nastavit adresu POP3 serveru jako IP adresu počítače s LAN SUITE (např. 192.168.1.1), případně zvolit typ serveru POP3. Dále je třeba zadat přihlašovací jméno (název účtu) a heslo – odpovídá jménu uživatele a heslu v LAN SUITE.

Outlook Express

Postup nastavení programu Outlook Express pro spolupráci s LAN SUITE.

1) Spusťte Outlook Express. Postupujte podle průvodce nebo z menu **Nástroje** vyberte **Účty** – **Přidat** – **Pošta…**.
2) Do řádku **Zobrazované jméno** vyplňte Vaše plné jméno a klikněte na **Další**.
3) Vyberte, že již máte e-mailovou adresu a vyplňte ji do řádku **E-mailová adresa** a klikněte na **Další**.

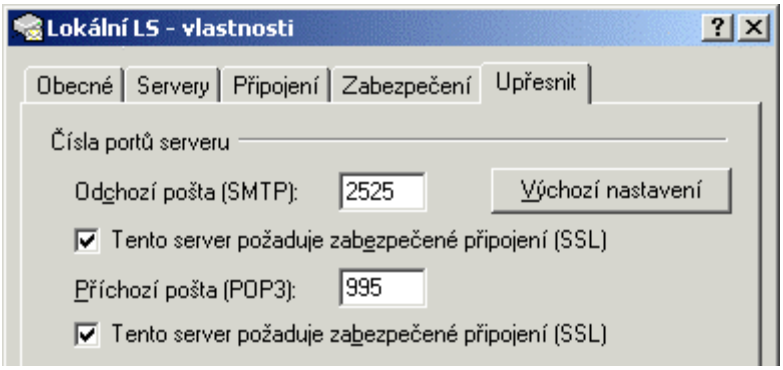


4) Typ serveru příchozí pošty nastavte na **POP3** a **Server příchozí pošty** i **Server odchozí pošty** nastavte na IP adresu počítače s LAN SUITE (např. 192.168.1.1) a klikněte na **Další**.
5) Nyní vyplňte **Název účtu** (uživatelské jméno v LAN SUITE) a **Heslo** (stejné jako v LAN SUITE) a klikněte na **Další**.
6) Stiskněte tlačítko **Dokončit**.

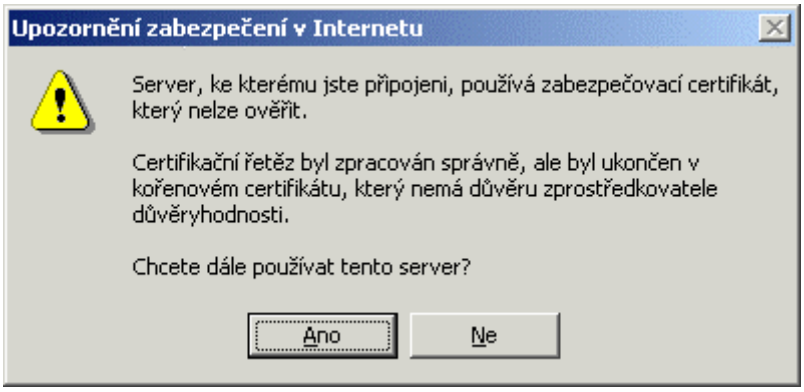
Nastavení Outlook Express pro SSL SMTP/POP3

Zabezpečení SMTP a POP3 serveru pomocí SSL zabraňuje mj. „odposlechu“ Vašeho hesla i Vašich e-mailů na cestě mezi SSL SMTP/POP3 serverem a Vaším počítačem. Pokud chcete, aby práce s Vaší POP3 schránkou a komunikace se SMTP serverem probíhala šifrovaně pomocí SSL, je třeba toto nastavit jak v LAN SUITE, tak v klientském programu.

V programu **Outlook Express** je ještě třeba kromě standardního nastavení ve vlastnostech poštovního účtu na záložce **Upřesnit** zaškrtnout pod čísly portů pro SMTP i POP3 volby **Tento server požaduje zabezpečené připojení (SSL)**. Dále u SMTP přepsat číslo portu na **2525** a provedená nastavení potvrdit **OK**.



Pokud administrátor LAN SUITE sám vygeneroval a podepsal SSL klíče, zobrazí se při přístupu z Outlooku Express k SSL SMTP/POP3 serveru následující hlášení:

