



# Konfigurace a provoz verze 4.0 ...

Cílem tohoto dokumentu je stručnou a přehlednou formou Vás seznámit s postupem instalace a konfigurace nové verze Mail602 Messaging Serveru včetně zprovoznění různých druhů klientských přístupů k poštovnímu úřadu.

## Mail602 MESSAGING SERVER 4.0

**Komplexní komunikační systém přinášející bezpečné internetové služby a lokální poštu pro celou Vaši síť, dále faxování, odesílání SMS zpráv, hlasový záznamník pro každého uživatele a navíc možnost použití téměř libovolného klientského programu.**

Jádro celého systému tvoří poštovní úřad, na kterém se nacházejí zásilky a ke kterému uživatelé přistupují klientskými programy z lokální sítě a prostřednictvím komunikačního serveru i odkudkoliv z Internetu. Pro přístup k poště lze používat browser (např. Internet Explorer), POP3 klienta (např. Outlook Express), MAPI klienta (např. Outlook 9x/2000), program Mail602 Klient a nebo mobilní telefon s podporou WAP.

Mezi hlavní rysy celého systému patří **bezpečnost**, kterou mj. zajišťuje **podpora digitálního podpisu, šifrování** obsahu zásilek i datových přenosů a řady kryptografických standardů (S-MIME, SSL, 2DES a speciálních algoritmů firmy Software602). Komunikační server má implementovanou i **antivirovou kontrolu zásilek** systémem AVG.

Pro **usnadnění administrace** je k dispozici kompletní **dálková konfigurace a správa** prostřednictvím webu a technologie DCOM. **Uživatelé lze asociovat se síťovým OS** (Novell NDS&Bindery a MS Windows NT/2000) a přímo jim tak nastavit potřebná práva.

Samozřejmostí je **podpora moderních způsobů komunikace** jako je ISDN, WAP, faxování přes Internet atd.

# Obsah

<b>MAIL602 MESSAGING SERVER 4.0.....</b>	<b>1</b>
<b>OBSAH .....</b>	<b>2</b>
<b>INSTALACE ADMINISTRÁTORA A MESSAGING SERVERU.....</b>	<b>4</b>
DŮLEŽITÉ POZNÁMKY K INSTALACI .....	4
<b>KONFIGURACE.....</b>	<b>6</b>
REGISTRACE A LICENCOVÁNÍ.....	6
ZALOŽENÍ (PŘIDÁNÍ) UŽIVATELŮ.....	7
VZDÁLENÁ SPRÁVA POŠTOVNÍHO ÚŘADU (DCOM) .....	7
NASTAVENÍ ARCHIVACE ZÁSILEK .....	8
NASTAVENÍ KÓDOVÁNÍ ZÁSILEK .....	8
PRVNÍ SPUŠTĚNÍ MESSAGING SERVERU .....	9
VZDÁLENÁ SPRÁVA KOMUNIKAČNÍHO SERVERU (WWW) .....	9
VOLBA ZPŮSOBU PŘIPOJENÍ K INTERNETU .....	9
KONFIGURACE ODESÍLÁNÍ A PŘÍJMU E-MAILŮ (NASTAVENÍ SMTP/POP3).....	10
KONFIGURACE WWW SERVERU .....	12
KONFIGURACE FAXOVÁNÍ (NASTAVENÍ SLUŽBY FAX).....	13
KONFIGURACE TELEFONNÍHO ZÁZNAMNÍKU .....	15
KONFIGURACE SDÍLENÉHO PŘÍSTUPU K INTERNETU .....	16
ZPŘÍSTUPNĚNÍ INFORMACÍ O UŽIVATELÍCH (NASTAVENÍ LDAP).....	23
KONFIGURACE ODESÍLÁNÍ A PŘÍJMU SMS .....	23
ANTIVIROVÁ KONTROLA ZÁSILEK .....	24
KONFIGURACE SPOJENÍ MAIL602 .....	24
<b>KLIENSKÉ PROGRAMY .....</b>	<b>27</b>
DIGITÁLNÍ PODPIS A ŠIFROVÁNÍ ZÁSILEK (S-MIME).....	27
<b>MAIL602 KLIENT .....</b>	<b>29</b>
<b>POP3 KLIENT .....</b>	<b>30</b>
OBECNĚ .....	30
JAK FAXOVAT Z POP3 KLIENTA ? .....	31
JAK NAKONFIGUROVAT SSL SMTP A POP3 ? .....	32
VYHLEDÁVÁNÍ E-MAILOVÝCH ADRES A INFORMACÍ U UŽIVATELÍCH .....	32
<b>MAPI KLIENT (MS OUTLOOK 9X/2000).....</b>	<b>33</b>
INSTALACE MAPI PODPORY .....	33

PŘÍSTUP K POŠTĚ A NASTAVENÍM SYSTÉMU MAIL602 .....	33
POZNÁMKY .....	34
<b>WWW KLIENT .....</b>	<b>34</b>
<b>WAP KLIENT.....</b>	<b>34</b>
<b>SYSTÉMOVÉ POŽADAVKY .....</b>	<b>35</b>

## Instalace Administrátora a Messaging Serveru

Mail602 Messaging Server je vhodné instalovat na počítač s faxmodemem (či obdobným zařízením), připojený k Internetu a splňující příslušné systémové požadavky.

Po spuštění instalace Mail602 Messaging Serveru z úvodní obrazovky nebo z adresáře MESSAG\SERVER\Disk1 na CD zvolte cílový adresář a při výběru komponent zaškrtněte instalaci Administrátora i Messaging Serveru. V dotazu týkajícím se napojení na již existující poštovní úřad ponechte řádku prázdnou. Pouze pokud provádíte upgrade nebo chcete server provozovat nad již existujícím poštovním úřadem, zadejte zde cestu na soubor M602.EMI.

Pokud Vám instalační program nabídne instalaci Administrátora jako služby, přečtěte si sekci **Důležité poznámky k instalaci**.

Pokud jste se při instalaci nenapojili na existující poštovní úřad, pak po instalaci potvrďte nabízené spuštění průvodce konfigurací nového poštovního úřadu a postupujte podle jeho pokynů. Poštovní úřad je vhodné založit na sdíleném diskovém prostoru, přičemž cestu lze zapsat i v UNC formátu (\\počítač\sdílení\cesta). Zvýšenou pozornost věnujte zadání kódovacího řetězce a hesla SUPERVISORA! Pro jistotu si tyto údaje ihned zaznamenejte a uschovejte na bezpečné místo, neboť jsou nutné pro následné provádění změn v konfiguraci. Pro korektní funkci celého systému je rovněž důležitá správně vyplněná internetová doména!

### ***Důležité poznámky k instalaci***

#### **Předpoklady pro asociaci uživatelů**

Asociace uživatelů tj. jejich on-line provázání s operačním systémem lze využívat v následujících případech :

- poštovní úřad je založen na disku počítače s Windows NT/2000,
- poštovní úřad je založen na disku serveru Novell Netware v režimu Bindery,
- na síti je k dispozici Novell NDS a stanice pro přístup do sítě využívají síťového klienta od firmy Novell.

Díky asociacím jednoduše převezmete uživatele ze síťového operačního systému do systému Mail602. Následně můžete asociovaným uživatelům nastavit potřebná síťová práva stisknutím jednoho tlačítka. Uživatel se pak také hlásí pouze do sítě (jméno a heslo) a přihlášení do pošty je ze sítě automaticky převzato – platí pouze pro přístup pomocí Mail602 Klient a Microsoft Outlook 9x/2000.

## **Předpoklady pro vzdálenou správu poštovního úřadu – DCOM**

Pokud budete chtít využívat vzdálenou správu poštovního úřadu prostřednictvím technologie DCOM (protokolem TCP/IP např. z Internetu, tzn. nejen klasicky po lokální síti prostřednictvím sdílení poštovního adresáře), nainstalujte program Administrátor (také) na počítač s operačním systémem Windows NT/2000 (tzv. *administrační server*), ze kterého je po síti dostupný poštovní úřad. Administrační server musí být dostupný protokolem TCP/IP z lokality, ze které chcete poštovní úřad spravovat.

Pokud chcete mít možnost provádět vzdálenou administraci i v případě, že na administračním serveru není nikdo přihlášen, potvrďte nabízenou instalaci administrační služby pod UŽIVATELSKÝM účtem (nejlépe uživatel ze skupiny Administrátoři) a v nastavení služby zvolte spouštět manuálně (spouštění zajišťuje DCOM).

Na administračním serveru je dále třeba založit uživatele se shodným jménem a heslem jako bude na vzdáleném počítači používat vzdálený správce a přidat ho ve Windows do skupiny Administrátoři.

## **Provoz jako NT/2000 služba**

Všechny služby systému Mail602 je třeba spouštět pod UŽIVATELSKÝM účtem, neboť systémový účet neumí pracovat s cestami v UNC formátu (\\server\cesta).

Pozn. Vlastní uživatel Administrátor někdy nemá oprávnění spouštět pod svým účtem služby.

