System i

Электронная почта в сети

версия 6 выпуск 1

System i

Электронная почта в сети

версия 6 выпуск 1

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом ознакомьтесь со сведениями, приведенными в разделе “Примечания”, на стр. 55.

Это издание относится к версии 6, выпуску 1, модификации 0 продукта IBM i5/OS (код продукта 5761-SS1), а также ко всем последующим выпускам и модификациям, если в новых изданиях не будет указано обратное. Данная версия работает не на всех моделях систем с сокращенным набором команд (RISC) и не работает на моделях с полным набором команд (CISC).

© Copyright International Business Machines Corporation 1998, 2008. Все права защищены.

Содержание

© Copyright IBM Corp. 1998, 2008

Электронная почта

Эта информация пригодится вам для планирования, настройки, применения, устранения неполадок электронной почты и управления ею в вашей системе.

Предполагается, что вы уже работали с операционной системой i5/OS и имеете представление о работе с TCP/IP, Простом протоколе передачи почты (SMTP) и об организации электронной почты.

Новое в выпуске V6R1

В данном разделе приведена информация о новинках и существенных изменениях в наборе разделов, посвященных электронной почте, в выпуске V6R1.

Поддержка SMTP S/MIME

Протокол защищенные/Многоцелевые расширения почты Internet (S/MIME) может использоваться для проверки отправителей при выполнении многочисленных транзакций согласно протоколу доставки SMTP. Этот протокол позволяет создавать электронные подписи и зашифровывать документы электронной почты. Новый интерфейс API QtmsCreateSendEmail предусматривает поддержку S/MIME.

В следующих разделах приводится определение S/MIME и действий по настройке, необходимых в случае применения в сценарии нового API:

- “Основы электронной почты” на стр. 2
- “Сценарий: Настройка API QtmsCreateSendEmail для использования протокола S/MIME” на стр. 7

Идентификация SMTP и поддержка SSL/TLS

Идентификация SMTP позволяет отслеживать отправителя электронной почты. Сервер i5/OS SMTP также поддерживает сеансы, защищенные с применением SSL или TLS.

- “Управление доступом к SMTP” на стр. 11
- “Мониторинг отправителя электронной почты” на стр. 26

Поддержка SSL/TLS сервером POP

Сервер POP i5/OS теперь поддерживает сеансы SSL/TLS. Этот сервер позволяет шифровать ИД пользователей и пароли.

- “Настройка почтовых клиентов POP” на стр. 31

Как просмотреть новые и измененные функции выпуска

Для того чтобы облегчить поиск изменений, в документации используются следующие значки:

- Значок » отмечает начало новой или измененной информации.
- Значок « отмечает конец новой или измененной информации.

В файлах PDF напротив новой или измененной информации вы можете заметить символы исправлений в виде вертикальной черты (|) на полях слева.

Сведения о других изменениях, появившихся в этом выпуске, можно найти в разделе Информация для пользователей.

© Copyright IBM Corp. 1998, 2008

Файл PDF об электронной почте

Файл PDF этой информации можно просмотреть и напечатать.

Для просмотра или загрузки этого документа в формате PDF выберите ссылку E-mail (около 692 Кб).

Сохранение файлов PDF

Для сохранения файла PDF на рабочей станции (для последующего просмотра и печати) выполните следующие действия:

1. Щелкните правой кнопкой мыши на приведенной ссылке на документ PDF.
2. Щелкните на опции локального сохранения PDF.
3. Выберите каталог, в котором следует сохранить файл PDF.
4. Щелкните на **Сохранить**.

Загрузка программы Adobe Reader

Для просмотра и печати этих PDF-файлов требуется программа Adobe Reader. Бесплатную копию этой программы можно загрузить с Web-сайта Adobe по адресу Adobe

(www.adobe.com/products/acrobat/readstep.html) .

Ссылки, связанные с данной

“Связанная информация по работе с электронной почтой” на стр. 52
В инструкциях к продуктам, публикациях IBM Redbooks, на Web-сайтах и в других сборниках разделов информационного центра содержится информация, связанная с разделами о работе с электронной почтой. Файлы PDF можно и просматривать, и печатать.

Основы электронной почты

Электронная почта - важный деловой инструмент. Операционная система i5/OS поддерживает протоколы SMTP и POP, позволяющие быстро обмениваться электронной почтой.

Методы рассылки

Ниже описаны дополнительные аспекты организации электронной почты, в частности, методы рассылки:

- Многоцелевые расширения почты Internet (MIME)

  Протокол MIME представляет собой стандартный метод организации различных форматов файлов. По протоколу SMTP можно передавать лишь текст, состоящий из 7-значных символов ASCII, длиной не более 1000 символов. Стандарт MIME был разработан для поддержки более сложных форматов файлов, таких как текст с форматированием, изображения, а также аудио- и видеофайлы. MIME преобразует файлы двоичного типа в данные SMTP, разделяя различные типы файлов в сообщении с помощью заголовков, прежде чем отправить сообщение по протоколу SMTP. Почтовый клиент, в свою очередь, получает сообщение и преобразует его с помощью заголовков MIME в файлы соответствующих типов.
- S/MIME

  Secure/MIME - это защищенная версия протокола MIME, позволяющая пользователям отправлять зашифрованные почтовыые сообщения с электронными подписями даже при работе с различными почтовыми программами.
- Среда AnyMail/400

  Вся почта, поступающая по протоколу SMTP и предназначенная для локальных пользователей (пользователей с учетными записями в данной системе), обрабатывается средой AnyMail/400. Среда почтового сервера - это система распределения электронной почты. Для обработки некоторых типов почтовых сообщений среда почтового сервера вызывает программы выхода, или подключаемые программы.

- службы рассылки SNA (SNADS)

  Служба рассылок системной сетевой архитектуры (SNADS) - это асинхронная служба рассылки IBM, определяющая набор правил для получения, маршрутизации и отправки почтовых сообщений в сети. В данном разделе SNADS обозначает тип пользовательского профайла, у которого в параметре **Предпочитаемый адрес** указано значение **ИД пользователя/Адрес**.С помощью параметра Предпочитаемый адрес среда почтового сервера определяет, в каких полях системного каталога рассылки указан применяемый адрес.

  Понятия, связанные с данным

  “Отправка и получение электронной почты” на стр. 30
  Ваша система может работать как почтовый сервер, на котором зарегистрированы пользователи электронной почты (SNADS, POP или Lotus).Пользователи могут отправлять, получать и читать свою почту с помощью программ-клиентов POP или SNADS.

  Задачи, связанные с данной

  “Блокировка очередей SNADS” на стр. 13
  Очереди рассылки SNADS, которые приложение SMTP использует для распределения электронной почты, можно заблокировать. Это обеспечивает дополнительную защиту, ограничивая распределение электронной почты.

Простой протокол передачи почты (SMTP) в i5/OS

Простой протокол передачи почты (SMTP) обеспечивает возможность отправки и приема почтовых сообщений операционной системой.

SMTP используется для организации непрерывной цепочки доставки почты от одного почтового сервера другому. Между отправителем (клиентом) SMTP и получателем (сервером) SMTP устанавливается прямое соединение. Клиент SMTP хранит почту на компьютере-отправителе, пока она не будет передана и успешно скопирована на сервер SMTP.

SMTP в этой операционной системе поддерживает рассылку записок, сообщений и документов в формате ASCII. Кроме обычного текстового формата, SMTP может поддерживать и другие форматы; для этого применяется протокол MIME. MIME - это стандарт Internet, обеспечивающий передачу почтовых сообщений с заголовками, описывающими содержимое сообщения для клиента. Эти сообщения могут содержать видео- и аудиоданные, а также двоичные файлы.

Доставка почты SMTP

Для того чтобы почта дошла по назначению, необходимо, чтобы протокол SMTP смог доставить ее, во-первых, на нужный хост и, во-вторых, нужному пользователю на этом хосте. Предположим, почта отправляется по адресу bobsmith@mycompany.com.

Прежде всего SMTP проверяет, принадлежит ли указанный электронный адрес (bobsmith) пользователю в локальной системе. Если нет, SMTP отправляет почту на следующий хост. Следующий хост может быть либо конечным хостом, либо промежуточным. Имя хоста определяется на основании информации об адресах, заданной в конфигурации протокола SMTP.

Затем SMTP преобразует адрес хоста, используя для этого сервер имен доменов (DNS) или локальную таблицу хостов. Имя хоста входит в учетную запись пользователя электронной почты (mycompany.com); IP-адрес применяется SMTP для определения почтового сервера, на который нужно отправлять почту (192.1.1.10).

1. При поиске сервером SMTP идресов имен хостов в таблице локальных хостов, адреса IPv6 игнорируются.
2. Если какие-либо из настроенных серверов DNS имеют адреса IPv6, тогда все серверы DNS должны поддерживать функцию рекурсии, чтобы распознавать почтовые домены, для которых эти настроенные серверы считаются не имеющими прав доступа.

Взаимодействие DNS и SMTP описано в следующих разделах:

- Настройка домена DNS
- Записи о почтовом шлюзе и записи типа MX

При приеме входящей почты сервер SMTP сначала преобразует имя целевого хоста в IP-адрес. Из-за того, что предусмотрена возможность создания псевдонимов, у сервера может быть несколько имен хостов. Сервер SMTP с помощью интерфейса сокетов определяет, принадлежит ли этот IP-адрес локальному хосту.