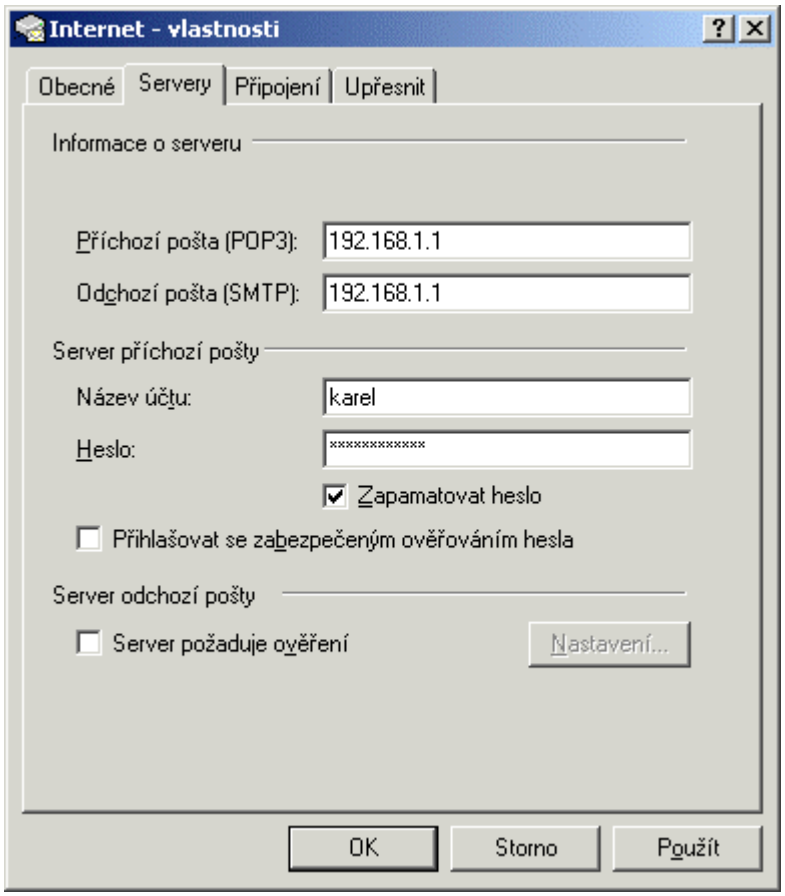


Pozn. V programu Netscape Messenger je SSL přenos implementován jako extenze protokolu SMTP, což bohužel není s LAN SUITE 2003 kompatibilní.

Outlook 9x/2000/XP

Postup nastavení programu Outlook 9x/2000/XP pro spolupráci s LAN SUITE.

1) Spusťte Outlook 9x/2000/XP.
2) Vyberte **Nástroje – Služby**.
3) Do kolonky **Poštovní účet** napište nějaký popisný název.
4) Do kolonky **Jméno** vyplňte jméno, které se bude objevovat u Vámi odeslaných zpráv.
5) Kolonku **Organizace** můžete ponechat prázdnou.
6) Do řádku **E-mailová adresa** vyplňte Vaši e-mailovou adresu, stejnou adresu vyplňte i do řádku **Adresa pro odpovědi**.
7) Přejděte na záložku **Servery**.
8) Do řádků **Příchozí pošta** i **Odchozí pošta** vyplňte IP adresu počítače s LAN SUITE (např. 192.168.1.1).



Ujistěte se, že je vybrána volba přihlašovat se pomocí jména a hesla. Nyní vyplňte **Název účtu** (uživatelské jméno v LAN SUITE) a **Heslo** (stejné jako v LAN SUITE).

WEB klient – přístup do pošty pomocí browseru

WEB klient umožňuje uživatelům přistupovat ke svým poštovním schránkám v LAN SUITE i přes internet pomocí browseru. Veškerá komunikace mezi browserem (uživatelem) a LAN SUITE probíhá pomocí protokolu HTTP nebo zabezpečeného protokolu HTTPS.

Přihlášení

Po spuštění browseru zadejte adresu počítače, kde běží LAN SUITE, ve formátu např. http://192.168.1.1/mail nebo http://www.adresaserveru.cz/mail.

- Zadejte Vaše uživatelské **Jméno.**
- Zadejte Vaše **Heslo.**
- Stiskněte tlačítko **Přihlásit**.

Pokud jste již přihlášeni a neprovedete žádnou operaci po dobu delší než 60 minut, budete automaticky odhlášeni.

Základní okno WEB klienta

Základní okno WEB klienta se skládá ze dvou hlavních částí, přičemž v horní části okna je vždy zobrazeno menu a dolní část se mění podle zvolené funkce.

V menu jsou na výběr následující příkazy:

- Nový dopis
- Došlá pošta – zobrazí se vždy po přihlášení.
- Odeslaná pošta
- Adresy
- Nastavení
- Nápověda
- Odhlášení – slouží k odhlášení od serveru.

Došlá pošta

V okně **Došlá pošta** jsou zobrazeny všechny přijaté zásilky včetně faxů. V levé části okna je zobrazen strom přihrádek a v pravé části pak seznam zásilek. Hlavní přihrádka se jmenuje **Došlá pošta** a lze v ní vytvořit další přihrádky pomocí volby **Přihrádka – Založit novou**. Zadaný název nové přihrádky je třeba potvrdit tlačítkem **Potvrdit**.

Před každou zásilkou je zaškrtávací políčko, které umožňuje danou zprávu (zprávy) označit a dále s ní (nimi) pracovat – odstranit nebo zkopírovat, přesunout do přihrádky. Pokud zaškrtnete políčko zcela nahoře, označíte/odznačíte všechny zprávy.

U každé zprávy jsou zobrazeny tři informace:

- Datum a čas
- Odesílatel
- Věc

Kliknutím na daný nápis můžete seznam zásilek setřídit podle tohoto parametru.

Zásilku otevřete kliknutím na odkaz, který tvoří vždy atribut, podle kterého je seznam zásilek setříděný.

Seznam zásilek můžete znovu načíst pomocí tlačítka **Obnovit**  , které je zobrazeno před názvem aktuální přihrádky. Seznam zásilek není automaticky aktualizován.

Pokud máte zásilek mnoho, jsou v dolní části okna zobrazeny dvě šipky, pomocí kterých lze procházet seznam zásilek.

Pozn. V seznamu došlé pošty jsou zobrazovány pouze ty zásilky, které se nacházejí na serveru, tzn. nebyly staženy a vymazány ze serveru pomocí POP3 klienta (např. Outlooku Express).