## Konfigurace

Obecně lze konfiguraci systému Mail602 shrnout do následujících pěti bodů :

1. instalace,
2. založení poštovního úřadu,
3. nastavení Administrátora – registrace, uživatelé, práva, ...,
4. nastavení komunikačního serveru,
5. instalace a konfigurace klientských programů.

Pokud bude v některém tématu uveden podnadpis „Administrátor“ nebo „Messaging Server“, znamená to, že popisované nastavení se provádí v příslušném programu.

### ***Registrace a licencování***

#### **Administrátor**

Po spuštění Administrátora kliknutím na název poštovního úřadu zobrazíte přihlašovací dialog. V některých případech může být také zapotřebí nejprve kliknout na Seznam úřadů.

#### **Licenční číslo serveru (umožňuje i provoz jako TRIAL verze)**

Pokud není systém zaregistrován, budete vyzváni k zadání licenčního čísla serveru. Toto číslo můžete zdarma získat na webových stránkách společnosti Software602, a.s. <http://www.software602.cz>. Po zadání tohoto čísla máte k dispozici všechny služby systému Mail602 Messaging Server po dobu 30 dnů pro 5 uživatelů. Pokud budete chtít Mail602 Messaging Server využívat i po vypršení těchto 30 dnů, musíte si zakoupit některý z klientských přístupů a potřebný počet add-on licencí (poštovních schránek).

#### **Klientské přístupy a add-on licence**

Každý z následujícího seznamu klientských přístupů je k dispozici po zadání příslušného licenčního čísla:

- **POP3** – např. MS Outlook Express a další aplikace podporující tento protokol,
- **MAPI** – Microsoft Outlook 9x/2000 a další aplikace podporující tento standard,
- **Mail602** – program Mail602 Klient – lokálně nebo po TCP/IP, ISDN, modemu,
- **WWW/WAP** – pro přístup k poště lze využívat libovolný browser nebo mobilní telefon s podporou WAP.

Pokud chcete zadat zakoupená licenční čísla pro některý z klientských přístupů nebo zvýšit počet poštovních schránek zadáním add-on licencí, vyberte příslušnou položku v pravé části okna s hlavní konfigurací poštovního úřadu.

## ***Založení (přidání) uživatelů***

### **Administrátor**

Po spuštění Administrátora kliknutím na název poštovního úřadu zobrazíte přihlašovací dialog. V některých případech může být také zapotřebí nejprve kliknout na Seznam úřadů.

Rozbalte strom Uživatelé a přejděte na položku Základní informace. V pravé části okna klikněte pravým tlačítkem a přidejte uživatele.

### **Asociace uživatele**

Pokud splňuje Vaše instalace potřebné předpoklady (viz Důležité poznámky k instalaci), můžete uživatele do systému Mail602 převzít a aktivně propojit přímo se síťovým operačním systémem.

Nejprve je však třeba asociace povolit. Klikněte na název Vašeho úřadu a v pravé části okna vyberte Typ asociace uživatelů. V nastavení si vyberte z možností nabízených dle Vaší konfigurace.

Pokud tedy máte asociování uživatelů povoleno, bude Vám nabídnuto přidání a asociování uživatele ze síťového operačního systému. Po potvrzení se zobrazí seznam uživatelů síťového operačního systému, ze kterých si můžete příslušného vybrat.

### **Ostatní případy (neasociovaný uživatel)**

Pokud Vám není asociace nabídnuta nebo zvolíte-li neasociovat, vyplňte přihlašovací a plné jméno uživatele a dvakrát heslo (lze také provést „statický“ import ze serveru).

## ***Vzdálená správa poštovního úřadu (DCOM)***

Pokud splňuje Vaše instalace potřebné předpoklady (viz Důležité poznámky k instalaci), můžete celý poštovní úřad spravovat vzdáleně pomocí stejného uživatelského rozhraní.

### **Nastavení administračního serveru**

Na správně nakonfigurovaném administračním serveru (viz Důležité poznámky k instalaci) spusťte program Administrátor. Po přihlášení k poštovnímu úřadu zvolte v menu

položku Administrátor – Povolení DCOM přístupu. Ukončete program Administrátor a proveďte RESTART počítače.

### **Vzdálené správa – připojení**

Na počítači, ze kterého chcete poštovní úřad spravovat, spusťte program Administrátor. Klikněte pravým tlačítkem na text u ikonky Administrátor a zvolte přidat počítač. Zadejte IP adresu a vyčkejte připojení k administračnímu serveru. Přihlášení a správa zvoleného poštovního úřadu pak již probíhá naprosto shodně s „lokální“ administrací.

**Pozn.** Na klientském počítači je třeba být přihlášen jako uživatel, který existuje i na administračním serveru ve Windows jako člen skupiny Administrátoři.

## ***Nastavení archivace zásilek***

### **Administrátor**

Všechny zásilky na poštovním úřadu systému Mail602 mohou být archivovány v centrálním kódovaném a komprimovaném archivu.

Nastavení parametrů archivace lze provádět v pravé části okna po kliknutí na název poštovního úřadu. Pro příchozí i odchozí zásilky lze odděleně nastavit způsob jejich archivace. U zásilek lze buď pouze evidovat jejich průvodku (tzn. bez obsahu dopisu) nebo archivovat obsah dopisu, případně i s připojenými soubory.

Odděleně se provádí nastavení pro odchozí faxy, neboť jejich grafická podoba klade zvýšené nároky na místo na disku s archivem.

## ***Nastavení kódování zásilek***

### **Administrátor**

Všechny zásilky uložené na poštovním úřadu jsou kódovány nastavenou metodou (Standard, DES, 2\*DES). Obvykle postačuje použití Standardní metody, která je i nejrychlejší.

Kódovány mohou být i faxy nacházející se ve frontě zásilek k odeslání. Doporučujeme používat volbu „nekódovat“, neboť faxy ve frontě nejsou ani při tomto nastavení běžnými prostředky čitelné. Kódování navíc zbytečně zatěžuje komunikační server.



## ***První spuštění Messaging Serveru***

Pokud server nalezne na počítači nainstalovanou předchozí verzi Messaging Serveru resp. Internet Serveru, budete při jeho prvním spuštění dotázáni, zda se má provést import „internetové“ konfigurace (SMTP, POP3, Proxy, WWW, atd.). Jestliže jste při instalaci nový Messaging Server napojili na stávající poštovní úřad, bude také automaticky načtena konfigurace Intranet Serveru (fax, hlas, atd.).

V ostatních případech budete muset komunikační služby nakonfigurovat ručně. Základní Internetové služby lze nastavit snadno pomocí průvodce konfigurací. Čtěte pozorně všechny zobrazované informace.

**Pozn.** Po spuštění můžete být vyzváni k zadání cesty na poštovní úřad – vyplňte cestu, kterou jste zvolili při zakládání poštovního úřadu. Pokud po Vás server při každém spuštění vyžaduje potvrzení této cesty, můžete do jeho zástupce doplnit za název programu za mezeru výše zmíněnou cestu.

## ***Vzdálená správa komunikačního serveru (WWW)***

### **Messaging Server**

V konfiguraci pro odborníky na záložce Administrace lze povolit dálkové ovládání komunikačního serveru tzn. konfigurace, sledování provozu, navazování dial-up atd.

Pokud povolíte dálkové ovládání, doporučujeme zvolit druhou nebo třetí možnost pro přihlášení – pro přístup je pak vyžadováno zadání jména a hesla. Pro zvýšení bezpečnosti lze navíc používat i IP filtr, který umožňuje omezit přístup k dálkovému ovládání např. na konkrétní IP adresy.

K dálkové administraci potom přistupujete pomocí browseru, do kterého zadáte adresu ve tvaru <http://server/admin/> (případně <https://server/admin/>).

**Pozn.** Pro používání vzdálené správy je třeba mít zapnutou službu WWW.

## ***Volba způsobu připojení k Internetu***

### **Messaging Server**

Pokud jste k Internetu připojeni pomocí modemu vytáčenou linkou nebo máte trvalé připojení realizováno jako permanentní dial-up pomocí modemů, přidejte v konfiguraci Messaging Serveru službu DIAL-UP a vyplňte jméno a heslo. Dále můžete na kartě Kdy navazovat spojení omezit časově a věcně události a intervaly, kdy je připojení navazováno.

V případě používání jediného faxmodemu pro připojení k Internetu i faxování je vhodné zapnout poslední možnost „Uvolnit TAPI zařízení ...“, která zajistí odeslání čekajících faxů.

Pro pevnou linku či jinak realizované trvalé připojení není třeba provádět žádné nastavení – Messaging Server se o navazování připojení prostě nebude starat.

## ***Konfigurace odesílání a příjmu e-mailů (nastavení SMTP/POP3)***

### **Administrátor**

Pokud budete chtít využívat pro přístup do pošty programy pracující na bázi protokolu POP3 (např. MS Outlook Express, Netscape Messenger, ...), je třeba ve vlastnostech uživatele zaškrtnout volbu „Vybírání POP3 protokolem povoleno“. To lze samozřejmě provést i hromadně, pokud označíte více uživatelů.