Понятия, связанные с данным

DNS

Записи о почтовом шлюзе и записи MX

Задачи, связанные с данной

Настройка домена DNS

“Настройка электронной почты” на стр. 14
Для того чтобы настроить электронную почту на своей системе, нужно настроить TCP/IP и сервера SMTP и POP и запустить почтовые сервера.

Почтовый протокол POP в i5/OS

Сервер Почтового протокола (POP) - это реализация интерфейса протокола POP версии 3 на сервере i5/OS.

Сервер POP поддерживает в этой операционной системе электронные почтовые ящики, из которых клиенты могут получать почту. Этот сервер могут применять все почтовые клиенты, поддерживающие протокол POP3, например, Netscape Mail, Outlook Express и Eudora. Клиенты могут работать в любой операционной системе: Windows, Linux, AIX или Macintosh.

Сервер POP выполняет роль временного хранилища сообщений до получения их почтовым клиентом. При подключении к серверу почтовый клиент проверяет содержимого почтового ящика. При наличии новых сообщений клиент получает их по одному. После получения сообщения клиент помечает его для удаления при завершении сеанса. После получения всех сообщений почтового ящика клиент передает команду завершения сеанса, после которой сервер удаляет все сообщения, помеченные для удаления, и отключается от клиента.

Для работы с сервером клиенты POP применяют *глагольные команды*.Команды, поддерживаемые сервером POP для данной операционной системы, описаны в разделе Почтовый протокол POP.

Задачи, связанные с данной

“Доступ к серверам электронной почты с помощью System i Navigator” на стр. 15
С помощью System i Navigator можно настроить работу с почтовыми серверами SMTP и POP.

“Настройка серверов SMTP и POP для электронной почты” на стр. 16
Работа электронной почты в системе обеспечивается двумя протоколами: SMTP (Простой протокол передачи почты) и POP (Почтовый протокол).

Ссылки, связанные с данной

“Протокол POP” на стр. 48
Почтовый протокол POP версии 3 описан в RFC 1939 (POP3), RFC 2449 (Механизм расширения POP3) и RFC 2595 (Использование TLS с IMAP, POP3 и ACAP). RFC - это разрабатываемые стандарты Internet.

Информация, связанная с данной

RFC Index

Сценарии: электронная почта

В этих сценариях показана передача электронной почты между локальными пользователями и способы настройки QtmsCreateSendEmail API для работы с S/MIME.

Сценарий: Отправка и получение почтовых сообщений в локальной системе

В этом сценарии показана передача электронной почты между локальными пользователями.

Ситуация

Джейн Смит, заведующей отделом кадров, нужно отправить сообщение Сэму Джонсу в юридический отдел. Они оба работают в штаб-квартире компании MyCompany. На следующем примере показан пример обработки электронной почты в системе.

Этот пример преследует следующие цели:

- Продемонстрировать взаимодействие почтового клиента и сервера, а также процесс обработки сообщения
- Отправить почту с помощью сервера SMTP
- Доставить почту пользователю POP

Сведения

Джейн пользуется почтовым клиентом Netscape. Она пишет сообщение и отправляет его по адресу SamJones@mycompany.com. На следующем рисунке проиллюстрирован путь почтового сообщения в сети.

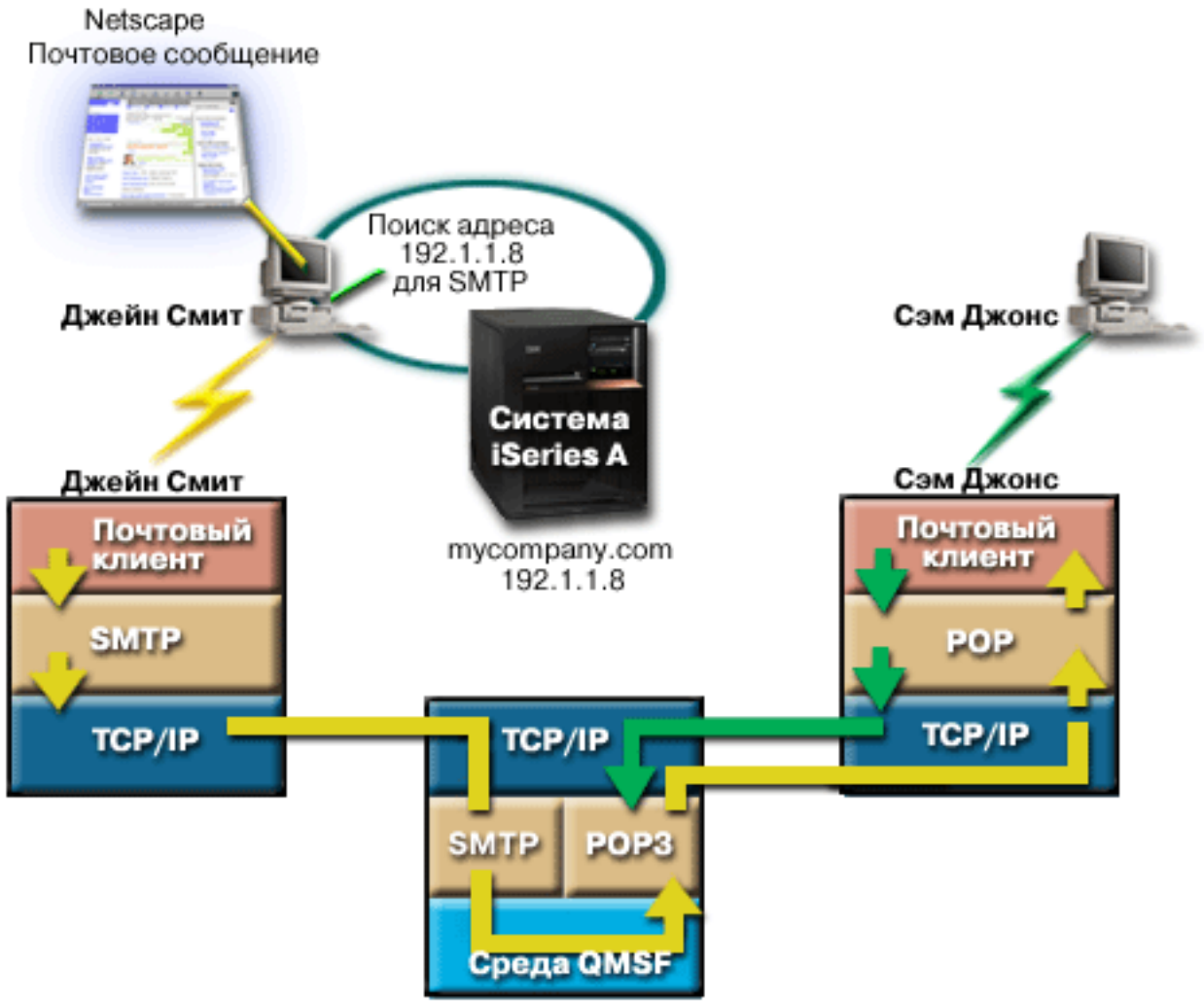

Рисунок 1. Пример настройки сети

Ниже описан каждый этап пути почтового сообщения в сети.

Этап 1: Клиент SMTP отправляет сообщение на сервер SMTP

Клиент SMTP на компьютере Джейн применяет данные конфигурации, заданные для сервера исходящей почты и для идентификации. В поле **От** указывается значение поля имени пользователя.Сервер исходящей почты - это хост, с которым связывается клиент SMTP на PC. Поскольку адрес указывается в виде доменного имени, то клиент SMTP запрашивает IP-адрес сервера SMTP у DNS и получает значение 192.1.1.8.

Клиент SMTP подключается к серверу SMTP через порт SMTP (порт 25 по адресу 192.1.1.8). Клиент и сервер обмениваются информацией с помощью протокола SMTP. Сервер SMTP принимает запрос на доставку почты, и сообщение передается клиентом на сервер по протоколу TCP/IP.

Этап 2: Сервер SMTP доставляет сообщение на сервер POP

Сервер SMTP проверяет имя домена получателя, чтобы определить, является ли получатель локальным. Так как получатель является локальным, почта записывается в файл интегрированной файловой системы, а информация сообщения с помощью API среды QMSF Создать сообщение помещается в очередь QMSF. Среда QMSF рассылает электронную почту, вызывая программы выхода или подключаемые программы для

обработки конкретных типов почтовых сообщений. В информации сообщения адрес Сэма указан в формате SMTP, поэтому среда вызывает программу выхода Преобразование адресов SMTP. Эта программа еще раз проверяет, является ли сообщение локальным. Так как сообщение действительно является локальным, программа с помощью системного каталога рассылки (данных, введенных командой WRKDIRE) находит адрес SMTP получателя. Программа находит адрес Сэма, а также обнаруживает в записи каталога для этого пользователя, что уровень обслуживания почты - системное хранилище сообщений; поэтому программа распознает его как учетную запись POP. После этого программа Преобразование адресов SMTP добавляет информацию профайла пользователя в сообщение. Она помечает информацию как локальную доставку POP. После этого среда QMSF вызывает программу выхода Локальной доставки POP, которая находит информацию профайла и имя файла интегрированной файловой системы и доставляет сообщение в почтовый ящик Сэма.

Этап 3: Клиент POP получает сообщение для Сэма Джонса с сервера POP

Немного позже Сэм решает проверить электронную почту. Клиент POP на его PC проверяет почту на сервере POP mycompany.com, передав имя пользователя SamJones и пароль (******). Имя домена вновь преобразуется в IP-адрес (с помощью DNS). Клиент POP связывается с сервером POP через порт POP с помощью протокола POP3. Сервер POP в операционной системе сравнивает имя пользователя почтового ящика и пароль с профайлом и паролем пользователя i5/OS. После проверки по имени профайла определяется почтовый ящик Сэма. Клиент POP загружает сообщение и отправляет запрос на сервер POP для удаления почты из почтового ящика POP. После этого Сэм читает сообщение в почтовом клиенте Netscape.