Odeslaná pošta

V levé části okna je vidět seznam složek a v pravé části okna seznam zásilek ve zvolené složce. Ve složkách jsou pouze zásilky přihlášeného uživatele. Seznam složek obsahuje:

- Zásilky k odeslání – zásilky čekající ve frontě na odeslání nebo právě odesílané.
- Faxy k odeslání – faxy čekající ve frontě na odeslání nebo právě odesílané.
- Odeslané zásilky – fyzicky odeslané zásilky.
- Odeslané faxy – fyzicky odeslané faxy.

Pokud má přihlášený uživatel administrátorská práva, má k dispozici navíc složky, které obsahují seznamy zásilek od všech uživatelů, a tak může spravovat frontu zásilek k odeslání.

- Všechny zásilky k odeslání
- Všechny faxy k odeslání
- Všechny odeslané zásilky
- Všechny odeslané faxy

Zásilky a faxy čekající ve frontě na odeslání můžete **Odložit** a pozdržet tak jejich odeslání nebo opět **Oživit**; případně můžete zásilku z fronty **Vymazat**. Obsah čekající zásilky si můžete i prohlédnout po kliknutí na odkaz (podle toho, jak je seznam setříděn). Zobrazenou zásilku zavřete tlačítkem **Zavřít**.

Zobrazený seznam zásilek můžete znovu načíst pomocí tlačítka **Obnovit**  , které je zobrazeno před názvem aktuální složky. Seznam zásilek není automaticky aktualizován.

Nový dopis

Okno pro přípravu nového dopisu obsahuje následující prvky:

- **Od:** – pokud má uživatel nadefinované aliasy, může zvolit e-mailovou adresu, pod kterou chce dopis odeslat.
- **Komu:** – do řádku můžete zapsat adresu adresáta(ů) nebo si po kliknutí na odkaz zobrazit seznamy adresátů.
  Faxové číslo můžete také zadat přímo, a to ve formátu např. F:+420222011218.
  Adresáty můžete z dopisu vyřazovat pomocí odkazu **Vyřadit**.
- **Na vědomí:** – adresáti na vědomí (CC); lze je zadat ručně nebo vybrat ze seznamu, který se zobrazí po kliknutí na odkaz.
- **Připojit soubory:** – po kliknutí se zobrazí okno pro výběr a připojení souborů.
- **Věc:** – věc (předmět) dopisu.
- Text e-mailu nebo faxu napište do velkého zadávací okna.
- **Připojit podpis** – připojí na konec dopisu textový podpis nadefinovaný v **Nastavení**.
- **Slepé kopie** – Pokud je zadáno více adresátů (nezáleží na tom, zda v položce Komu nebo Na vědomí) a zaškrtnete tuto volbu, nebude hlavička zásilky obsahovat ostatní adresáty (adresáti o sobě nebudou navzájem vědět).
- **Doporučeně** – zásilka (e-mail) bude odeslána jako doporučená. Příjemce bude vyzván k potvrzení přijetí této zásilky a odesílatel toto potvrzení obdrží jako e-mail. **Pozn.** Příjemce nemusí přijetí zásilky potvrdit, aby si ji mohl přečíst.
- **Formát** – můžete zvolit formát odesílané zásilky a souborů dle standardu:
  - MIME ISO Latin2 – doporučujeme
  - MIME bez diakritiky – v textu dopisu bude odstraněna diakritika
  - RFC822 + UUEncode – starší formát zásilek

Připojení souborů

Při přípravě nového dopisu se po kliknutí na odkaz **Připojit soubory** zobrazí okno pro výběr a připojení souborů.

1) Tlačítkem **Procházet…**otevřete okno pro výběr souboru. Vyberte soubor a výběr potvrďte tlačítkem **Otevřít**.

2) Připojte soubor tlačítkem **Připojit**.

Tento postup můžete dle potřeby opakovat pro další připojované soubory. Pokud chcete některý soubor ze seznamu připojovaných souborů odstranit, označte ho a klikněte na tlačítko **Vyřadit** označené. Nakonec potvrďte seznam připojených souborů tlačítkem **OK**.

Adresy

Okno se seznamy adresátů má dvě horizontálně rozdělené části. V horní části jsou hlavní seznamy:

- **Lokální uživatelé pošty** – seznam všech uživatelů, kteří jsou založeni v LAN SUITE na kartě Uživatelé.
- **Vlastní seznamy** – každý uživatel si může vytvořit své vlastní seznamy adresátů.
- **Veřejné seznamy** – tyto seznamy jsou společné, pro všechny uživatele. Pouze uživatelé s právy administrátora je ale mohou spravovat.
- **Najít osoby…** – Tato volba umožňuje vyhledávat osoby pomocí adresářových služeb definovaných na počítači s LAN SUITE.

Lokální uživatelé pošty

Kliknutím na jméno uživatele otevřete okno pro přípravu nového dopisu tomuto uživateli. Pomocí zaškrtávacích políček můžete vybrat i více uživatelů, pak použijte tlačítko **Poslat dopis**.

Práce s vlastními a veřejnými seznamy

Práce s vlastními a veřejnými seznamy je podobná. Vlastní seznamy si mohou uživatelé upravovat sami, zatímco Veřejné seznamy mohou modifikovat pouze uživatelé s právy administrátora.