### **Messaging Server – SMTP**

V konfiguraci vyberte/přidejte SMTP službu a v jejím nastavení proveďte následující úpravy :

- zkontrolujte zaškrtnutí SMTP serveru pro všechna rozhraní,
- na záložce Příjem zásilek se ujistěte, že máte zaškrtnutou volbu „Povolit relay faxů“, jinak by uživatelé POP3 klientů nemohli odesílat faxy,
- pokud odesíláte poštu přes SMTP server u poskytovatele, zapište jeho adresu na záložce Odesílání zásilek do kolonky „Nadřazený uzel“ a zaškrtněte tuto volbu,
- v případě SMTP příjmu pošty od nadřazeného uzlu ho můžete nadefinovat a v případě potřeby nastavit vysílání příkazu ETRN včetně jeho parametrů,
- při povolené akceptaci vadných lokálních adres budou zásilky se správnou doménou ale špatným jménem doručovány do složky Nezařazená pošta, do které mají přístup pouze uživatelé s právem „Rozdělování nezařazené pošty“, které jde nastavit ve vlastnostech jednotlivých uživatelů. V opačném případě je bude server vracet odesílatelům jako nedoručitelné.

### **Messaging Server – POP3**

Dále vyberte/přidejte POP3 službu a

- zkontrolujte zaškrtnutí POP3 serveru pro všechna rozhraní,
- pokud chcete, aby Messaging Server v pravidelných intervalech stahoval poštu z POP3 schránek na Internetu, nastavte tyto schránky spolu s jejich parametry na záložce „Výběr POP3 schránek na internetu“.

V případě, že využíváte tzv. „doménový koš“ nebo-li jednu POP3 schránku, do které je směřována pošta pro celou doménu (nebo více e-mailových adres), zvolte u položky „Pro Mail602 uživatele“ možnost „podle adres v dopisu“. Server v tomto případě po vybrání POP3 schránky poštu automaticky roztrídí do schránek příslušných uživatelů, podle jejich e-mailových adres.

## Nastavení Relay

Funkce Relay dovoluje SMTP serveru přijmout zásilku, jejíž adresát na tomto poštovním úřadu nemá schránku, a dále ji pak odeslat protokolem SMTP jejímu adresátovi.

Omezení služby Relay snižuje možnost zneužití SMTP serveru pro rozesílání nevyžádaných zásilek (SPAM) jinými servery či uživateli. Proto doporučujeme použít alespoň jedno z nabízených nastavení :

- pouze pro uživatele – server testuje, zda odesílatel existuje v rámci poštovního úřadu,
  - předcházející POP3 přístup – server umožňuje odesílat zásilky po dobu 120 minut pouze uživateli, který nejprve realizoval úspěšný přístup do své POP3 schránky,
- omezení přes IP filtr - Pro přístup k SMTP Relay pak platí IP filtr. V něm lze omezit přístup k SMTP serveru (a tím tedy i k jeho Relay funkci) např. pouze na počítače z lokální sítě a na SMTP server poskytovatele.
- Relay faxů – umožňuje odesílat faxy uživatelům POP3 klientů na adresu číslo@fax.

## Nastavení Anti-SPAM

Funkce Anti-SPAM může chránit uživatele proti opakovanému příjmu nevyžádaných zásilek. Zásilky lze filtrovat dvěma způsoby:

- veřejná Anti-SPAM služba MAPS RBL  
Před přijetím každé zásilky se Messaging Server dotáže serveru služby MAPS RBL, zda server/odesílatel zásilky není uveden v seznamu šířitelů nevyžádaných zásilek. Pokud tam je uveden, zásilka je odmítnuta.
- seznam serverů/odesílatelů, jejichž zásilky náš server nepřijímá  
Zásilky lze též odmítat pomocí vlastního seznamu SPAM-serverů/odesílatelů. Položky seznamu lze editovat jednotlivě nebo importovat a exportovat jako celek. Pro import je třeba předem připravit adresy do textového souboru, kde bude na každé řádce jedna adresa.

## Nastavení Messaging Serveru pro SSL SMTP/POP3

Zabezpečení SMTP a POP3 serveru pomocí SSL zabraňuje mj. „odposlechu“ Vašeho hesla i Vašich e-mailů na cestě mezi SMTP/POP3 serverem a Vaším počítačem. Pro využití těchto funkcí je třeba, aby je podporoval jak server tak i klient.

Nejprve je třeba v Messaging Serveru vygenerovat klíče pro SSL komunikaci. To lze udělat např. v nastavení SMTP služby, kdy po stisku tlačítka „Nastavení SSL“, následně tlačítka „Vytvořit soukromý a veřejný klíč“ a zadání několika údajů budou tyto klíče automaticky vygenerovány.

Potom již stačí zaškrtnout volbu „SSL SMTP server“ v nastavení služby SMTP resp. volbu „SSL POP3 server“ v nastavení služby POP3.

## ***Konfigurace WWW serveru***

### Messaging Server

V konfiguraci Messaging Serveru přidejte službu WWW. Na záložce SSL WWW server máte poté možnost si v Nastavení SSL jednoduše stiskem tlačítka vytvořit soukromý a veřejný klíč pro zabezpečenou komunikaci mezi browserem a Vaším WWW serverem. Tu využijete zejména při přístupu do pošty pomocí browseru resp. WWW klienta.

Na kartě (SSL) WWW server lze nastavit adresáře pro práci WWW serveru. Pokud chcete vytvořit např. jen vnitro-firemní Intranet, zapněte IP filtr – v potaz budou brány jen řádky s cílovou adresou serveru a maskou 255.255.255.255.

Na záložce Zprávy lze zapnout zaznamenávání operací prováděných WWW serverem i ve formátu W3C, čehož lze využít pro následnou analýzu některým z komerčně dostupných programů.

**Pozn.** Služba WWW je zapotřebí pro využívání vzdálené správy Messaging Serveru, pro přístup do pošty z browseru (WWW klient), pro přístup do pošty pomocí mobilního telefonu (WAP klient).

### Administrátor – uživatelské WWW stránky

Ve stromu Uživatelé přejděte na položku Uživatelé WWW, kde ve složce WWWServer0 (resp. WWWServer1 pro SSL WWW server) můžete jednotlivým uživatelům založit jejich domovské adresáře a vygenerovat základ osobní stránky. Po stisku pravého tlačítka myši můžete změnit Základní adresář (hlavní adresář na disku s domovskými stránkami) a u jednotlivých uživatelů volbou Upravit nadefinovat jejich konkrétní domovský adresář –

zadáva se pouze název adresáře bez cesty (např. karel). Domovské stránky jsou pak browserem dostupné na adrese např. <http://server/~karel> (kde server je buď IP adresa počítače s Messaging Serverem nebo jeho název).

### **Administrátor – virtuální adresáře a přístupová práva**

V programu Administrátor lze též definovat přístupová práva uživatelů do virtuálních adresářů WWW serveru (tzv. directory alias). Děje se tak ve stromu Uživatelé – Uživatelé WWW, ve složce WWWServer0 (resp. WWWServer1 pro SSL WWW server).

Ve stromu Virtuální adresáře je třeba zadat jméno tohoto virtuálního adresáře a reálný adresář, ve kterém jsou umístěny dané HTML soubory. Lze také zvolit zda se v tomto adresáři mohou spouštět CGI skripty a případně jméno autentifikace. Pro přístup do virtuálního adresáře z browseru je třeba zadat URL adresu ve tvaru <http://server/virtuálníadresář>. Pokud byla přiřazena autentifikace, bude třeba v browseru zadat nejprve jméno a heslo.

Seznam Autentifikací umožňuje definovat skupiny uživatelů, kteří mají mít přístup k určité oblasti WWW serveru (virtuálnímu adresáři). Při zakládání nové “autentifikace” zvolíme její jméno (např. Dealeri) a následně přes pravé tlačítko myši přidáme ze seznamu příslušné uživatele. Pro přístup může uživatel používat své heslo pro přístup do Mail602 nebo heslo zadané speciálně pro tuto autentifikaci.

## ***Konfigurace faxování (nastavení služby Fax)***

### **Administrátor**

Při faxování z programů Mail602 Klient nebo Microsoft Outlook 9x/2000 (MAPI) lze k odesílaným faxům přidávat úvodní stránku včetně loga firmy, přičemž logo může být různé podle jazyka použitého ve faxu. Logo v různých grafických formátech lze zavést v pravé části okna po kliknutí na název poštovního úřadu. Odesílání faxů lze také časově omezit výběrem položky „Faxové spojení“.

Všechny došlé faxy jsou standardně doručovány do složky „Neroztříděné faxy“, do které mají přístup pouze uživatelé s právem „Rozdělování nezařazené pošty“, které jde nastavit ve vlastnostech jednotlivých uživatelů. Tato složka je dostupná všemi klientskými programy vyjma POP3 a WAP.

Faxy mohou být také doručovány přímo do došlé pošty konkrétním uživatelům na základě „identifikace“ odesílacího faxu nebo ve spolupráci s pobočkovou ústřednou (viz

dále), pokud mají nadefinována tzv. virtuální faxová čísla. V rámci Administrátora se toto nastavení provádí ve vlastnostech uživatelů na kartě „Adresy a čísla“ – Faxové číslo. Lze použít i zástupné znaky jako \* (hvězdička) a ? (otazník).