Понятия, связанные с данным

“Планирование работы с электронной почтой” на стр. 10
Прежде чем приступить к настройке электронной почты, вы должны определиться с планом использования электронной почты в своей системе.

Ссылки, связанные с данной

“Простой протокол передачи почты (SMTP)” на стр. 46
Простой протокол передачи почты (SMTP) основан на TCP/IP и позволяет отправлять и принимать почтовые сообщения. Обычно он применяется вместе с POP3 или IMAP для сохранения сообщений в почтовом ящике на сервере и периодического запроса почты с сервера пользователем.

“Протокол POP” на стр. 48
Почтовый протокол POP версии 3 описан в RFC 1939 (POP3), RFC 2449 (Механизм расширения POP3) и RFC 2595 (Использование TLS с IMAP, POP3 и ACAP). RFC - это разрабатываемые стандарты Internet.

Сценарий: Настройка API QtmsCreateSendEmail для использования протокола S/MIME

В этом сценарии показано, каким образом можно настроить API QtmsCreateSendEmail для использования secure/MIME (S/MIME).

Описание задачи

Пользователю Джону Смиту, ИД которого jsmith, нужно настроить API QtmsCreateSendEmail для использования secure/MIME (S/MIME). S/MIME представляет собой более безопасный метод отправки почты программными средствами, по сравнению с API QtmmSendMail.

Дополнительные сведения

Для отправки подписанных и зашифрованных сообщений Джону необходимо установить в своей системе i5/OS V6R1 следующие компоненты:

- i5/OS PASE (5761-SS1 компонент 33)
- Диспетчер цифровых сертификатов (5761-SS1 компонент 34)
- OpenSSL (5733-SC1 компонент 1)

Создание хранилища пользовательских сертификатов

Для применения S/MIME требуется хранилище пользовательских сертификатов. В данной операционной системе пользовательским сертификатам присваиваются имена типа *ИДпользователя*.usrcrt. Сертификаты располагаются в каталоге /qibm/userdata/icss/cert/download/client.

Джон должен создать хранилище сертификатов пользователей для своего пользовательского профайла, под которым запускается задание создания и отправки почтовых сообщений. Управлять хранилищем пользовательских сертификатов можно с помощью Диспетчера цифровых сертификатов (DCM).

Для создания хранилища пользовательских сертификатов выполните следующие действия:

1. Создайте подкаталог, используя имя профайла пользователя:

   ```
   cd  /qibm/userdata/icss/cert/download/client
   mkdir  jsmith
   ```

2. Откройте в Web-браузере страницу задач System i, введя следующий URL: http://*имя_вашей_системы*:2001.
3. Для перехода к пользовательскому интерфейсу DCM выберите **Диспетчер цифровых сертификатов** из списка продуктов на странице задач System i. На левой панели выберите **Создать новое хранилище сертификатов**.
4. На странице Создания нового хранилища сертификатов выберите **Хранилище сертификатов другой системы** и нажмите **Продолжить**.
5. На странице Создать сертификат в новом хранилище сертификатов выберите **Нет - Не создавать сертификат в хранилище сертификатов**.
6. На странице Имя хранилища сертификатов и пароль задайте путь к хранилищу сертификатов и пароль. Путь к хранилищу сертификатов должен включать в себя ваш ИД пользователя. Например, Джон задал путь /qibm/userdata/icss/cert/download/client/jsmith/jsmith.kdb.

Экспорт пользовательского сертификата отправителя в System i

Джон пользуется Web-браузером Internet Explorer (IE) 6. Пользовательский сертификат отправителя получен от Сертификатной компании (CA) и установлен в IE 6.

Для экспорта пользовательского сертификата отправителя на платформу System i Джону необходимо выполнить следующие действия:

1. В окне IE выбрать меню **Сервис → Опции Internet**.
2. Во вкладке **Содержание** нажать кнопку **Сертификаты**.
3. Во вкладке **Личные** выбрать сертификат отправителя и нажать кнопку **Экспорт**.
4. В окне приветствия мастера экспорта сертификатов нажать **Далее**.
5. На странице Экспортировать личный ключ экспорта выбрать **Да, экспортировать личный ключ** и нажать **Далее**.
6. На странице Экспортировать формат файла выбрать **Включить надежную защиту (требуется IE 5.0, NT 4.0 SP4 или выше)** в меню **Обмен личной информацией - PKCS #12 (.PFX)**.
7. На странице Пароль ввести пароль сертификата.
8. На странице Файл для экспорта указать имя файла, который необходимо экспортировать, например: C:\temp\jsmithcert.pfx и нажать **Next**.
9. В окне завершения работы мастера экспорта сертификатов нажать **Готово**.
10. С помощью FTP отправить пользовательский сертификат отправителя jsmithcert.pfx в режиме ASCII, на платформу System i. В данном примере предполагается, что файл будет отправлен в каталог /home/jsmith интегрированной файловой системы ОС System i. Подробные сведения об импорте сертификата содержатся в разделе “Импорт сертификата отправителя в System i” на стр. 9.

Экспорт пользовательских сертификатов получателя в System i

Для экспорта пользовательского сертификата получателя на платформу System i Джону необходимо выполнить следующие действия:

1. В окне IE выбрать меню **Сервис → Опции Internet**.
2. Щелкнуть на вкладке **Содержание** в окне Опции Internet, а затем нажать кнопку **Сертификаты**.
3. Во вкладке **Личные** окна Опции Internet выбрать сертификат, а затем нажать **Экспорт**.

   Для экспорта нескольких сертификатов необходимо повторить действия от 3 до 7 для каждого сертификата.
4. В окне приветствия мастера экспорта сертификатов нажать **Далее**.
5. На странице Экспортировать формат файла выберите **DER кодированный двоичный X.509 (.CER)**.
6. На странице Файл для экспорта указать имя файла, который необходимо экспортировать, например: C:\temp\receiveruser.cer и нажать **Next**.
7. В окне завершения работы мастера экспорта сертификатов нажать **Готово**.
8. С помощью FTP отправить пользовательский сертификат получателя receiver.cet в режиме ASCII, на платформу System i. В данном примере предполагается, что файл будет отправлен в каталог /home/jsmith интегрированной файловой системы ОС System i. Подробные сведения об импорте сертификата получателя содержатся в разделе “Импорт сертификата получателя в System i”.
9. Повторить все предыдущие действия для каждого получателя, который используется в S/MIME.

Импорт сертификата отправителя в System i

После этого Джон должен импортировать свой пользовательский сертификат и личный ключ в хранилище пользовательских сертификатов с помощью DCM. Пароль для импортированного сертификата должен совпадать с паролем хранилища ключей. Кроме того, необходимо импортировать все сертификаты пользователей, которым Джон будет отправлять электронные сообщения.

1. Откройте в Web-браузере страницу задач System i, введя следующий URL: http://*имя_вашей_системы*: 2001.
2. Для перехода к пользовательскому интерфейсу DCM выберите **Диспетчер цифровых сертификатов** из списка продуктов на странице задач System i.
3. На странице Выбор хранилища сертификатов выберите **Хранилище сертификатов другой системы** и нажмите **Продолжить**.
4. На странице Имя хранилища сертификатов и пароль задайте путь к хранилищу сертификатов, имя файла и пароль. Нажмите кнопку **Продолжить**. Имя файла Джона - /qibm/userdata/icss/cert/download/client/jsmith/ jsmith.kdb.
5. Разверните меню **Управление сертификатами → Импортировать сертификат**. Выберите **Сервер или клиент**, чтобы импортировать сертификат отправителя. Нажмите **Продолжить**.
6. На странице Импортировать сертификат сервера или клиента введите каталог интегрированной файловой системы и имя файла сертификата отправителя и нажмите **Продолжить**. В “Экспорт пользовательского сертификата отправителя в System i” на стр. 8 каталогом интегрированной файловой системы и файлом является /home/jsmith/ jsmithcert.pfx.
7. Укажите метку сертификата, то есть, адрес электронной почты отправителя, используя символы нижнего регистра. Нажмите **Продолжить**.
8. Нажмите **OK**.

Импорт сертификата получателя в System i

Для импорта сертификата получателя на платформу System i выполните следующие действия:

1. Откройте в Web-браузере страницу задач System i, введя следующий URL: http://*имя_вашей_системы*: 2001.

2. Для перехода к пользовательскому интерфейсу DCM выберите **Диспетчер цифровых сертификатов** из списка продуктов на странице задач System i.
3. На странице Выбор хранилища сертификатов выберите **Хранилище сертификатов другой системы** и нажмите **Продолжить**.
4. На странице Имя хранилища сертификатов и пароль задайте путь к хранилищу сертификатов, имя файла и пароль. Нажмите кнопку **Продолжить**. Имя файла Джона - /qibm/userdata/icss/cert/download/client/jsmith/jsmith.kdb.
5. Разверните меню **Управление сертификатами → Импортировать сертификат**. Выберите **Сертификатная компания**, чтобы импортировать сертификат получателя. Нажмите **Продолжить**.
6. На странице Импортировать сертификат сертификатной компании (CA) укажите каталог интегрированной файловой системы и имя файла сертификата получателя и нажмите **Продолжить**. В “Экспорт пользовательских сертификатов получателя в System i” на стр. 9 каталогом интегрированной файловой системы и файлом получателя является /home/jsmith/receiveruser.cer.
7. Укажите метку сертификата CA, то есть, адрес электронной почты получателя, используя символы нижнего регистра. Нажмите **Продолжить**.
8. Повторить все предыдущие действия для каждого сертификата получателя, который будет использоваться отправителем.