- **Poslat dopis** – pošle dopis na vybrané uživatele/seznamy
- **Nový seznam** – založí nový seznam
- **Vymazat** – vymaže vybrané uživatele/seznamy
- **Storno**

Seznam otevřete kliknutím na jeho název. Pokud máte otevřen nějaký seznam, mate navíc k dispozici následující možnosti:

- **Nový adresát** – slouží k přidání adresáta do seznamu
- **Přejmenovat seznam** – slouží k přejmenování aktuálně otevřeného seznamu
- **Zavřít** – zavře otevřený seznam

Kliknutím na jméno adresáta otevřete okno pro přípravu nového dopisu tomuto uživateli. Kliknutím na jeho adresu ji můžete upravit, příp. přejmenovat adresáta.

Nastavení

V horní části okna **Nastavení** jsou následující tlačítka:

- **Informace** – zobrazí informace o přihlášeném uživateli a verzi WEB klienta
- **Přihlašovací heslo** – slouží ke změně přihlašovacího hesla uživatele
- **Automatické třídění došlé pošty** – definuje pravidla pro automatické zpracování příchozí pošty
- **Povolit/Zakázat službu „Následuj mě“** – aktivuje/deaktivuje příslušná pravidla automatického zpracování došlé pošty

V dolní části okna jsou další volby a nastavení:

- **Zobrazit čas načtení došlé pošty** – v okně došlé pošty zobrazuje čas posledního načtení seznamu zásilek
- **3-řádkový náhled neprohlédnutých zásilek** – zapne/vypne tento náhled
- **Zvýraznit odkazy k dokumentům na internetu** – rozpoznané odkazy v zásilkách budou aktivní. Pro jejich zobrazení bude stačit na ně kliknout myší.
- **Šířka řádky** – maximální zobrazovaný počet znaků na řádce
- **Zásilek na stránku** – počet zásilek v seznamu zobrazovaný na jedné stránce
- **Hlavička prohlížené zásilky** – hlavičku prohlížené zásilky si lze nechat zobrazovat jako žádnou, základní nebo plnou
- **Textový podpis** – lze definovat podpis, který se bude připojovat na konec každé odesílané zásilky
- **Formát internet zásilek** – přednastavený formát pro odesílání internetových zásilek (lze následně měnit u každé zásilky)
- **Výchozí seznam adresátů** – nastavený seznam adresátů se zobrazí jako první při výběru Komu a Na vědomí u nového dopisu
- **ZIPovat připojené soubory odesílané zásilky** – soubory, které připojíte k zásilce, budou nakonec odeslány jako jeden komprimovaný soubor
- **ZIPovat připojené soubory prohlížené zásilky** – soubory připojené k zásilce jsou komprimovány pro snadnější stahování. Všechny připojené soubory lze pak stáhnout v jednom ZIP archivu nebo jednotlivě.

- **Kontrolovat připojené soubory odesílané zásilky*** – každý soubor připojovaný k novému dopisu bude kontrolován na přítomnost počítačových virů.
- **Kontrolovat připojené soubory prohlížené zásilky*** – každý soubor připojený k došlé zásilce bude kontrolován na přítomnost počítačových virů (při otevření zásilky).

*Pokud používáte LAN SUITE Antivirus Edition, budou soubory kontrolovány technologií BitDefender™. V opačném případě je třeba, aby byl na počítači s LAN SUITE nainstalován antivirový systém AVG verze 6.0 a vyšší.

Automatické třídění došlé pošty

Nové pravidlo pro automatické zpracování přidáte stiskem tlačítka **Přidat nový filtr**. Již zadané pravidlo můžete modifikovat stiskem tlačítka **Upravit** u příslušného filtru nebo vymazat stiskem ✕. Pravidla jsou na zásilky aplikována postupně shora dolů. Pořadí zobrazených pravidel lze měnit pomocí šipek vedle příslušného pravidla.

U každého pravidla se definuje, kdy bude prováděno – v části **Provádět**, za jakých podmínek – v části **Podmínky** a co bude provádět – v části **Akce**.

Provádět

Dané pravidlo může být aplikováno **Vždy** nebo **Pouze při zapnuté službě „Následuj mě“** (nebo při vypnuté). Provádění pravidla lze také zabránit volbou **Nikdy**.

Pozn. Pokud zvolíte provádění **Pouze při zapnuté službě „Následuj mě“**, bude se dané pravidlo aplikovat pouze v případě, že v **Nastavení** stisknete tlačítko **Povolit službu „Následuj mě“** (tlačítko se změní na **Zakázat službu „Následuj mě“**).

Podmínky

V této části můžete definovat podmínky, které musí splňovat zásilka, aby na ní bylo dané pravidlo aplikováno. Pokud zde nic nezaškrtnete, bude pravidlo aplikováno na všechny zásilky (dle nastavení v části **Provádět**).

Po zaškrtnutí některé volby zadejte její hodnotu. Lze používat i zástupné znaky ? a *. Zadání lze omezit zaškrtnutím a vyplněním hodnoty ve sloupci **kromě**.

Příklad: Pokud nevyplníte odesílatele a zaškrtnete **kromě** a zadáte petr@firma.cz, aplikuje se dané pravidlo **na všechny zásilky kromě** zásilek od uvedeného odesílatele.