## Messaging Server

V konfiguraci Messaging Serveru vyberte/přidejte službu Fax. Při přidávání ze seznamu zařízení, která jsou k dispozici, vyberte Vámi používaný faxmodem, který máte nainstalovaný ve Windows (např. TAPI–ZyXEL U-1496E ...) nebo přímo některý z komunikačních portů (např. COM2), na který máte faxmodem připojený.

**Pozn.** ISDN zařízení musí mít ve Windows nainstalované ovladače CAPI.

Pokud budete používat faxmodemy dva, přidejte službu dvakrát. Potom máte možnost v nastavení příslušné služby na první záložce říci, zda bude daný faxmodem určen pouze pro odesílání (pouze výstupní) nebo jen pro příjem faxů (pouze vstupní). Pokud ne zvolíte ani jednu z možností budou faxy odesílány či přijímány právě volným faxmodemem.

V nastavení služby fax proveďte následující úpravy :

- na záložce Zařízení zvolte dole záložku Pro odborníky a zvolte místo (a případně upravte jeho vlastnosti) v Pravidlech pro vytáčení – toto nastavení mj. ovlivňuje vytáčení tónovou/pulsní volbou nebo nuly pro státní linku atp.,
- při použití ISDN nastavte na příslušné záložce telefonní číslo, na kterém bude faxový server naslouchat (lze obvykle vybrat jedno ze čtyř telefonních čísel),
- na záložce FAX si můžete nastavit Identifikaci faxu, tj. text, který se zobrazuje protějšší straně při faxování.

Na záložce FAX lze také nechat všechny přijaté faxy automaticky tisknout na libovolné tiskárně, která je z daného počítače (ve Windows) s komunikačním serverem. Faxy se tisknout okamžitě po dokončení jejich příjmu komunikačním serverem.

Informace o nalezené OLE podpoře Vás informují, jaké soubory můžete připojit k odesílanému faxu a komunikační server je automaticky zkonvertuje do faxového formátu.

Při potížích s odesíláním či příjmem faxů zkuste snížit rychlosti vysílání/příjmu na dolní záložce FaxModem na záložce FAX, případně nastavte ovládací příkazy manuálně na Class1.

## Nastavení pobočkové ústředny

Pro přímé doručování faxů konkrétním uživatelům do jejich poštovních schránek, je třeba jim nastavit v Administrátorovi virtuální faxová čísla a dále nastavit ústřednu tak, aby volání na tato čísla směřovala na linku s faxmodemem připojeným k Messaging Serveru. Po

přijetí volání faxmodemem mu musí být ústředna schopna zopakovat tónově (DTMF volbou) původně volané číslo (linku). Pokud ústředna při opakování čísla vkládá před/za něj nějaké další znaky, nastavte v Administrátorovi číslo se zástupnými znaky „?“ (např. pokud ústředna pro číslo 123 předává AA123B, pak nastavte ??123?).

## ***Konfigurace telefonního záznamníku***

### **Administrátor**

Po přihlášení k poštovnímu úřadu klikněte na jeho název a v pravé části okna nastavte položku „Uvítací zpráva pro modemy“ podle typu Vašeho faxmodemu. Pokud si nejste typem modemu jisti, vyzkoušejte Rockwell (příp. HCF Rockwell).

Hlasové vzkazy jsou standardně doručovány do složky „Nezařaditelná pošta“, do které mají přístup pouze uživatelé s právem „Rozdělování nezařazené pošty“, které jde nastavit ve vlastnostech jednotlivých uživatelů.

Hlasové vzkazy také mohou být ve spolupráci s pobočkovou ústřednou doručovány přímo do došlé pošty konkrétním uživatelům (viz dále), pokud mají nadefinována tzv. hlasová čísla, která většinou bývají shodná s linkovým číslem daného uživatele. V rámci Administrátora se toto nastavení provádí ve vlastnostech uživatelů na kartě „Adresy a čísla“ – Hlasové číslo. Lze použít i zástupné znaky jako \* (hvězdička) a ? (otazník).

### **Vzdálené ovládání telefonního záznamníku**

Pokud uživateli ve vlastnostech povolíte Hlasový přístup a na záložce „Jména a hesla“ mu nastavíte heslo pro hlasový přístup (heslo nesmí obsahovat jiné znaky než číslice), bude mít možnost pracovat s nahranými vzkazy i vzdáleně pomocí libovolného telefonu s tónovou volbou.

Stačí, když zavolá na telefonní číslo, kde naslouchá komunikační server a po vyzvednutí linky zadá tónově číslo své linky (svoje „Hlasové číslo“) a následně své „hlasové“ heslo.

Dále je možno používat tyto povely :

- 1 přehraj zprávy (implicitní)
- 2 přehraj předchozí zprávu
- 4 přehraj jen neviděné/resp. všechny
- 5 smaž aktuální zprávu/resp. (po dokončení přehrávání všech zpráv) smaž všechny zprávy
- 6 další zprávu
- 7 (po dokončení přehrávání všech zpráv), konec=polož linku

- 0 přeskoč všechny zprávy
- \* přeskoč uvítací zprávy
- 99 zaznamenej novou vlastní uvítací zprávu
- # potvrzení nové vlastní uvítací zprávy

## Messaging Server

V konfiguraci Messaging Serveru přidejte službu Hlas (pokud ještě není v seznamu aktivních služeb) a ze seznamu zařízení, která jsou k dispozici, vyberte Vámi používaný modem s podporou hlasu (voice), který máte nainstalovaný ve Windows (např. TAPI-ZyXEL U-1496E ...) nebo přímo některý z komunikačních portů (např. COM2), ke kterému je modem připojen.

V nastavení služby na kartě Hlas vyberte Hlasový mód odpovídající typu Vašeho modemu (pokud si nejste jisti, vyzkoušejte typ Rockwell nebo HCF Rockwell).

## Nastavení pobočkové ústředny

Pro přímé doručování hlasových vzkazů konkrétním uživatelům do jejich poštovních schránek, je třeba jim nastavit v Administrátorovi hlasová čísla a dále nastavit ústřednu tak, aby pokud volaný uživatel do určitého počtu zazvonění (nebo do určité doby) nezvedne telefon, směřovala volání na linku s faxmodemem připojeným k Messaging Serveru. Po přijetí volání faxmodemem mu musí být ústředna schopna zopakovat tónově (DTMF volbou) původně volané číslo (linku). Pokud ústředna při opakování čísla vkládá před/za něj nějaké další znaky, nastavte v Administrátorovi číslo se zástupnými znaky „?“ (např. pokud ústředna pro číslo 123 předává BB123A, pak nastavte ??123?).

## ***Konfigurace sdíleného přístupu k Internetu***

Přístup k Internetu z lokální sítě zajišťuje služba Proxy. Veškeré požadavky od klientských programů (stanic) procházejí komunikačním serverem, a proto se nejsnáze využívají aplikace s vestavěnou podporou Proxy nebo SOCKS (v ostatních případech je třeba nakonfigurovat tzv. Mapované spojení – viz další text).

## Nastavení Proxy

V nastavení služby Proxy v Messaging Serveru lze hned na první záložce konfigurovat běžně používané proxy brány, mezi které patří zejména HTTP/HTTPS/HTTP-FTP využívaná browsery pro přístup k WWW serverům na Internetu. Ve Vámi používaném browseru stačí uvést jako adresu proxy serveru IP adresu komunikačního serveru a port číslo 80.



SOCKS proxy verze 4 a 5 není závislá na používaném protokolu, a proto ji lze využít např. pro program ICQ nebo pro aplikace přenášející libovolná i kódovaná data.

Narozdíl od HTTP-FTP proxy na portu 80 sloužící pro browsery je FTP proxy na portu 21 určena pro využití přímo z FTP klientských programů (např. WS\_FTP, Cute FTP apod.).

**Tab. 1 Nastavení běžných FTP klientů pro používání FTP proxy**

<b>CuteFTP</b> Host : IP adresa MSG Type : <a href="#">user@site</a> Enable firewall access	<b>WS_FTP Pro</b> Use firewall Host name : IP adresa MSG User with no login
<b>FTP Explorer</b> Use Firewall Host : IP adresa MSG Firewall type : <a href="#">user@hostname</a>	<b>FAR file manager</b> Firewall:port : IP adresa MSG

Dále je podporována Telnet proxy pro využívání programu Telnet skrz komunikační server. V programu Telnet lze zadat spojení na IP adresu komunikačního serveru, který Vás následně vyzve k zadání cílové adresy a portu.

RealAudio proxy umožňuje na stanicích v lokální síti, které jsou připojeny k Internetu pouze pomocí proxy, přehrávat multimediální klipy z Internetu pomocí programu RealPlayer firmy RealNetworks.