Понятия, связанные с данным

Диспетчер цифровых сертификатов

Ссылки, связанные с данной

API Создать и отправить электронное сообщение MIME (QtmsCreateSendEmail)

Планирование работы с электронной почтой

Прежде чем приступить к настройке электронной почты, вы должны определиться с планом использования электронной почты в своей системе.

Прежде чем начать настройку электронной почты, ответьте на следующие вопросы:

1. Что будет представлять собой адресная книга?
2. Какой IP-адрес у вашего сервера DNS?
3. Применяется ли брандмауэр? Если да, то какой у него IP-адрес?
4. Применяется ли почтовый сервер Proxy, почтовый маршрутизатор или функция передачи почты? Если да, то какой у него IP-адрес?
5. Будет ли применяться база данных Domino?
6. Будет ли применяться сервер POP i5/OS для получения почты?

За информацией о принципах работы электронной почты обратитесь к разделу, в котором приведен пример сценария электронной почты.

Если будут применяться серверы Domino и i5/OS SMTP, обратитесь к разделу Размещение серверов Domino и SMTP в одной системе. Дополнительная информация о сервере Domino приведена в разделе Domino и на Web-сайте Lotus Domino for i5/OS.

Если вы не собираетесь применять серверы SMTP и POP, отключите их, чтобы они не могли быть использованы без вашего ведома.

Понятия, связанные с данным

“Сценарий: Отправка и получение почтовых сообщений в локальной системе” на стр. 5
В этом сценарии показана передача электронной почты между локальными пользователями.

Domino

Задачи, связанные с данной

“Настройка электронной почты” на стр. 14
Для того чтобы настроить электронную почту на своей системе, нужно настроить TCP/IP и сервера SMTP и POP и запустить почтовые сервера.

“Размещение серверов Domino и SMTP в одной системе” на стр. 38
Если серверы Domino SMTP работают в одной системе, рекомендуется связать их с разными IP-адресами.

Информация, связанная с данной

Lotus Domino для i5/OS

Управление доступом к электронной почте

Для того чтобы защитить свои данные от разрушительных воздействий, необходимо контролировать, кто имеет доступ к системе через электронную почту.

В этом разделе приведены советы по защите почтовых серверов от лавинных атак и рассылок нежелательных рекламных сообщений (″спама″).

Понятия, связанные с данным

Примеры независимых пулов дисков

“Определение неполадок электронной почты” на стр. 48
Здесь описаны действия, которые помогут в анализе неполадок электронной почты.

Задачи, связанные с данной

“Ограничение пересылки сообщений” на стр. 27
Для того, чтобы ваш почтовый сервер не использовался для рассылки нежелательной почты (спама) или для отправки больших объемов электронной почты, можно воспользоваться функцией ограничения пересылки и указать, кто именно может использовать вашу систему для пересылки сообщений. Тем не менее, при ограничении пересылки сообщений, вы не сможете защитить свою электронную почту путем идентификации.

“Ограничение соединений” на стр. 29
В целях обеспечения защиты системы, вы можете запретить подключение пользователей, которые излишне загружают сервер.

Информация, связанная с данной

Защита AS/400 для Internet: Защита AS/400 от HARM в сети Internet

Управление доступом к SMTP

Для защиты системы от атак рассыльщиков нежелательной почты (спама) следует должным образом настроить доступ к серверу SMTP.

Если вы хотите разрешить клиентам SMTP доступ к системе, то необходимо защитить ее от атак одним из следующих способов:

- По возможности избегайте использования записей *ANY *ANY в системном каталоге рассылки. Отсутствие записи *ANY *ANY затрудняет применение протокола SMTP для атаки системы или сети лавинной рассылкой. Переполнение происходит, когда вспомогательная память заполняется ненужной почтой, перенаправляемой через вашу систему на другую систему.
- Задайте надлежащие ограничения для пулов вспомогательной памяти (ASP), чтобы лишить пользователей возможности переполнить систему ненужными объектами. Просмотреть и настроить пороги для ASP можно с помощью либо системного инструментария (SST), либо специальных сервисных средств (DST).
- С помощью команды Изменить запись предварительного задания (CHGPJE) настройте максимальное число создаваемых предварительных заданий. Это позволит ограничить число заданий, создаваемых во время атаки типа ″отказ в обслуживании″. По умолчанию максимальное пороговое значение равно 256.
- Запретите несанкционированный доступ к серверу рассыльщиков нежелательной почты, ограничив возможности пересылки и подключения к серверу.

- В системах, на которых установлена операционная система i5/OS V6R1, рассылку нежелательной почты (спама) можно запретить, требуя идентификации при отправке электронных сообщений. Если идентификации требует удаленный сервер, вы можете установить функцию идентификации на своем локальном сервере.

Ссылки, связанные с данной

Команды Изменить атрибуты SMTP (CHGSMTPA)

Управление доступом POP

Для защиты системы необходимо управлять доступом к ней по протоколу POP.

Вы можете указать, используется ли сервером POP шифрование для защиты потоков данных POP, включая ИД пользователей и пароли. Шифрование обеспечивается протоколами SSL и TLS. Для того, чтобы указать на наличие поддержки защищенных сеансов POP, задайте параметр ALWSSL в команде CL Изменить атрибуты сервера POP (CHGPOPA).

Если вы разрешите клиентам обращаться к системе по протоколу POP, обратите внимание на следующее:

- Почтовый сервер POP выполняет идентификацию клиентов, обращающихся к своим почтовых ящикам. Клиент отправляет на сервер свой ИД пользователя и пароль.

  Почтовый сервер POP сравнивает указанные ИД пользователя и пароль с профайлом и паролем i5/OS этого пользователя. Так как у вас нет возможности управлять способом хранения ИД пользователя и пароля в клиенте POP, рекомендуется создать специальный пользовательский профайл с минимальными правами доступа в системе. Для того чтобы исключить возможность создания интерактивного сеанса с помощью этого пользовательского профайла, задайте в пользовательском профайле следующие значения:
  Укажите в параметре Начальное меню (INLMNU) значение *SIGNOFF
  Укажите в параметре Первоначальная программа (INLPGM) значение *NONE
  Укажите в параметре Ограничение возможностей (LMTCPB) значение *YES
- Задайте надлежащие ограничения для пулов вспомогательной памяти (ASP), чтобы лишить пользователей возможности переполнить систему ненужными объектами. Если задан порог памяти ASP, то система не прервет работу из-за нехватки памяти. Просмотреть и настроить пороги для ASP можно с помощью либо системного инструментария (SST), либо специальных сервисных средств (DST).
- Порог ASP должен обеспечивать, с одной стороны, защиту системы от лавинной рассылки, с другой - нормальную работу системы, в частности, хранение и доставку почты. Если почтовому серверу не удается доставить почту из-за недостаточного объема выделенной для этого памяти в системе, то это причинит неудобства пользователям. При интенсивном использовании памяти работа почтового сервера будет остановлена.

  Как правило, серьезных проблем из-за нехватки памяти не возникает. Как только клиент получает почту, почтовый сервер удаляет ее из памяти системы.

Понятия, связанные с данным

“Определение неполадок электронной почты” на стр. 48
Здесь описаны действия, которые помогут в анализе неполадок электронной почты.

Запрет доступа к электронной почте

В зависимости от того, как используется система, может понадобиться запретить пользователям доступ к электронной почте через серверы SMTP и POP. Доступ к электронной почте можно запретить полностью или частично.

Запрет доступа к SMTP

Для того, чтобы запретить в своей системе получение и рассылку почты с помощью SMTP, необходимо запретить запуск сервера SMTP.

Сервер SMTP по умолчанию запускается вместе с TCP/IP. Если протокол SMTP не будет применяться, не настраивайте его в своей системе (и запретите другим пользователям настраивать его).

Отключение автоматического запуска SMTP при запуске TCP/IP:

В некоторых случаях, если SMTP время от времени используется, вам может потребоваться ограничить права доступа пользователей к серверу SMTP.

Для отключения автоматического запуска задания сервера SMTP при запуске TCP/IP выполните следующие действия:

1. В System i Navigator разверните меню ***система*** → **Сеть** → **Серверы** → **TCP/IP**.
2. Щелкните правой кнопкой на **SMTP** и выберите **Свойства**.
3. Отмените выбор пункта **Запускать вместе с TCP/IP**.

Запрет доступа к портам SMTP:

Для того чтобы защитить сервер SMTP, можно ограничить доступ к портам SMTP.