Akce

Pokud jsou tedy splněny podmínky nastavené v části **Provádět** a zásilka splňuje parametry zadané v části **Podmínky**, provede se se zásilkou nastavená akce:

- **Nic** – spolu s volbou **Po provedení akce vymazat** lze použít pro automatické mazání určitých zásilek.
- **Přesunout do přihrádky** – Pokud jste si vytvořili alespoň jednu přihrádku v došlé poště, můžete nechat zásilky do této přihrádky automaticky přesouvat.
- **Přeposlat** – Zásilky mohou být automaticky postupovány na danou adresu(y), v případě více adres i jako slepé kopie.
- **Odpovědět** – Server vygeneruje automatickou odpověď a odešle ji na adresu odesilatele původní zásilky. Text odpovědi zadejte do editačního okénka. Na došlé faxy není možné automaticky odpovědět.
- **Upozornit** – Server vygeneruje upozorňovací mail, který bude obsahovat zvolené položky, a odešle ho na zadanou adresu. Omezit lze i celkový maximální počet znaků, což může být výhodné při posílání upozornění např. na mobilní telefon nebo pager.

Poznámky

- Do položek Odesílatel, Adresát (v části Podmínky) a Komu, Na vědomí (v části Akce) lze zadat pouze po jedné adrese. Pokud potřebujete zadat více adres, nadefinujte další pravidla.
- Pokud chcete, aby zásilka zpracovaná některým pravidlem již nebyla dále zpracovávána dalšími pravidly, zaškrtněte v daném pravidle volbu **Dále nezpracovávat**.

Práce s poštou z mobilního telefonu (WAP)

K elektronické poště v LAN SUITE lze přistupovat i z mobilních telefonů podporujících **protokol WAP**. Pomocí WAP klienta lze provádět základní operace s poštou, jako je odesílání nové pošty a čtení, odpovídání a mazání došlé pošty.

WAP klient je přístupný po zadání cesty http://adresaserveru/wap do prohlížeče v mobilním telefonu. Po zadání přihlašovacího jména a hesla se uživateli zobrazí seznam jeho

došlé pošty. Další operace se provádějí výběrem ze zobrazeného menu. Některé užitečné funkce WAP klienta lze najít i v menu „Options“, jehož způsob vyvolání je závislý na typu používaného telefonu (spec. tlačítko u tel. Nokia, přidržení tlačítka Yes u tel. Ericsson, apod.).

Odesílání faxů z LAN SUITE

Způsoby odesílání faxů z počítačů v síti

Fax lze odeslat z počítače v síti pomocí LAN SUITE dvěma základními způsoby:

- přímo z klientského programu pro práci s elektronickou poštou,
- pomocí tiskového ovladače Fax602 (a programu SendFax).

Přímé odeslání faxu z poštovního klientského programu

Tímto způsobem můžete odeslat fax z libovolného programu pro práci s elektronickou poštou.

Pokud chcete odeslat fax přímo z poštovního klientského programu, stačí pouze zadat faxové číslo jako e-mail adresáta ve formátu: faxové_číslo@fax nebo faxové_číslo@fax.fax.

Adresu adresáta je třeba zadat v jednom z těchto dvou formátů. Obsah faxu pak vytvoříte jako u běžného e-mailu. LAN SUITE rozezná, že jde o fax, právě podle domény **fax** nebo **fax.fax**, převede obsah e-mailu do faxového formátu a odešle ho. V závislosti na konfiguraci serveru je možné jako fax odeslat i připojené soubory (ve formátu HTML, DOC, XLS, RTF atd. – viz záložka **Fax** v konfiguraci LAN SUITE).

Formát faxového čísla v e-mailové adrese

Pokud chcete odeslat fax přímo z poštovního klientského programu, stačí pouze zadat faxové číslo jako e-mail adresáta ve formátu: faxové_číslo@fax nebo faxové_číslo@fax.fax, kde část **faxové_číslo** musí být v jednom z povolených formátů:

Pro mezinárodní volání doporučujeme plný (kanonický) formát bez mezer

Plný (kanonický) formát telefonního čísla bez mezer vždy obsahuje **kód země, oblasti a vlastní číslo – např. +420xxxxxxxxx.** Znak „+“ na začátku čísla nelze zadat jako součást e-mailové adresy, a proto je zapotřebí ho nahradit znaky „%2B“.

Příklad 1: **%2B420222011218@fax** (pražské telefonní číslo 222 011 218)
Příklad 2: **%2B421263830601@fax** (bratislavské telefonní číslo +421 2 63830601)

Telefonní číslo v plném formátu nemůže obsahovat např. 0 pro přechod na „státní“ linku nebo 00 pro mezinárodní volání. Aby LAN SUITE vytáčela čísla správně, je třeba korektně nastavit **Vlastnosti vytáčení** na záložce **Fax/TAPI** (nebo CAPI) v konfiguraci LAN SUITE**.**

Telefonní číslo z e-mailové adresy je před vytočením porovnáno s nastavenými hodnotami a výsledkem je pak vlastní vytáčené číslo.