DNS proxy předává DNS požadavky ze sítě DNS serveru v Internetu a zpět vysílá odpovědi, čímž je pro všechny aplikace v síti plně zajištěna funkce DNS. Stanice v síti LAN ale často generují "zbytečné" DNS požadavky, kvůli kterým se pak navazují dial-up spojení. Pokud je tomu třeba předejít, zaškrtněte volbu "Nenavazovat dial-up spojení kvůli DNS". DNS proxy pak pracuje pouze v případě, že je dial-up spojení již navázáno z jiného důvodu.

### Sledování činnosti Proxy serveru

Na záložce Zprávy lze kromě standardního zapnout i zaznamenávání operací s cache a prováděných proxy serverem ve formátu W3C, čehož lze využít pro následnou analýzu některým z komerčně dostupných programů.

### Nastavení Proxy pro odborníky

Kromě změny portů, na kterých jsou v provozu příslušné druhy proxy, lze nastavit i parametry vyrovnávací paměti (cache).

Perioda úklidu cache udává časový interval v minutách, po kterém bude obsah vyrovnávací paměti testován a uvolněn vymazáním souborů s prošlou expirační lhůtou.

Expirační doba souborů v cache je doba v hodinách, po které budou soubory uložené ve vyrovnávací paměti vymazány.

Některé WWW a FTP servery nesdělují klientským programům velikost souborů a další informace. Pak se může stát, že při přerušení spojení v cache zůstane nekompletní soubor. Pokud povolíte volbu „Vyžadovat informace o souborech“, nebudou se soubory bez připojených informací do cache ukládat.

Při zapnuté volbě „Skripty (CGI, ASP) vždy provádět“ se proxy pokusí podle URL adresy zjistit, zda je daná HTML stránka produktem CGI skriptu a neuloží ji do cache, aby se při příštím pokusu o stažení znovu aktivoval CGI skript a do browseru se neposlala tedy stránka uložená v cache paměti.

Do HTML stránek může vysílající WWW server vložit 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 přepínač „Povolit řízení cache HTML příkazy“ nezaškrtnete, proxy příkazy neakceptuje a z HTML stránek je vymazává.

Nadřízený proxy/cache server: HTTP proxy server obvykle přijímá data z cílových serverů. V některých případech je vhodné nastavit vícecestupňovou proxy, kdy pak jeden proxy server žádá data po nadřazeném serveru. Typicky se jedná o využití velké proxy cache provozovatele internetového napojení.

## Mapované 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 v Messaging Serveru v nastavení služby Proxy na příslušné záložce.

Pokud tedy klientský program na stanici v privátní síti potřebuje navázat TCP/IP spojení s konkrétním počítačem v Internetu, zadá se místo adresy tohoto počítače v klientském programu adresa Messaging Serveru, ve kterém se na kartě 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 Messaging Serverem. Jedná se tedy o jakýsi přesměrovávač, jehož prostřednictvím se mohou po TCP/IP spojit dva počítače.

Výhodou je, že klientský program nemusí podporovat žádný typ firewallu. Vlastností (nevýhodou) pak je, že se stanice takto může připojit pouze na jediný počítač v Internetu, resp. na ty počítače, které jsou konkrétně vypsány v Messaging Serveru.

Na kartě Mapovaná spojení je tedy nutné:

- Voličem Protokol vybrat, jakým protokolem se má spojení realizovat (TCP nebo UDP).
- Ve sloupci Spojení z – který počítač se bude připojovat (pole IP adresa a IP maska).
- Ve dvojici polí Na tento počítač – přes který port počítače bude navazován kontakt s Messaging Serverem (pole IP adresa a Port).
- Ve dvojici polí Mapovat na – na který počítač se má toto spojení směřovat (pole Cílová adresa a Port).

Zdrojový počítač s maskou a IP adresa počítače s Messaging Serverem musí být uvedeny číselnou IP adresou; číslo jeho portu a adresa a port cílového počítače mohou být uvedeny i symbolicky.

**Pozn.** Formát tabulky tedy umožňuje i takové nastavení, kdy se přes jeden port počítače s Internet Serverem může současně spojovat více počítačů na několik různých cílových počítačů, protože definujeme, který zdrojový počítač (sít') se má spojovat na který cílový počítač.

**Pozn.** Pokud počítači s Messaging Serverem přiřadíte více IP adres, můžete např. zpřístupnit více než jeden NEWS server na Internetu; vždy jeden server na jedno napojení, přičemž všechny užívají stejný NEWS port (ve střední části tabulky zadejte nejen číslo portu, ale i IP adresu). Pokud chcete, aby mapované spojení pracovalo současně na všech IP adresách tohoto počítače, zadejte tuto adresu jako 0.0.0.0. Jiným řešením je použít pro stejnou IP adresu různá čísla portů.

#### **Příklad použití pro News**

Následující příklad definuje, že všechny počítače z jedné podsítě budou přes jakoukoliv IP adresu počítače s Messaging Serverem spojeny s konkrétním NEWS serverem v Internetu.

192.168.1.0	255.255.255.0	0.0.0.0:news	news_srv.xyz.cz:news
-------------	---------------	--------------	----------------------

## Omezení přístupu určitých uživatelů k Internetu

### Autentifikace do Proxy

Pokud hodláte omezit přístup jednotlivých uživatelů k Internetu pomocí jména a hesla, vyberte v konfiguraci Messaging Serveru službu Proxy a v nastavení zaškrtněte volbu Autentifikace požadována. Po restartu komunikačního serveru bude třeba pro přístup k Internetu nejprve zadat jméno a heslo.

Navíc máte možnost v Administrátorovi ve vlastnostech uživatele nastavit právo na použití Proxy. Kdo toto právo nemá, nedostane se browserem přes Proxy na Internet ani po zadání svého správného jména a hesla.

### Zakázané URL

Existuje i možnost zakázat přístup na konkrétní adresy na Internetu z konkrétních počítačů. To lze provést pomocí nastavení „Zakázaných URL“ v Messaging Serveru v nastavení služby Proxy.

Konfigurační karta umožňuje omezení přístupu uživatelů proxy, SOCKS a DNS na zde specifikované servery, resp. zakazuje převod těchto URL na IP adresy. Uživatelé (stanice v síti), kterým má být zakázán přístup na danou URL adresu, se specifikují pomocí IP adresy a IP masky. Je tedy možné zakázat uvedené URL jen pro jeden počítač, nebo pro celou podsít' apod. Na rozdíl od IP filtru se zde zakázané cílové počítače specifikují svými jmény nebo jejich částmi doplněnými znaky „\*“ a „?“.

#### Příklady

www.pornosoft.com ... zakáže přístup na jediný server konkrétního uvedeného jména

\*kachny\* ... zakáže přístup na všechny servery, v jejichž názvu se vyskytuje řetězec „kachny“

www.ufo.\* ... zakáže přístup na počítač ve všech doménách/zemích (tj. například v doménách com, cz, sk atd.).

Seznam zakázaných URL lze vyexportovat do textového souboru nebo ho lze naopak z textového souboru načíst. Textový soubor musí obsahovat pouze takové řetězce, které obsahují URL adresy (na jednom řádku vždy jedna adresa). Na řádku také mohou být tři položky oddělené mezerami; první dvě položky jsou vstupní adresa a maska, třetí položkou je vlastní URL adresa – podobně jako na konfigurační kartě.

## Nastavení IP filtru (firewall)

Pomocí IP filtru můžete definovat, která spojení prostřednictvím proxy a SOCKS se mohou navazovat. IP filtr se dále používá i pro filtrování přenosu požadavků na SMTP server, Name server (NS) a pro přístup na WWW server, který je součástí Mail602 Messaging Serveru.

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 ze 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 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 k některým počítačům můžete použít filtr zakázaných URL.

## Příklady nastavení IP filtru

- 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

- 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

- Je zapotřebí potlačit funkci firewallu; 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

- Budete chtít povolit komunikaci pouze uživateli s IP 192.168.1.1. Adresy nastavte takto:

semafor	Vstupní adr.	Vstupní maska	Cílová adr.	Cílová maska
zelená	192.168.1.1	255.255.255.255	0.0.0.0	0.0.0.0

## ***Zpřístupnění informací o uživateli (nastavení LDAP)***

### **Administrátor**

Po přihlášení k poštovnímu úřadu klikněte na jeho název a v pravé části okna zvolte „Údaje pro LDAP server“ a vyberte, jaké informace budete navenek o uživateli poskytovat. Tato nastavení se dotkne pouze uživatelů, které Administrátor povolil zobrazovat pomocí LDAP serveru.

Ve vlastnostech konkrétního uživatele nejprve na kartě „Práva a přístup“ zaškrtněte „Zobrazovat údaje v LDAP serveru“. Následně vyplňte informace na kartě LDAP (zobrazeny budou pouze údaje označené symbolem „X“).

### **Messaging Server**

V konfiguraci Messaging Serveru přidejte službu LDAP (pokud ještě není v seznamu aktivních služeb). Jméno a heslo pro administrátorský přístup do LDAP serveru se týká aplikací třetích stran, které mohou zapisovat údaje přímo do LDAP serveru.