Для того, чтобы отключить запуск SMTP и запретить связывание пользовательских приложений, например, приложения API сокетов, с портом SMTP системы, выполните следующие действия:

1. В System i Navigator разверните меню ***система*** → **Сеть** → **Серверы** → **TCP/IP**.
2. Щелкните правой кнопкой на значке **Конфигурация TCP/IP** и выберите **Свойства**.
3. В окне Свойства конфигурации TCP/IP выберите страницу **Запреты на порты**.
4. На странице Запреты на порты нажмите кнопку **Добавить**.
5. На странице Добавить запрет на порт введите следующие данные:
   - **Имя пользователя**: Введите имя защищенного пользовательского профайла в вашей системе. (Защищенный пользовательский профайл - это профайл, у которого нет программ с принятыми правами доступа и пароль которого неизвестен другим пользователям.) Резервирование порта для конкретного пользователя не позволяет всем остальным пользователям применять этот порт.
   - **Начальный порт**: `25`
   - **Конечный порт**: `25`
   - **Протокол**: `TCP`
6. Нажмите кнопку **OK** для добавления запрета.
7. На странице **Запреты на порты** нажмите кнопку **Добавить** и повторите операцию для протокола UDP.
8. Нажмите кнопку **OK**, чтобы сохранить запреты на порты и закрыть окно **Свойства конфигурации TCP/IP**. Запреты на порты вступают в силу при следующем запуске TCP/IP. Если протокол TCP/IP работал во время настройки запретов на порты, то его необходимо перезапустить.

Блокировка очередей SNADS:

Очереди рассылки SNADS, которые приложение SMTP использует для распределения электронной почты, можно заблокировать. Это обеспечивает дополнительную защиту, ограничивая распределение электронной почты.

Для того чтобы заблокировать очереди рассылки, введите в командной строке:

```
HLDDSTQ  DSTQ(QSMTPQ)PTY(*NORMAL)
HLDDSTQ  DSTQ(QSMTPQ)PTY(*HIGH)
```

Понятия, связанные с данным

“Основы электронной почты” на стр. 2
Электронная почта - важный деловой инструмент. Операционная система i5/OS поддерживает протоколы SMTP и POP, позволяющие быстро обмениваться электронной почтой.

Запрет доступа к POP

Если вы не хотите, чтобы кто-либо мог получить доступ к вашей системе с помощью протокола POP, необходимо запретить запуск сервера POP.

Если сервер POP не будет применяться, не настраивайте его в своей системе (и запретите другим пользователям настраивать его).

Отключение автоматического запуска POP при запуске TCP/IP:

В некоторых случаях, если POP время от времени используется, вам может потребоваться ограничить права доступа пользователей к серверу POP.

Сервер POP по умолчанию запускается вместе с TCP/IP. Для отключения автоматического запуска задания сервера POP при запуске TCP/IP выполните следующие действия:

1. В System i Navigator разверните меню ***система*** **→ Сеть → Серверы → TCP/IP**.
2. Щелкните правой кнопкой на значке **POP** и выберите **Свойства**.
3. Отмените выбор пункта **Запускать вместе с TCP/IP**.

Запрещение доступа к портам POP:

Для того чтобы защитить сервер POP, можно ограничить доступ к портам POP.

Для того, чтобы отключить запуск сервера POP и запретить связывание пользовательских приложений, например, приложения API сокетов, с портом POP системы, выполните следующие действия:

1. В System i Navigator подключитесь к своей системе и разверните меню **Сеть → Серверы → TCP/IP**.
2. Щелкните правой кнопкой на значке **Конфигурация TCP/IP** и выберите **Свойства**.
3. В окне Свойства конфигурации TCP/IP выберите страницу **Запреты на порты**.
4. На странице Запреты на порты нажмите кнопку **Добавить**.
5. На странице Добавить запрет на порт введите следующие данные:
   - **Имя пользователя**: Введите имя защищенного пользовательского профайла в вашей системе. (Защищенный пользовательский профайл - это профайл, у которого нет программ с принятыми правами доступа и пароль которого неизвестен другим пользователям.) Резервирование порта для конкретного пользователя не позволяет всем остальным пользователям применять этот порт.
   - **Начальный порт**: `110 995`
   - **Конечный порт**: `110 995`
   - **Протокол**: `TCP`
6. Нажмите кнопку **OK** для добавления запрета.
7. На странице Запреты на порты нажмите кнопку **Добавить** и повторите операцию для протокола UDP.
8. Нажмите кнопку **OK**, чтобы сохранить запреты на порты и закрыть окно Свойства конфигурации TCP/IP.

Запреты на порты вступают в силу при следующем запуске TCP/IP. Если протокол TCP/IP работал во время настройки запретов на порты, то его необходимо перезапустить.

Настройка электронной почты

Для того чтобы настроить электронную почту на своей системе, нужно настроить TCP/IP и сервера SMTP и POP и запустить почтовые сервера.

Понятия, связанные с данным

“Простой протокол передачи почты (SMTP) в i5/OS” на стр. 3
Простой протокол передачи почты (SMTP) обеспечивает возможность отправки и приема почтовых сообщений операционной системой.

“Планирование работы с электронной почтой” на стр. 10
Прежде чем приступить к настройке электронной почты, вы должны определиться с планом использования электронной почты в своей системе.

Доступ к серверам электронной почты с помощью System i Navigator

С помощью System i Navigator можно настроить работу с почтовыми серверами SMTP и POP.

Для того чтобы начать работу с POP или SMTP в System i Navigator, выполните следующие действия:

1. Дважды щелкните на папке **Client Access Express**.
2. Дважды щелкните на **System i Navigator**. Если вы работаете с System i Navigator впервые, щелкните на значке **Создать соединение**, чтобы настроить соединение со своей системой.
3. В System i Navigator разверните меню ***система*** **→ Сеть → Серверы → TCP/IP**.
4. Дважды щелкните на значке **SMTP** или **POP** - будет показано окно диалога Свойства SMTP или Свойства POP.

Понятия, связанные с данным

“Почтовый протокол POP в i5/OS” на стр. 4
Сервер Почтового протокола (POP) - это реализация интерфейса протокола POP версии 3 на сервере i5/OS.

Настройка TCP/IP для работы с электронной почтой

Прежде чем настраивать электронную почту в системе, нужно настроить TCP/IP.

Приведенные ниже инструкции помогут вам выполнить первоначальную настройку электронной почты в системе. Если TCP/IP уже настроены в вашей системе, можно переходить непосредственно к настройке серверов SMTP (Простого протокола передачи почты) и POP (Почтового протокола).

1. В System i Navigator разверните меню ***система*** **→ Сеть → Настройка TCP/IP**.
2. Щелкните правой кнопкой мыши на пункте **TCP/IP** и выберите опцию **Создать интерфейс** для требуемого типа сети. Для создания нового интерфейса TCP/IP следуйте инструкциям мастера. Мастер запросит у вас следующую информацию:
   - Тип соединения
   - Аппаратный ресурс
   - Описание линии
   - IP-адрес
   - Имя хоста
   - Имя домена

     Имя хоста и имя домена составляют полное имя вашего хоста. Полное имя хоста используется SMTP для связи с другими хостами.

     Например, если ASHOST - имя локального хоста, а DOMAIN.COMPANY.COM - имя локального домена, то полное имя хоста - ASHOST.DOMAIN.COMPANY.COM.
   - Запускаемые серверы
3. После того как Мастер настроит соединение, щелкните правой кнопкой мыши на **TCP/IP** и выберите опцию **Свойства**.Появится окно диалога Свойства TCP/IP.
4. Щелкните на вкладке **Таблица хостов**.
5. Нажмите **Добавить**.Будет показано окно Запись таблицы хостов TCP/IP.
6. Введите IP-адрес и имя хоста, которые вы указали при работе с Мастером создания интерфейса TCP/IP.
7. Нажмите **OK** в окне Запись таблицы хостов TCP/IP.
8. Нажмите **OK** в окне Свойства TCP/IP.

Понятия, связанные с данным

"Определение неполадок электронной почты" на стр. 48
Здесь описаны действия, которые помогут в анализе неполадок электронной почты.

Задачи, связанные с данной

"Настройка серверов SMTP и POP для электронной почты"
Работа электронной почты в системе обеспечивается двумя протоколами: SMTP (Простой протокол передачи почты) и POP (Почтовый протокол).

Настройка серверов SMTP и POP для электронной почты

Работа электронной почты в системе обеспечивается двумя протоколами: SMTP (Простой протокол передачи почты) и POP (Почтовый протокол).

Примечание: Для работы почты должны быть настроены оба этих протокола.

Понятия, связанные с данным

"Почтовый протокол POP в i5/OS" на стр. 4
Сервер Почтового протокола (POP) - это реализация интерфейса протокола POP версии 3 на сервере i5/OS.

Задачи, связанные с данной

"Настройка TCP/IP для работы с электронной почтой" на стр. 15
Прежде чем настраивать электронную почту в системе, нужно настроить TCP/IP.

Настройка сервера SMTP

После настройки TCP/IP система автоматически настраивает SMTP. Тем не менее, вам придется изменить некоторые свойства SMTP, чтобы сервер SMTP мог работать с электронной почтой.

Для изменения свойств SMTP выполните следующие действия:

1. В System i Navigator разверните меню ***система*** → **Сеть** → **Серверы** → **TCP/IP**.
2. Дважды щелкните на **SMTP**.
3. Щелкая на вкладках, перечисленных в следующей таблице, задайте указанные в соответствующем столбце значения полей. Затем выполните следующие действия.