Pro vnitrostátní volání doporučujeme zkrácený formát

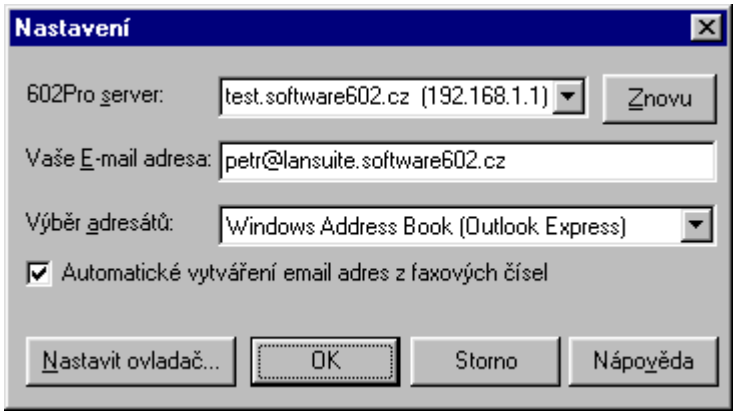
Telefonní číslo můžete také zadat přímo tak, jak ho chcete vytočit. Zadejte číslo bez mezer před @ přesně tak, jak byste ho vytáčeli ručně na telefonu. Číslo nesmí obsahovat **pomlčky, závorky, plus, mezery ani žádné další formátovací znaky!**

Příklad 1: **222011218@fax** (přímo vytočit pražské číslo 222 011 218)

Příklad 2: **512345678@fax** (přímo vytočit brněnské číslo 512 345 678)

Odesílání faxů z Outlooku Express

Pokud máte nainstalován doplňkový program **SendFax**, můžete s výhodou využít jeho funkci **Automatické vytváření e-mail adres z faxových čísel**. V konfiguraci programu SendFax zvolte pro výběr adresátů **Windows Address Book (Outlook Express)** a zaškrtněte výše zmíněnou volbu.

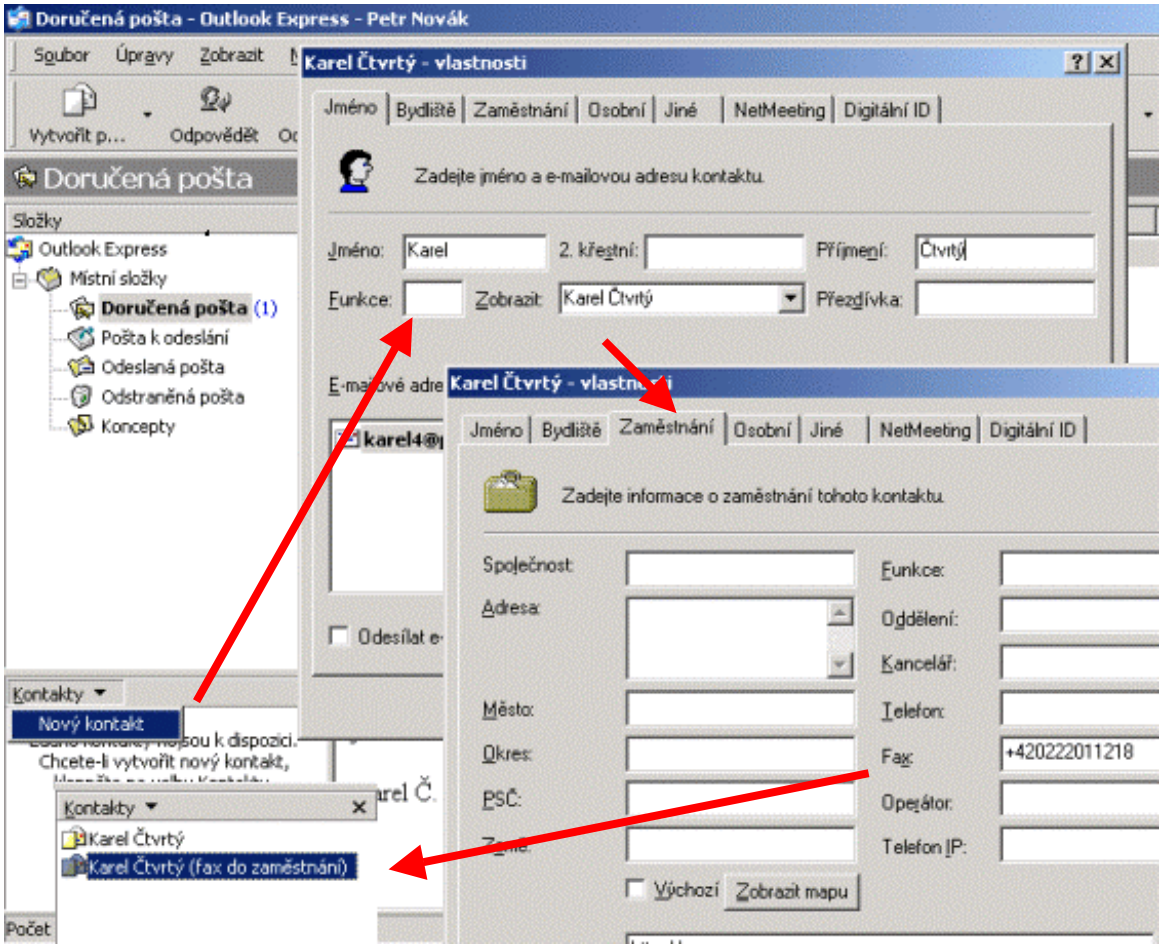


Tato funkce automaticky převádí faxová čísla zadaná do příslušných položek v Kontaktech (fax do zaměstnání, fax domů) na e-mailové adresy a vytváří příslušné nové kontakty. Pokud je tato funkce aktivní, zobrazuje ikonu vpravo dole v Systray vedle hodin.

Pozn. Pokud je na pracovní stanici zároveň nainstalován Outlook Express a MS Outlook 9x/2000/XP, nelze tuto funkci aktivovat. V tomto případě používejte raději jako klientský program MS Outlook 9x/2000/XP, kde je tato funkce implicitně aktivní (viz dále).