## ***Konfigurace odesílání a příjmu SMS***

### **Varianta 1 – pouze odesílání (zdarma)**

Pokud chcete krátké textové zprávy (SMS) odesílat zdarma, přidejte v konfiguraci Messaging Serveru službu SMS a jako zařízení zvolte TCP/IP. Po aktivaci této služby jsou SMS odesílány automaticky pomocí webových stránek mobilních operátorů (u nás Eurotel, Oskar, Paegas). Podmínkou pro používání této služby je fungující připojení k Internetu (lhostejno zda dial-up nebo pevné).

Pokud se Messaging Server nachází za nějakým dalším serverem, který např. plní funkci předřazeného firewallu, lze na záložce TCP/IP nadefinovat použití příslušného druhu proxy.

### **Varianta 2 – odesílání i příjem**

Pokud potřebujete, aby odesílání krátkých textových zpráv (SMS) bylo spolehlivější a byl umožněn i jejich příjem, přidejte v konfiguraci Messaging Serveru službu SMS a jako

zařízení zvolte GSM telefon připojený k serveru. V nastavení služby je třeba ještě na kartě SMS vyplnit číslo servisního centra mobilního operátora, případně i PIN telefonu.

V Administrátorovi lze pak jednotlivým uživatelům nastavit jejich privátní „SMS čísla“ (může to být i řetězec znaků). Pokud přichází SMS obsahuje jako první slovo toto „SMS číslo“, je automaticky doručena přímo do schránky příslušného uživatele.

## ***Antivirová kontrola zásilek***

### **Messaging Server**

Pro fungování antivirové kontroly zásilek komunikačním serverem je třeba mít na počítači s Messaging Serverem nainstalován antivirový systém AVG verze 6.0 od firmy Grisoft (stačí jednouživatelská verze).

Nastavení kontroly se provádí v konfiguraci komunikačního serveru na kartě Antivirová kontrola. Kontrolu lze globálně zapnout či vypnout a stanovit, co se má se zásilkou stát v případě, že v ní je identifikován virus.

## ***Konfigurace spojení Mail602***

Pro přenos zásilek mezi Mail602 poštovními úřady (nebo mezi programem Mail602 Klient a komunikačním serverem) se používá šifrovaný protokol Mail602 s možností komprimace vyvinutý přímo pro toto použití. Vyznačuje se dobrým systémem šifrování (standard, DES - zejména při spojení úřadů přes heslo) a schopností navázání přenosu dat po předchozím předčasném rozpojení přenosu.

Tento protokol je možné použít na řadě přenosových médií, především se jedná o modemy (AT příkazy), ISDN (CAPI rozhraní), TCP/IP (po LAN nebo i s vytáčením).

### **Administrátor**

#### **Nastavení parametrů vlastního úřadu**

Nejprve je třeba provést nastavení týkající se vlastního poštovního úřadu. To lze učinit v hlavní konfiguraci po kliknutí na název poštovního úřadu.

Nastavení se provádí na záložkách dle typu spojení. Zatímco u telefonního spojení se na dolní záložce nastavují tel. čísla, u TCP/IP spojení se nastavují IP adresy. Je možno nastavit až 8 čísel (adres). U telefonního čísla se vždy určuje, zda se jedná o standardní analogovou linku nebo o ISDN (X.75 nebo V.120). Další parametry jsou shodné pro oba typy spojení.



Je vhodné vybrat exportní seznam, který se bude při daném typu spojení implicitně přenášet na protější úřad. Dále je vhodné nastavit maximální čekací dobu (případně i počet zásilek), po které budou zásilky odeslány. V opačném případě budou zásilky odesílány okamžitě po zařazení do výstupní fronty. Samozřejmě, že lze také časově omezit jak příjem, tak i odesílání zásilek.

Přístup pouze přes heslo zabezpečuje poštovní úřad před navázáním spojení se zcela neznámými poštovními úřady. Pokud použijete tuto volbu, nezapomeňte toto heslo nastavit o tři řádky níže.

Automatická výměna zásilek zajišťuje, že při spojení jsou odeslány zásilky pro protější úřad a zároveň jsou přijaty zásilky pro vlastní úřad.

Potvrzování zásilek umožňuje mezi úřady přenášet doručanky, tzn. odesílat potvrzení o přečtení doporučených zásilek.

Při automatické výměně seznamů se mezi poštovními úřady automaticky přenášejí aktualizované exportní seznamy, tj. seznamy dostupných adresátů na příslušném úřadě.

### **Navázání spojení s externím poštovním úřadem**

Pokud chcete navázat spojení s nějakým externím Mail602 poštovním úřadem, přejděte do stromu Připojení a zvolte Protější úřady. Po kliknutí pravým tlačítkem myši v pravé části okna zvolte Nový.

Většina parametrů se nastavuje shodně s předchozím tématem (jako u vlastního úřadu) s tím rozdílem, že se navíc zadává např. tel. číslo (IP adresa) protějšího úřadu.

Také se specifikuje, jak často má náš úřad (server) zjišťovat, zda se na protějším úřadu nenachází nějaká pošta určená právě pro něho.

### **Princip zálohování spojení**

V případě, že pro protější úřad zvolíte oba typy spojení (telefonní i TCP/IP), pak v jeho vlastnostech můžete určit, který druh spojení bude preferován pro prvních „x“ pokusů. Pokud se spojení nepodaří po „x“ pokusech navázat, začne se zkoušet alternativní spojení.

Např. Pětikrát se zkusí spojení po TCP/IP a pokud se nepovede navázat, dojde k pokusu o navázání přímého modemového spojení (třeba po ISDN).

### **Exportní seznamy**

Pomocí exportních seznamů může administrátor definovat, jací uživatelé mají být „nabízeni“ ke komunikaci protějším Mail602 poštovním úřadům. Exportních seznamů lze

založit několik a používat je dle potřeby – např. v jednom budou uvedeni pouze obchodní zástupci pro Čechy a ve druhém jen pro Slovensko. Pro komunikaci s partnery na Slovensku pak administrátor nastaví seznam obsahující pouze obchodní zástupce ze Slovenska.

### **Telefonický a TCP/IP přístup programem Mail602 Klient**

Pokud má mít uživatel možnost přistupovat k poště programem Mail602 Klient protokolem TCP/IP nebo modemem, je třeba mu ve vlastnostech povolit „TCP/IP a Telefonní přístup“. Další nastavení se provádí po rozbalení stromu Připojení. Je třeba nastavit parametry pro „Tel. a TCP/IP přístup“.

Položka exportní seznam specifikuje seznam lokálních uživatelů (může být i upravený), který bude mít klient při tel/TCP přístupu k dispozici.

Pro zvýšení bezpečnosti poštovního úřadu lze říci, že při tel/TCP přístupu bude nejprve ověřeno heslo pro přístup k poštovnímu úřadu, a teprve pak se bude ověřovat jméno a heslo uživatele.

Uživatele přistupujícího po tel/TCP lze omezit maximální velikostí odesílaných resp. přijímaných zásilek a také časově – kdy nemůže služeb poštovního úřadu/serveru využívat.

Na závěr je třeba specifikovat, jaké zásilky může takto připojený uživatel odesílat :

- standardní = e-mailly,
- faxy,
- Z-Modem = pouze data.

### **Messaging Server**

Službu Mail602 lze při přidávání klasicky přiřadit buď k protokolu TCP/IP nebo k modemu (CAPI ISDN, TAPI zařízení, COM port). Je také možno mít službu přidanou dvakrát (jednou pro TCP/IP a podruhé pro modem), čehož se využívá při zálohování spojení.

Ve vlastnostech služby Mail602 lze na záložce Služba specifikovat používanou úroveň šifrování při přenosu a pracovní intervaly. Také lze specifikovat, zda mají být zásilky při přenosu komprimovány.

Při použití ISDN nezapomeňte na stejnojmenné záložce zadat telefonní číslo, na kterém bude server naslouchat.

## Klientské programy

- **Mail602** – přístup pomocí programu Mail602 Klient po lokální síti, protokolem TCP/IP (i přes Internet) nebo přímo modem-modem,
- **POP3** – např. MS Outlook Express, Netscape Messenger,
- **MAPI** – přístup z MS Outlook 9x/2000,
- **WWW/WAP** – přístup do pošty z browseru/mobilního telefonu.

## Digitální podpis a šifrování zásilek (S-MIME)

Abyste mohli začít využívat technologie S-MIME pro digitální podepisování a/nebo šifrování zásilek, musíte nejprve získat tzv. certifikát (nebo také Digital ID), který obsahuje Váš veřejný klíč certifikovaný nějakou certifikační autoritou.

### Jak získat certifikát

Pro získání certifikátu je třeba o něj nejprve zažádat na www stránkách certifikační autority (u nás např. na [www.ica.cz](http://www.ica.cz)). Při podávání žádosti vygeneruje browser unikátní dvojici klíčů – soukromý a veřejný, načež veřejný předá certifikační autoritě k certifikaci. Ta po ověření totožnosti (v případě testovacích certifikátů bez ověření) vydá žadateli certifikát.