Щелкните на этой вкладке	Затем сделайте следующее
Общие	Выберите **Запускать при запуске TCP/IP**. [1]
Общие	Выберите **Не ограничен** в поле **Размер блоков сообщений**.
Общие	Если вы используете почтовый маршрутизатор, введите его имя, например, mailrouter.company.com. Имя почтового маршрутизатора - это имя системы, на которую сервер SMTP отправляет почту, если она адресована не локальному получателю. Более подробную информацию можно найти в справке System i Navigator.
Общие	Если в системе установлен брандмауэр, выберите опцию **Пересылать исходящую почту маршрутизатору через брандмауэр**.
Общие	Если вы будете обмениваться почтовыми сообщениями с серверами Domino, то отмените выбор переключателя **Считать знак процента символом маршрутизации**.
Общие	Если вам нужно передавать все нелокальные почтовые сообщения на другой сервер SMTP, укажите полное глобальное имя домена системы обмена почтой в поле **Домен почтового сервера пересылки**.
Общие	Если вам нужно, чтобы сервер SMTP поддерживал перевод пустой строки (LF) или перевод строки с возвратом каретки (CRLF) выберите **Разрешить перевод пустой строки**. Если вам нужно, чтобы сервер SMTP поддерживал только CRLF, снимите отметку с поля **Разрешить перевод пустой строки**.
Автоматическая регистрация	Если для отправки и приема почты применяются команды SNDDST и RCVDST, и вместо маршрутизации Internet применяется SNADS, то выберите переключатель **Автоматически добавлять удаленных пользователей в системный каталог**.

Щелкните на этой вкладке	Затем сделайте следующее
Автоматическая регистрация	Если для отправки и приема почты применяются команды SNDDST и RCVDST, соответственно, выберите в поле **Добавить пользователей** опцию **Системная таблица псевдонимов**.
[1] Это изменение вступает в силу при следующем запуске сервера SMTP.	

4. Для подтверждения изменений нажмите **OK**.

Задачи, связанные с данной

“Идентификация электронной почты для локальной работы и пересылки” на стр. 26
Рассылку нежелательной почты (спама) можно запретить на сервере, требуя идентификации при отправке электронных сообщений. Требовать идентификации нельзя, если вы хотите ограничить пересылку сообщений. Рекомендуется настроить идентификацию для своего сервера.

Включение поддержки SSL между сервером SMTP и клиентом в системе получателя:

Для включения SSL между сервером SMTP и клиентом в системе получателя выполните следующие действия. Предполагается, что сертификат сервера уже создан на сервере SMTP.

Для выполнения этой задачи убедитесь в наличии подключения к системе получателя.

Запуск и настройка Диспетчера цифровых сертификатов (DCM)

1. Через Web-браузер подключитесь к серверу SMTP: http://*ваша_система*: 2001/
2. На странице задач i5/OS выберите **Диспетчер цифровых сертификатов**, а затем - **Выбрать хранилище сертификатов**.
3. На странице Выбор хранилища сертификатов выберите ***SYSTEM** и нажмите **Продолжить**.
4. На странице Хранилище сертификатов и пароль введите пароль для хранилища сертификатов.
5. Откройте меню **Управление приложениями → Обновить присвоение сертификата** и выберите **Сервер**.
6. Выберите **Сервер SMTP TCP/IP i5/OS** и нажмите кнопку **Обновить присвоение сертификата**, если это необходимо.

Настройка сервера SMTP

Для включения поддержки SSL, с помощью команды Изменить атрибуты SMTP (CHGSMTPA) установите значение параметра ALWAUTH, равное *LCLRLY либо *RELAY.

- Значение *RELAY означает, что применение SSL поддерживается только электронными сообщениями, отправленными с другого сервера SMTP.
- При установке значения *LCLRLY также включаются параметры Проверка сообщений MSF (VFYMSFMSG) и Проверка от пользователя (VFYFROMUSR). Значение по умолчанию также может привести к запрету на прием некоторых сообщений электронной почты. Решите, нужна ли вам поддержка таких запретов.

Настройка клиента SMTP

Необходимо настроить клиента SMTP System i таким образом, чтобы он мог входить в систему сервера получателя SMTP System i. С помощью команды CL Добавить запись в список SMTP (ADDSMTPLE) добавьте запись в список идентификации хостов:

```
ADDSMTPLE TYPE(*HOSTAUTH) HOSTNAME(вашасистема.realm.com) USERNAME(получатель) PASSWORD(xxxx)
```

Имя хоста, которое сохраняется в символах верхнего регистра, должно совпадать с адресом электронной почты. Если адрес электронной почты имеет вид myemail@yoursystem, необходимо добавить следующую запись:

```
ADDSMTPLE TYPE(*HOSTAUTH) HOSTNAME(YOURSYSTEM) USERNAME(получатель) PASSWORD(xxxx)
```

Включение поддержки SSL между сервером SMTP и клиентом в системе отправителя:

Для выполнения этой задачи необходимо подключение к системе отправителя.

1. Через Web-браузер подключитесь к серверу SMTP: http://*ваша_система*: 2001/
2. На странице задач i5/OS выберите **Диспетчер цифровых сертификатов**, а затем - **Выбрать хранилище сертификатов**.
3. На странице Выбор хранилища сертификатов выберите ***SYSTEM** и нажмите **Продолжить**.
4. На странице Хранилище сертификатов и пароль введите пароль для хранилища сертификатов и нажмите кнопку **Продолжить**. Если у вас нет пользовательского сертификата или если вы собираетесь создать пользовательский сертификат, выполните действия от 5 до 8; иначе, переходите к действию 9.
5. На странице Создание сертификата выберите **Сертификат пользователя** и нажмите **Продолжить**.
6. На странице Создание сертификата пользователя заполните обязательные поля информацией, необходимой для создания сертификата, и нажмите **Продолжить**.
7. В окне Потенциальное нарушение сценария нажмите **Да**.
8. На странице Создать сертификат пользователя нажмите кнопку **OK**. Клиентский сертификат пользователя будет применяться системой.
9. Откройте меню **Управление приложениями → Обновить присвоение сертификата**, выберите **Сертификат сервера или клиента**.
10. На странице Обновить присвоение сертификата выберите **Клиент** и нажмите **Продолжить**.
11. Выберите **Клиент TCP/IP i5/OS** и нажмите кнопку **Обновить присвоение сертификата**.

Установка сертификатной компании получателя в системе отправителя:

Если цифровой сертификат получателя выпущен сертификатной компанией (CA), неизвестной системе отправителя, следует установить цифровой сертификат данной сертификатной компании в системе отправителя.

Экспорт локального сертификата CA и отправка его системе отправителя

Предполагается, что сертификатная компания является локальной; тем не менее, вы можете воспользоваться этой процедурой для экспорта любого сертификата CA, неизвестной системе отправителя.

Для экспорта сертификата локальной CA выполните следующие действия:

1. Нажмите кнопку **Выбрать хранилище приложений** и выберите **Локальная сертификатная компания (CA)**. Нажмите **Продолжить**.
2. На странице Хранилище сертификатов и пароль введите пароль.
3. Откройте меню **Управление локальной CA → Экспорт** и выберите **Файл - Экспортировать в файл**. Нажмите **Продолжить**.
4. На странице Экспорт сертификата введите каталог и имя файла, в котором будет храниться сертификат CA. Если указанный каталог не существует, создайте его с помощью команды mkdir.
5. На странице Сертификат экспортирован успешно нажмите **OK**.
6. С помощью FTP в режиме ASCII отправьте сертификат CA с системы получателя на систему отправителя.

Установка сертификата CA в системе отправителя

1. На странице Выбор хранилища сертификатов выберите ***SYSTEM** и нажмите **Продолжить**.
2. На странице Хранилище сертификатов и пароль введите пароль и нажмите кнопку **Продолжить**.
3. Разверните меню **Управление сертификатами → Импортировать сертификаты**, выберите **Сертификатная компания (CA)** и нажмите **Продолжить**.

4. На странице Импортировать сертификат сертификатной компании (CA) укажите каталог, в котором хранится сертификат CA получателя. Нажмите **Продолжить**.
5. Присвойте сертификату метку и нажмите **Продолжить**. Отображается следующее сообщение: `Сертификат импортирован`
6. Нажмите кнопку **OK**.

Настройка сервера POP

Перед тем как клиенты смогут получать почту по протоколу POP, необходимо настроить сервер POP.

POP-сервер передает почту из почтового ящика пользователя клиенту POP по его запросу. Настройка сервера POP завершает подготовку системы к работе с электронной почтой.

Для настройки сервера POP для работы с такими почтовыми программами, как Netscape Mail и Eudora Pro, выполните следующие действия:

1. В System i Navigator разверните меню ***система*** **→ Сеть → Серверы → TCP/IP**.
2. Дважды щелкните на **POP**.
3. Значения полей приведены в следующей таблице.

Щелкните на этой вкладке	**Затем сделайте следующее**
Общие	Выберите **Запускать при запуске TCP/IP**.
Общие	Для того, чтобы разрешить как сеансы TLS/SSL, так и незащищенные сеансы по протоколу POP, выберите значение **Защищенные и незащищенные** в поле **Запуск поддержки Socket layer при запуске сервера**.
Настройка	Выберите **Не ограничен** в поле **Размер блоков сообщений**.
Настройка	Если клиенты POP подключаются к системе по коммутируемым соединениям и работают с большим объемом почты, то увеличьте значение в поле **Тайм-аут простоя**.
Связи	Выберите опцию **Применять только вместо неподдерживаемых CCSID**.

4. Для подтверждения изменений нажмите **OK**.

Выбор сертификата для сервера POP:

Выполните эту задачу, если вы не назначили сертификат серверу POP при создании локальной сертификатной компании (CA), либо планируете получать сертификаты от глобальной CA.