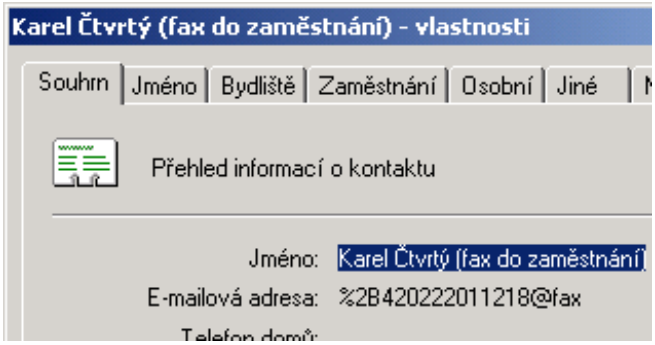
Příklad

Do Kontaktů zadáme Karla Čtvrtého s jeho e-mailovou adresou. Pokud na záložce Zaměstnání vyplníme i položku Fax (zadáme např. +420222011218), vytvoří SendFax



automaticky nový kontakt „Karel Čtvrtý (fax do zaměstnání)“, na který můžeme přímo z Outlook Expressu odesílat e-maily, které ale budou doručeny jako faxy.

Pokud na kontaktu „Karel Čtvrtý (fax do zaměstnání)“ kliknete pravým tlačítkem a zvolíte **Vlastnosti**, zobrazí se Vám následující okno.



Odesílání faxů z Outlooku 9x/2000/XP

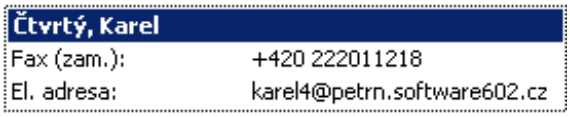
Pokud máte nainstalován doplňkový program **SendFax**, můžete odesílat faxy z Outlooku přímo na faxová čísla, která máte zaznamenána v Kontaktech v položkách Fax (zam.) a Fax

(domů). V konfiguraci programu SendFax zvolte pro výběr adresátů **MAPI (Microsoft Outlook)**.

Formáty faxových čísel

Faxová čísla zadávaná do Kontaktů v Outlooku 9x/2000/XP **musí být v jednom z následujících formátů**:

- +420 222011218
- +420222011218
- +420 222 011 218

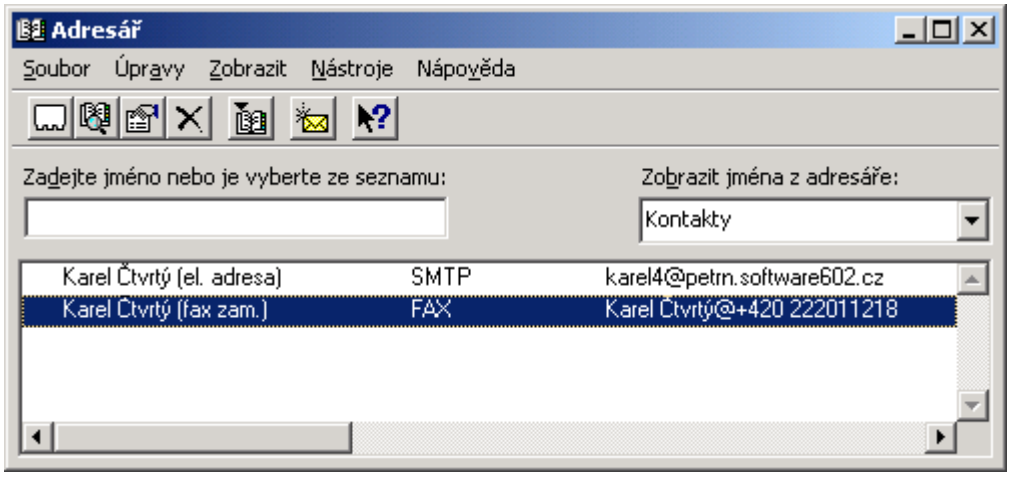


Žádné další oddělovače nebo kombinace znaků nejsou povoleny!

Příklad

Do Kontaktů zadáme Karla Čtvrtého s jeho e-mailovou adresou a do položky **Fax (zam.)** zadáme jeho faxové číslo do zaměstnání např. ve formátu +420 222011218.

Pro odeslání faxu stačí otevřít **Adresář**, vybrat faxový kontakt daného uživatele a zvolit **Nová zpráva**.



Konverze připojených souborů do faxového formátu

Obsah e-mailu a připojené soubory musí být před odesláním převeden do grafického faxového formátu. Převod může provést přímo na pracovní stanici tiskový ovladač Fax602 (součást programu SendFax) nebo na serveru LAN SUITE. LAN SUITE konvertuje pomocí interních funkcí základní textové a grafické soubory. Externě může konvertovat do faxového formátu různé dokumenty pomocí tisku na pozadí na tiskárnu Fax602.

Interně podporované formáty souborů

- TXT, GIF, JPG, BMP, PCX, TIF, WMF, CLP, DCX, DIB, CUT.

Externě podporované formáty souborů

Záleží na tom, jaký software je nainstalován na počítači s LAN SUITE.

- **DOC** – Word7 a vyšší, 602Text
- **XLS** – Excel97 a vyšší, 602Tab
- **WPD** – 602Text
- **WLS** – 602Tab
- **RTF** – Word7 a vyšší, 602Text
- **HTM, HTML** – MS Internet Explorer 4 a vyšší, Word7 a vyšší

Aktuálně externě podporované formáty souborů jsou zobrazeny v **Konfiguraci pro odborníky** na záložce **Fax**.