Žádost o certifikát a jeho následnou instalaci je vhodné provádět z browseru, se kterým „spolupracuje“ klientský program pro práci s poštou, jenž hodláte v budoucnu používat. V opačném případě je nutno klíč nejprve vyexportovat a následně nainportovat do příslušného browseru.

Do kterého browseru certifikát instalovat a jak certifikát vyexportovat se dozvíte v následujících odstavcích.

### Důležitá upozornění

Soukromý klíč je vygenerován a uložen na počítači, ze kterého byla podána žádost o certifikát. Navíc je dostupný pouze tomu uživateli, který ho vygeneroval. Certifikát je svázán s e-mailovou adresou. V případě její změny je nutno žádat o nový certifikát. Pokud chcete certifikát a soukromý klíč přenést na jiný počítač, je třeba ho nejprve vyexportovat.

***Doporučujeme Vám si certifikát včetně soukromého klíče vyexportovat a zálohovat na bezpečné místo, neboť v případě jeho ztráty či poškození (např. při porušení instalace Windows) si nebudete moci Vám (i dříve) doručené zašifrované e-maily přečíst !***

***Je třeba zajistit maximální možnou ochranu soukromého klíče, tj. zabezpečit přístup ke klíči i do Windows heslem (příp. i do počítače) atp.***

### **Internet Explorer a správa certifikátů**

Instalaci certifikátu do Internet Exploreru je třeba provést v případě, že chcete používat některý z následujících poštovních programů :

- Mail602 Klient,
- MS Outlook Express,
- MS Outlook 98/2000.

Export certifikátu včetně soukromého klíče je dostupný posloupností Nastavení – Možnosti sítě Internet – záložka Obsah – Certifikáty – po výběru tlačítko Exportovat.

### **Netscape Communicator a správa certifikátů**

Instalaci certifikátu do Netscape Communicatoru je třeba provést v případě, že chcete pro práci s elektronickou poštou využívat Netscape Messenger, který je jeho součástí.

Export certifikátu včetně soukromého klíče je dostupný posloupností Communicator – Tools – Security Info – položka Yours pod Certificates – po výběru tlačítko Export.

### **Jak odeslat digitálně podepsanou a/nebo zašifrovanou zasilku**

Než začnete posílat digitálně podepsané či zašifrované zasilky, je třeba nastavit Vámi používaný klientský program – viz následující odstavce.

Pokud chcete někomu poslat digitálně podepsanou zasilku, stačí pak v klientském programu zvolit (stisknout tlačítko) digitálně (elektronicky) podepsat (někdy také parametr Signed) a zprávu odeslat.

Pokud chcete, aby byla zasilka i zašifrovaná a její obsah nemohl rozšifrovat nikdo jiný než její oprávnění příjemce, zvolte „Zašifrovat“. To můžete ale udělat až poté, co získáte certifikát adresáta Vaší zasilky a přiřadíte ho k odpovídající adrese v seznamu adresátů. Pokud tedy ještě tento certifikát nemáte, nechte si od Vašeho korespondenčního partnera poslat digitálně podepsanou zasilku, ve které je certifikát automaticky obsažen.

### **Nastavení Mail602 Klient**

V menu Nastavení vyberte Nastavení prostředí Mail602 Klienta a zvolte záložku Bezpečnost. Z nabídky aliasů vyberte e-mailovou adresu, k níž hodláte získaný certifikát přiřadit, a stiskněte tlačítko Vybrat. Ze seznamu certifikátů vyberte ten, který chcete používat.

Dále můžete upravit upřednostňovaný šifrovací algoritmus, a také kdy Vás má program upozornit, že úroveň šifrování použitá v nějaké zásilce je příliš nízká (nebezpečně).

Z důvodu zachování kompatibility se staršími klientskými programy při posílání digitálně podepsaných zásilek doporučujeme zaškrtnout volbu Používat oddělený podpis.

Pokud si chcete uložit adresu odesílatele digitálně podepsané zasilky spolu s jeho certifikátem tak, abyste mu mohli příště poslat zašifrovanou zasilku, vyberte Vlastnosti zasilky a po volbě Uložit adresu odesílatele přiřaďte k adrese tlačítkem Vybrat z nabídnutého seznamu příslušný certifikát. Pak již můžete adresu uložit do libovolného seznamu.

## Nastavení Outlook Express

V aplikaci Outlook Express není třeba provádět žádná nastavení. Při prvním pokusu o odeslání digitálně podepsané zprávy budete pouze vyzváni k potvrzení certifikátu (Digital ID), který chcete používat. Vše ostatní již aplikace nastaví automaticky za Vás.

## Nastavení MS Outlook 9x/2000

V menu Nástroje zvolte Možnosti a záložku Zabezpečení. Po stisku tlačítka nastavit zabezpečenou el. poštu zadejte nějaký název (formát ponechte S/MIME). Zaškrtněte obě volby o výchozím nastavení a tlačítkem vybrat vyberte Podpisové osvědčení (Osvědčení zašifrování se vyplní automaticky.). Ponechte zaškrtnutou volbu o posílání těchto osvědčení se zabezpečenými zprávami.

## Nastavení Netscape Messenger

Netscape Communicator je nastaven pro posílání digitálně podepsaných a/nebo šifrovaných zásilek automaticky po instalaci certifikátu.

# Mail602 Klient

Existují dva základní typy instalace programu Mail602 Klient :

- uživatelský,
- administrátorský.

## Uživatelská instalace programu Mail602 Klient

Slouží k instalaci programu Mail602 Klient na lokální pevný disk na počítači v síti.

- Instalace se spouští z adresáře MESSAG\MAIL602\USER\Disk1.
- Po spuštění stačí zadat identifikační údaje (jméno a firmu), zvolit cílový adresář.

## Administrátorská instalace programu Mail602 Klient

Instalace se spouští z adresáře MESSAG\MAIL602\NETINST\Disk1. Instaluje program Mail602 Klient na síť, přičemž lze volit ze dvou možností. Po spuštění administrátorské instalace, budete moci po zadání identifikačních údajů a cílového adresáře zvolit jednu ze dvou možností :

- **Kopírování instalačních souborů** – výsledkem je pouze **kopie** instalačních souborů na síťovém disku, která obsahuje předvolené typy přístupů k poště. Uživatelé pak mohou instalovat program Mail602 Klient na svůj lokální disk ze sítě. Každý uživatel má tedy na konec program na svém lokálním disku.
- **Instalování síťové instalace** – provede instalaci programu Mail602 Klient na síťový disk, odkud potom program spouští uživatelé. Nejprve ale musí ze síťového adresáře spustit setup.exe, který jim vytvoří ikony, tiskárnu Fax602 a zaregistruje aplikaci.. Program je tedy nainstalován pouze na síťovém disku a uživatelé u sebe mají pouze konfigurační soubory.

## POP3 klient

Hlavní výhodou použití POP3 klienta (např. MS Outlook Express) je to, že je zdarma součástí operačního systému Windows a uživatelé ho zpravidla používají i doma pro práci se svou soukromou elektronickou poštou.

### *Obecně*

Pro POP3 přístup je také třeba provést určitá nastavení v Administrátorovi a Messaging Serveru – viz výše. Dále je v konfiguraci libovolného POP3 klienta (např. MS Outlook Express, Netscape Messenger, ...) třeba nastavit :

- Vaši e-mailovou adresu nastavte na uživatel@doména, kde doména odpovídá doméně zadané v závěru instalace poštovního úřadu,
- adresu serveru s odesílanou a příchozí poštou (SMTP a POP3 serveru) nastavte na IP adresu počítače s Mail602 Messaging Serverem,
- pokud je to třeba, vyberte typ serveru s příchozí poštou POP3,
- název účtu (uživatelské jméno) a heslo odpovídá Vašemu jménu a heslu uživatele v poštovním úřadu,
- pro zjednodušení práce je vhodné potvrdit volbu Zapamatovat heslo.

## ***Jak faxovat z POP3 klienta ?***

Uživatelé POP3 klientských programů (např. MS Outlook Express, Netscape Messenger, apod.) mohou odesílat faxy v zásadě dvěma způsoby :

- odesláním e-mailu na adresu ve formátu číslo@fax,
- tiskem na tiskový ovladač Fax602, který je součástí instalace programu SendFax.

Zkontrolujte si také nastavení Messaging Serveru a Administrátora, která souvisejí s POP3 klienty – viz výše.

### **Faxování přímo z poštovního klienta**

Fax lze napsat a odeslat přímo a jednoduše jako standardní e-mail na adresu ve formátu číslo@fax (např. 420-2-22011218@fax). Messaging Server obsah dopisu převede na fax a odešle ho na číslo, které je součástí adresy. Převod faxu včetně souborů připojených k záznamu probíhá pomocí vnitřních funkcí programu (většinou grafické formáty) nebo pomocí funkcí OLE automation voláním asociovaných aplikací (např. MS Word pro formát DOC, atd.).

Pokud používáte MS Outlook Express nebo MS Outlook 9x/2000, 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 je třeba povolit zaškrtnutím políčka v konfiguračním dialogu programu SendFax.