1. Запустите Диспетчер цифровых сертификатов IBM. Если вам необходимо получить или создать сертификаты, либо выполнить еще какие-либо действия по настройке системы сертификатов, то это следует сделать сейчас. Сведения о настройке системы осблуживания сертификатов содержатся в разделе Настройка DCM.
2. Нажмите **Выбрать хранилище сертификатов**.
3. Выберите ***SYSTEM**.Нажмите **Продолжить**.
4. Введите пароль для доступа к хранилищу сертификатов *SYSTEM. Нажмите **Продолжить**.
5. После обновления содержимого левого меню навигации разверните **Управление приложениями**.
6. Выберите **Назначить сертификат**.
7. Выберите **Приложение сервера**.Нажмите **Продолжить**.
8. Выберите **Сервер POP TCP/IP i5/OS**.
9. Нажмите кнопку **Назначить сертификат**, чтобы назначить сертификат данному серверу POP.
10. Выберите в списке сертификат, который нужно назначить серверу.

11. Нажмите **Назначить новый сертификат**.
12. После выбора всех сертификатов для сервера POP нажмите кнопку **Готово**.

Регистрация пользователей электронной почты

Для регистрации пользователей электронной почты необходимо создать пользовательские профайлы.

Пользовательские профайлы системы iSeries предназначены для идентификации отправителей и получателей электронной почты. Для любого пользователя, которого вы хотите включить в вашу систему электронной почты, должен существовать свой профайл.

При создании пользовательского профайла пользователь автоматически регистрируется в системном каталоге рассылки. На основе системного каталога рассылки SMTP определяет, куда доставлять локальную электронную почту.

Для создания пользовательского профайла для пользователей SNADS и POP выполните следующие действия:

1. В System i Navigator разверните меню ***система*** → **Пользователи и группы**.
2. Щелкните правой кнопкой мыши на опции **Все пользователи** и выберите **Создать пользователя**.
3. Введите имя и пароль пользователя.

   Примечание: Этот пароль применяется пользователями POP для защиты своих почтовых ящиков POP.
4. Нажмите кнопку **Характеристики**.
5. Щелкните на вкладке **Права доступа**.Убедитесь, что задан класс прав доступа **Пользователь**.
6. Нажмите **OK**.
7. Нажмите кнопку **Личные**.
8. Откройте вкладку **Почта**.
9. Выберите опцию **Уровень почтового обслуживания**.
   - Если вы регистрируете пользователя SNADS, выберите **Индекс пользователя**.
   - Если вы регистрируете пользователя POP3, выберите **Почтовый ящик системы**.
10. Выберите **Тип предпочитаемого адреса**.
    - Если вы регистрируете пользователя SNADS, выберите **ИД и адрес пользователя**.
    - Если вы регистрируете пользователя POP3, выберите **Имя SMTP**.
11. Убедитесь, что в поле Домен правильно указано имя домена сервера SMTP. Как правило, по умолчанию указано верное имя, однако при наличии нескольких локальных доменов может потребоваться изменить его.
12. Нажмите **OK**.Регистрация пользователя SNADS завершена. Если вы регистрируете пользователя POP, который будет работать с сервером i5/OS POP исключительно для получения электронной почты, то перейдите к следующему шагу.
13. Нажмите кнопку **Задания**.
14. Откройте вкладку **Запуск сеанса**.
15. В поле **Начальное меню** укажите **Выход из системы**.В этом случае пользователь сможет входить в систему только для чтения своей почты или для того, чтобы изменить пароль. Попытка выполнить какую-либо другую операцию приведет к автоматическому выходу пользователя из системы.
16. Нажмите **OK**.
17. Нажмите **OK**.
18. Повторите эту процедуру для всех пользователей, для которых вы хотите создать профайлы.

Понятия, связанные с данным

“Отправка и получение электронной почты” на стр. 30
Ваша система может работать как почтовый сервер, на котором зарегистрированы пользователи

электронной почты (SNADS, POP или Lotus).Пользователи могут отправлять, получать и читать свою почту с помощью программ-клиентов POP или SNADS.

Задачи, связанные с данной

“Отправка электронной почты с помощью служб рассылки Системной сетевой архитектуры (SNADS)” на стр. 33
Почту можно отправлять с помощью клиента SNADS. Отправитель сообщения должен быть локальным пользователем SNADS.

Запуск и остановка серверов электронной почты

Запустите необходимые серверы. Это позволит гарантировать, что все серверы работают правильно и что внесенные в их конфигурацию изменения вступили в силу. В некоторых случаях возникает необходимость перезапуска серверов. Для этого необходимо остановить их, а затем снова запустить.

Задачи, связанные с данной

“Проверка серверов электронной почты” на стр. 36
Наиболее часто проблемы с почтой возникают из-за того, что не запущены нужные серверы. Проверьте состояние почтовых серверов и убедитесь, что все они запушены, прежде чем начать их использовать.

Запуск почтовых серверов

После запуска серверов ваша система начинает работу в качестве почтового сервера с зарегистрированными на нем пользователями.

Для запуска серверов выполните следующие действия:

1. В System i Navigator разверните меню ***система*** **→ Сеть**.
2. Щелкните правой кнопкой на значке **Конфигурация TCP/IP** и выберите **Свойства**.Будет показано окно диалога Свойства конфигурации TCP/IP.
   - Если TCP/IP находится в состоянии Запущено, нажмите **OK** и перейдите к следующему шагу.
   - В противном случае, нажмите **Отмена** и закройте окно Свойства конфигурации TCP/IP; затем щелкните правой кнопкой мыши на значке **Конфигурация TCP/IP** и выберите **Запустить**. После этого нажмите **OK**.
3. Разверните **Серверы → TCP/IP**. Если серверы SMTP и POP не запущены, запустите их:
   a. Щелкните правой кнопкой на **SMTP** и выберите **Запустить**.
   b. Щелкните правой кнопкой на **POP** и выберите **Запустить**.
4. В командной строке введите STRMSF для запуска Среды почтового сервера.
5. Если применяется SNADS, введите STRSBS QSNADS для запуска подсистемы QSNADS.

Теперь серверы запущены, и ваша система работает как почтовый сервер, на котором зарегистрированы пользователи электронной почты.

Остановка почтовых серверов

С помощью System i Navigator можно завершать работу почтовых серверов.

Для завершения работы серверов выполните следующие действия:

1. В System i Navigator разверните меню ***система*** **→ Сеть → Серверы → TCP/IP**.Если серверы SMTP и POP запущены, остановите их:
   a. Щелкните правой кнопкой мыши на **SMTP** и выберите **Остановить**.
   b. Щелкните правой кнопкой мыши на **POP** и выберите **Остановить**.
2. В командной строке введите ENDMSF для завершения работы Среды почтового сервера.
3. Если применяется SNADS, введите ENDSBS QSNADS для завершения работы подсистемы QSNADS.

Настройка профайла коммутируемого соединения электронной почты

Если вы не применяете службу AT&T Global Network, необходимо сначала настроить профайла почтового соединения.

Для того чтобы настроить профайл коммутируемого соединения вручную, выполните следующие действия:

Примечание: Если вы пользуетесь поддержкой AT&T Global Network, перейдите к разделу Настройка мастера коммутируемого подключения к ISP.

1. В System i Navigator разверните меню ***система*** → **Сеть** → **Службы удаленного доступа**.
2. Щелкните правой кнопкой на значке **Профайлы соединений получателей** и выберите **Создать профайл**.
3. Выберите **PPP** в поле **Протокол**.
4. Выберите **Коммутируемая линия** в поле **Тип соединения**.
5. Разверните **Конфигурация TCP/IP** и выберите **Соединения**.
6. Разверните **Серверы** → **TCP/IP**.
7. Щелкните правой кнопкой на **SMTP** и выберите **Свойства**.
8. Перейдите на страницу **Планировщик**.Выберите переключатель **Запускать планировщик вместе с SMTP** и укажите созданный профайл соединения.
9. Перейдите на страницу ETRN и отметьте переключатель **Поддержка ETRN (Получение почты с помощью телефонного соединения)**. Нажмите **Добавить** и укажите имя домена сервера исходящей почты ISP.
10. Включите поддержку брандмауэра и укажите в качестве брандмауэра почтовый сервер ISP, применяемый для отправки почты.
11. Перейдите к настройке нового коммутируемого соединения ISP с помощью мастера.

Задачи, связанные с данной

“Настройка коммутируемого соединения с ISP с помощью мастера”
Перед использованием функции планировщика SMTP для отправки большого объема почты через провайдера Internet (ISP) необходимо настроить профайл коммутируемого соединения.

Настройка коммутируемого соединения с ISP с помощью мастера

Перед использованием функции планировщика SMTP для отправки большого объема почты через провайдера Internet (ISP) необходимо настроить профайл коммутируемого соединения.

Для выполнения этой задачи можно воспользоваться Мастером настройки коммутируемого соединения с ISP.

Предварительные требования:

Если вы не применяете службу AT&T Global Network, необходимо сначала выполнить инструкции из раздела Настройка профайла почтового коммутируемого соединения. Мастер создания соединения задает IP-адреса почтовых серверов (SMTP и POP), имена хостов этих серверов, а также имя и пароль соответствующих учетных записей.

Для запуска мастера и настройки планировщика SMTP выполните следующие действия:

1. В System i Navigator разверните меню ***система*** → **Сеть** → **Службы удаленного доступа**.
2. Щелкните правой кнопкой на значке **Профайлы соединений отправителей** и выберите **Создать коммутируемое соединение с AT&T Global Network**.
3. Для того чтобы начать работу, на панели Приветствие нажмите кнопку **Далее**.
4. На панели **Тип приложения** выберите **Приложение для работы с почтой** и нажмите **Далее**.

5. Для настройки нового коммутируемого соединения с AT&T Global Network продолжите работу с Мастером.