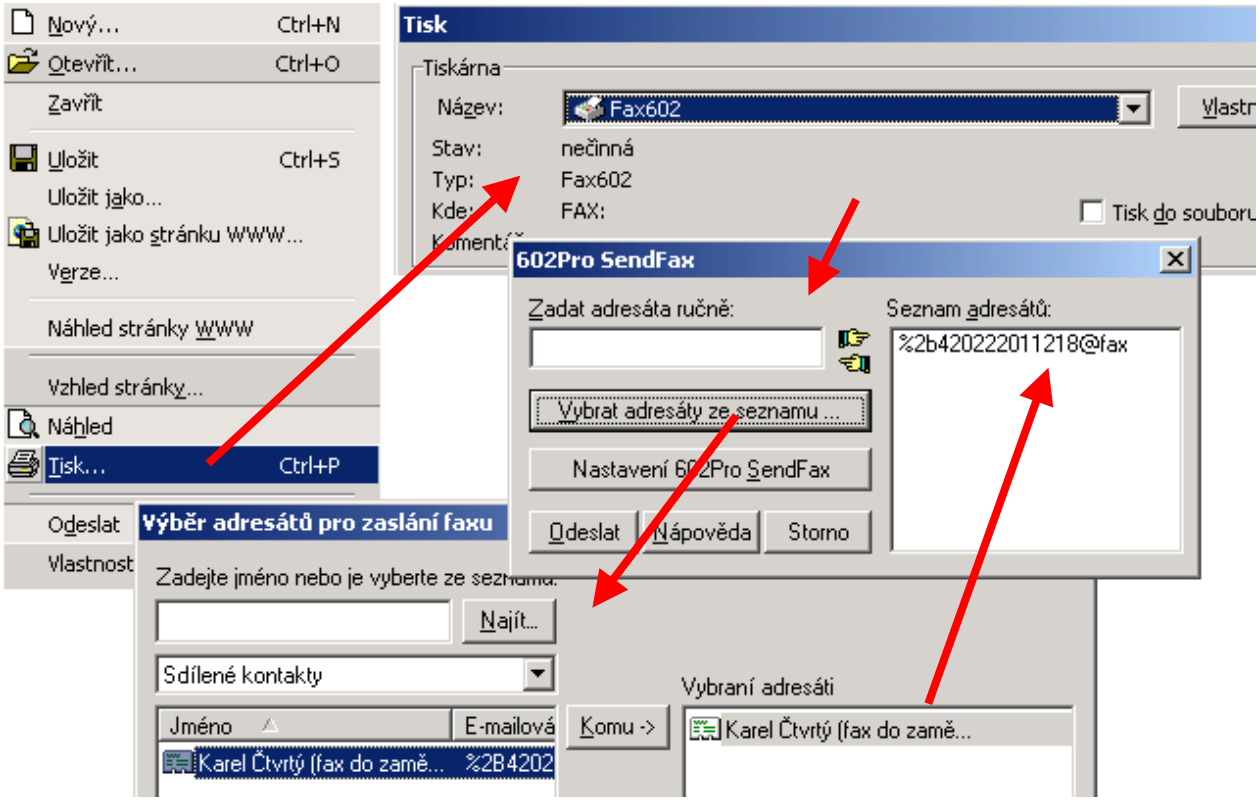
Pozn. Pro některé aplikace může být na serveru zapotřebí nastavit tiskárnu Fax602 jako výchozí.

Odesílání faxů tiskem na tiskárnu Fax602

Tiskárna Fax602 umožňuje snadné odesílání vytvořených dokumentů prakticky ze všech aplikací pracujících pod Windows.

Pokud chcete odeslat fax z libovolné „Windows“ aplikace (např. Microsoft Word), stačí jako tiskárnu zvolit **Fax602** (nainstaluje se s programem SendFax) a potvrdit tisk dokumentu. Objeví se dialog „602Pro SendFax“, ve kterém můžete zadat adresáty ručně a/nebo je vybrat z nabízeného seznamu (viz Seznamy v Konfiguraci).

Po zadání adresáta(ů) stiskněte pro odeslání faxu tlačítko **Odeslat**. Pro kontrolu se ještě otevře okno s náhledem faxu. Pokud opravdu chcete fax odeslat, stiskněte tlačítko **Odeslat** (nebo můžete fax zrušit tlačítkem **Storno**). Po odeslání faxu vygeneruje LAN SUITE potvrzení, které obdržíte e-mailem.


Nový... Ctrl+N
Otevřít... Ctrl+O
Zavřít
Uložit Ctrl+S
Uložit jako...
Uložit jako stránku WWW...
Verze...
Náhled stránky WWW
Vzhled stránky...
Náhled
Tisk... Ctrl+P
Odeslat
Vlastnost
Tisk
Tiskárna
Název: Fax602
Stav: nečinná
Typ: Fax602
Kde: FAX:
Tisk do souboru
602Pro SendFax
Zadat adresáta ručně:
Seznam adresátů:
%2b420222011218@fax
Vybrat adresáty ze seznamu ...
Nastavení 602Pro SendFax
Odeslat
Nápověda
Storno
Výběr adresátů pro zaslání faxu
Zadejte jméno nebo je vyberte ze seznamu:
Najít...
Sdílené kontakty
Jméno
E-mailová
Karel Čtvrtý (fax do zamě... %2B4202
Komu ->
Vybraní adresáti
Karel Čtvrtý (fax do zamě...