### **Tisk na tiskárnu Fax602 a nastavení programu SendFax**

Druhý způsob faxování spočívá v tisku na virtuální tiskárnu-faxový ovladač, který je součástí instalace programu SendFax. Tak lze faxovat z libovolné Windows aplikace, která umožňuje volbu tiskárny. Pro faxování pak jen stačí nastavit jako tiskárnu Fax602 a po zvolení adresáta přímo z Adresáře Outlook Express je fax odeslán. Adresy lze volit také z adresářů poštovních programů podporujících standardní rozhraní MAPI (např. z Kontaktů v MS Outlooku 9x/2000) nebo Simple MAPI (např. Netscape Messenger).

Instalace programu SendFax se spouští z adresáře MESSAG\POP3\Disk1.

V programu SendFax je třeba nastavit tři (v některých případech čtyři) položky :

- **602Pro Server** – IP adresa počítače, na němž běží Messaging Server.
- **Vaše e-mail adresa** – zpravidla ta, kterou máte nastavenou v POP3 klientovi.
- **Seznamy** - program SendFax si neudrhuje vlastní seznamy faxových adresátů - ty je třeba udržovat v jednom z nabízených klientských programů - buď MS Outlook Express nebo některý MAPI klient, například MS Outlook 9x/2000, případně některý Simple MAPI klient (např. Netscape Messenger).

- **Automatická konverze faxových adres/zásilek** - Pokud používáte MS Outlook Express nebo MS Outlook 9x/2000, můžete si faxová čísla zapisovat přímo do příslušných položek v Kontaktech (fax do zaměstnání, fax domů), a ty pak využít při posílání faxových zásilek. Jinou možností je faxové číslo zadat do adresáře přímo jako standardní e-mail adresu ve formátu číslo@fax (např. 420-2-22011218@fax).

## ***Jak nakonfigurovat SSL SMTP a POP3 ?***

Zabezpečení SMTP a POP3 serveru pomocí SSL zabraňuje mj. „odposlechu“ Vašeho hesla i Vašich e-mailů na cestě mezi SMTP/POP3 serverem a Vaším počítačem.

Pokud chcete, aby práce s Vaší POP3 schránkou a komunikace s SMTP serverem probíhala šifrovaně pomocí SSL, je třeba toto nastavit jak v Messaging Serveru, tak v klientském programu.

### **Nastavení POP3 klientů**

V programu **Outlook Express** je ještě třeba kromě standardního nastavení ve vlastnostech poštovního účtu na záložce „Upřesnit“ zaškrtnout pod čísla portů pro SMTP a POP3 volbu zabezpečení přes SSL. Dále u SMTP přepsat číslo portu na 2525 a provedená nastavení potvrdit.

V jiných programech postupujte dle jejich nápovědy nebo manuálu.

**Pozn.** V programu Netscape Messenger je SSL přenos implementován jako extenze protokolu SMTP, což bohužel není s Mail602 Messaging Serverem verze 4.0 kompatibilní.

## ***Vyhledávání e-mailových adres a informací u uživatelích***

### **Outlook Express**

Zvolte v menu **Nástroje – Účty** a po stisku tlačítka **Přidat** vyberte **Adresářová služba**. Jako adresu LDAP serveru zadejte IP adresu počítače s Mail602 Messaging Serverem. Na závěr vyberte právě zadanou adresářovou službu a v jejích vlastnostech na kartě **Upřesnit** zadejte jako výchozí bod vyhledávání **c=CZ**.

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

### **Netscape Messenger**

V menu **Communicator** zvolte **Address Book**. V okně **Address Book** vyberte v menu **File – New Directory**. Adresářovou službu si libovolně pojmenujte, do řádky **LDAP server**



zadejte IP adresu počítače s Mail602 Messaging Serverem a do řádky Search Root zadejte c=CZ.

Pokud chcete pomocí této Adresářové služby vyhledávat klikněte na ni v levé části okna nebo si ji předvolte v konfiguraci programu.

## **MAPI klient (MS Outlook 9x/2000)**

MAPI podporu je třeba nainstalovat na všechny stanice, ze kterých budou uživatelé přistupovat k poštovnímu úřadu systému Mail602 programy MS Outlook 9x/2000.

### ***Instalace MAPI podpory***

Před instalací MAPI podpory je třeba nastavit MS Outlook 9x/2000 jako výchozího poštovního klienta (zpravidla v nastavení Internet Exploreru na záložce Programy).

Instalace se spouští z adresáře MESSAG\MAPI\Disk1. Instalace probíhá automaticky a na jejím závěru se spustí průvodce nastavením profilu pro MS Outlook 9x/2000.

Z nabízených služeb vyberte Mail602 služby, a pak vyplňte název profilu. Následně zadejte „cestu na EMI“ (cestu k poštovnímu úřadu) a vyplňte jméno a heslo uživatele.

Vyberte si způsob zpracování zásilek a pokud hodláte používat pro práci s poštou pouze (většinou) MS Outlook 9x/2000, zaškrtněte příslušnou volbu. Tato dvě nastavení lze kdykoliv změnit z Ovládacích panelů volbou Pošta (Mail602 služby-Vlastnosti-karta Došlá pošta).

Doporučujeme ještě zkontrolovat nastavení ukládání osobních adres. Nastavení lze provést opět přes Ovládací panely volbou Pošta na záložce Adresy. Je třeba mít nastaven konkrétní vlastní adresář nebo Kontakty.

### ***Přístup k poště a nastavením systému Mail602***

Pro nastavení parametrů a funkcí systému Mail602 je po instalaci MAPI podpory v Outlooku dostupná nová záložka Mail602 v menu Nastavení-Možnosti.

Zde lze mj. nastavit automatické třídění došlé pošty – odpovědi, postupování, SMS avíza na mobilní telefon apod.

Složky systému Mail602 (Došlá pošta, Archiv, Fronty zásilek, atd.) se zobrazí v seznamu složek, který lze buď zobrazit trvale přes menu Zobrazit nebo jen dočasně kliknutím na název otevřené složky (např. Doručená pošta).

## Poznámky

Pokud chcete zadat ručně adresáta faxu, zadejte do elektronické adresy faxové číslo a jako typ el. adresy vyplňte FAX602.

## WWW klient

Nejjednodušší a zároveň nejuniverzálnější způsob pro práci s poštou v systému Mail602 představuje WWW Klient, pro jehož používání stačí mít nainstalovaný pouze browser (např. Internet Explorer).

Pro vyvolání WWW klienta stačí do browseru zadat URL ve tvaru `http://server/mail` nebo pro přístup zabezpečený pomocí SSL pak `https://server/mail` (kde server je buď IP adresa počítače s Messaging Serverem nebo jeho název). Po zadání jména a hesla lze již normálně pracovat s poštou.

**Upozornění :** Při úplně prvním vyvolání WWW klienta je třeba zadat kromě jména a hesla i cestu k poštovnímu úřadu (nejlépe ve tvaru `\\server\cesta`).

**Pozn. :** WWW klient je součástí instalace komunikačního serveru.

## WAP klient

Do pošty lze přistupovat i z mobilních telefonů podporujících protokol WAP. Pomocí WAP klienta lze provádět základní operace s poštou, jako je odesílání nové a čtení, odpovídání a mazání došlé pošty.

WAP klient je přístupný po zadání cesty `http://server/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.).

**Pozn.** Pro využívání WAP klienta je třeba, aby byla v rámci Messaging Serveru zprovozněna služba WWW a aby byl tento server přímo přístupný z Internetu. Rovněž je třeba uskutečnit nejprve alespoň jeden přístup z WWW klienta, při kterém dojde k zadání cesty k poštovnímu úřadu.

**Pozn. :** WAP klient je součástí instalace komunikačního serveru.

## Systémové požadavky

### Sít'

- Libovolná kombinace Novell Netware, Windows 9x/2000/NT.
- Pro přístup na Internet a vzdálenou správu je vyžadován protokol TCP/IP.
- Libovolné připojení k Internetu (pevná linka i dial-up), se statickou případně dynamickou IP adresou.

### Server

- Počítač s procesorem Pentium a vyšším,
- operační systém Windows 9x/2000/NT (pro vzdálenou správu je vyžadován systém Windows 2000/NT),
- minimální doporučená velikost paměti je 32 MB (Win 9x) a 64 MB (ostatní),
- místo na disku cca 25 MB (další místo je třeba pro poštu),
- volitelně faxmodem, ISDN zařízení, Dialogic fax, SMS brána apod.

**Pozn.:** Pošta (soubory tvořící poštovní úřad) může být uložena na jiném file serveru.

### Stanice

- Hardware odpovídající použitému operačnímu systému,
- operační systém dle používaného klientského programu :
  - browser nebo POP3 klient – libovolný systém s podporou TCP/IP,
  - MAPI nebo Mail602 klient – Windows 9x/2000/NT,
- (pro vzdálenou správu ze stanice je vyžadován systém Windows 98/2000/NT),
- (místo na disku pro program Mail602 Klient cca 9 MB).

**Pozn.:** Program Mail602 Klient bez podpory některých funkcí existuje i v 16-bitové a MS-DOS verzi.