После настройки коммутируемого соединения вы можете приступить к планированию пакетных заданий электронной почты ISP.

Задачи, связанные с данной

"Настройка профайла коммутируемого соединения электронной почты" на стр. 22
Если вы не применяете службу AT&T Global Network, необходимо сначала настроить профайла почтового соединения.

"Планирование пакетных заданий электронной почты ISP"
Для того чтобы сократить продолжительность установления соединения, для заданий электронной почты можно запланировать периодическое коммутируемое подключение к ISP.С помощью планировщика SMTP можно задать периодичность, с которой система будет подключаться к ISP и отправлять почту.

Планирование пакетных заданий электронной почты ISP

Для того чтобы сократить продолжительность установления соединения, для заданий электронной почты можно запланировать периодическое коммутируемое подключение к ISP.С помощью планировщика SMTP можно задать периодичность, с которой система будет подключаться к ISP и отправлять почту.

Предварительные требования:

Настройте соединение с помощью Мастера настройки ISP.

Для настройки планировщика SMTP на отправку электронной почты ISP выполните следующие действия:

1. В System i Navigator разверните меню ***система*** → **Сеть** → **Серверы** → **TCP/IP**.
2. Дважды щелкните на **SMTP**.
3. Перейдите на страницу **Планировщик**.
4. Отметьте переключатель **Запускать планировщик вместе с SMTP**.
5. Выберите **Профайл двухточечного соединения**, созданный с помощью Мастера создания соединения с AT&T Global Network или вручную.
6. Задайте периодичность, с которой SMTP будет отправлять находящиеся в очереди почтовые сообщения, установив **Интервал передачи почты** (в минутах).
7. При работе с поставщиком Internet, отличным от AT&T Global Network, включите переключатель **Передавать команду ETRN при подключении к удаленному серверу**.
8. Введите IP-адрес сервера входящей почты, а также Зарегистрированный хост и домен ISP, для которого сервер SMTP будет передавать команду ETRN.
9. Нажмите **OK**.

Задачи, связанные с данной

"Настройка коммутируемого соединения с ISP с помощью мастера" на стр. 22
Перед использованием функции планировщика SMTP для отправки большого объема почты через провайдера Internet (ISP) необходимо настроить профайл коммутируемого соединения.

"Настройка сервера SMTP для получения почты по коммутируемому соединению"
Сервер SMTP позволяет работать с почтой удаленным филиалам компании, использующим коммутируемое соединение.

Настройка сервера SMTP для получения почты по коммутируемому соединению

Сервер SMTP позволяет работать с почтой удаленным филиалам компании, использующим коммутируемое соединение.

Системе должен быть выделен статический IP-адрес. Она также должна быть зарегистрирована в DNS. С каждым хостом и доменом, для которого сервер будет собирать почту, должна быть связана запись типа MX, указывающая на данную систему. Кроме того, в локальной таблице хостов системы должны быть заданы псевдонимы для всех этих хостов. Если удаленные серверы работают в операционной системе i5/OS, то в них должна быть настроена поддержка Запланированных пакетных заданий электронной почты ISP.

Для обслуживания запросов на получение и отправку электронной почты от удаленных систем выполните следующие действия:

1. В System i Navigator разверните меню ***система*** → **Сеть** → **Серверы** → **TCP/IP**.
2. Дважды щелкните на **SMTP**.
3. Перейдите на страницу **ETRN**.
4. Включите переключатель **Поддержка ETRN (Получение почты по коммутируемому соединению)**.
5. Нажмите **Добавить** для указания хоста и домена ISP.Повторите эту операцию для всех хостов.
6. Нажмите **OK**.

Задачи, связанные с данной

“Планирование пакетных заданий электронной почты ISP” на стр. 23
Для того чтобы сократить продолжительность установления соединения, для заданий электронной почты можно запланировать периодическое коммутируемое подключение к ISP.С помощью планировщика SMTP можно задать периодичность, с которой система будет подключаться к ISP и отправлять почту.

Поддержка нескольких доменов

Сервер SMTP можно настроить на поддержку нескольких доменов для функций провайдера Internet (ISP).

Для выполнения сервером SMTP функций ISP этот сервер должен работать в нескольких доменах. В конфигурации клиента SMTP должно быть указано, к какому интерфейсу подключаться, какую почту пересылать, а какую считать локальной или передавать брандмауэру.

1. В System i Navigator разверните меню ***система*** → **TCP/IP** → **Сеть**.
2. Щелкните правой кнопкой на **SMTP** и выберите **Свойства**.
3. Перейдите на страницу **Несколько доменов**.
4. Нажмите **Добавить** и укажите поддерживаемые домены и интерфейсы.
5. Нажмите **OK**.

Понятия, связанные с данным

“Предварительные требования для маршрутизации почты” на стр. 25
Описаны предварительные этапы настройки шлюза почты.

Защита электронной почты

Для защиты электронной почты можно воспользоваться брандмауэрами, функциями ограничения пересылки и соединений, а также фильтрами, предотвращающими проникновение вирусов.

Создание защищенной среды на сервере SMTP является очень важным аспектом. Сервер SMTP и его пользователи должны быть защищены как от внутренних, так и от внешних помех.

Понятия, связанные с данным

| “Основы электронной почты” на стр. 2
| Электронная почта - важный деловой инструмент. Операционная система i5/OS поддерживает протоколы
| SMTP и POP, позволяющие быстро обмениваться электронной почтой.

Ссылки, связанные с данной

| API Создать и отправить электронное сообщение MIME (QtmsCreateSendEmail)

Информация, связанная с данной

Отправка электронной почты через маршрутизатор или брандмауэр

Почтовый маршрутизатор - это промежуточная система, в которую SMTP доставляет почту, если не может определить, где находится точный IP-адрес получателя.

Почтовый маршрутизатор отправляет почту на IP-адрес или на другой маршрутизатор. Если локальный сервер не может доставить почтовое сообщение в указанную систему, то вы можете направить его в альтернативную целевую систему. Если у вас есть брандмауэр, его можно использовать в качестве маршрутизатора.

Перед настройкой маршрутизатора ознакомьтесь с разделом “Предварительные требования для маршрутизации почты”.

Для настройки маршрутизатора выполните следующие действия:

1. В System i Navigator разверните меню ***система*** → **Сеть** → **Серверы** → **TCP/IP**.
2. Дважды щелкните на **SMTP**.
3. Перейдите на страницу **Общие**.
4. Введите имя Почтового маршрутизатора.

Для маршрутизации почты через брандмауэр выполните следующие действия:

1. В System i Navigator разверните меню ***система*** → **Сеть** → **Серверы** → **TCP/IP**.
2. Дважды щелкните на **SMTP**.
3. Перейдите на страницу **Общие**.
4. В поле **Почтовый маршрутизатор** введите имя брандмауэра, например, `FWAS400.company.com`.
5. Выберите **Пересылать отправляемые сообщения маршрутизатору через брандмауэр**.

Предварительные требования для маршрутизации почты

Описаны предварительные этапы настройки шлюза почты.

Перед тем как настраивать почтовый маршрутизатор, ознакомьтесь с приведенной ниже информацией:

- Операционной системой промежуточного сервера не обязательно должна быть i5/OS. Все, что требуется почтовому маршрутизатору, - это таблица хостов с адресами всех систем, в которые ему необходимо направлять почтовые сообщения. Если функции почтового маршрутизатора выполняет операционная система система i5/OS, то никаких требований к версии применяемого программного обеспечения не предъявляется.
- Для пересылки почты из исходной системы в целевую можно задавать только один промежуточный маршрутизатор. Применение каскадных почтовых маршрутизаторов недопустимо.
- При запуске SMTP должен получать IP-адрес почтового маршрутизатора из локальной таблицы хостов или от сервера имен доменов (DNS). Если SMTP не сможет получить IP-адрес почтового маршрутизатора, то маршрутизатор использоваться не будет.
- Информация о почтовом маршрутизаторе используется брандмауэром для пересылки почты SMTP хостам, находящимся за пределами локального (защищенного) домена. Необходимо разрешить почтовому маршрутизатору пересылку почты через брандмауэр. При включении брандмауэра почта для получателей, расположенных вне домена операционной системыi5/OS, также будет проходить через маршрутизатор. i5/OS версии V5R1 и более поздней поддерживает несколько локальных доменов. Можно настроить отдельные локальные домены, не отправляющие почту через брандмауэр.

Задачи, связанные с данной

“Поддержка нескольких доменов” на стр. 24
Сервер SMTP можно настроить на поддержку нескольких доменов для функций провайдера Internet (ISP).

Идентификация электронной почты для локальной работы и пересылки

Рассылку нежелательной почты (спама) можно запретить на сервере, требуя идентификации при отправке электронных сообщений. Требовать идентификации нельзя, если вы хотите ограничить пересылку сообщений. Рекомендуется настроить идентификацию для своего сервера.

Для включения идентификации сервера выполните следующие действия:

1. В System i Navigator разверните меню ***система*** **→ Сеть → Серверы → TCP/IP**.
2. Дважды щелкните на **SMTP**.
3. Щелкните на вкладке **Идентификация** и задайте указанные в соответствующем столбце значения полей. Затем выполните следующие действия.

Щелкните на этой вкладке	Затем сделайте следующее
Идентификация	Выберите значение **Требовать TLS/SSL и идентифицировать ее локально и при пересылке** , если вы хотите, чтобы сервер применял TLS/SSL для локальной идентификации и при пересылке сообщений.
Идентификация	Выберите значение **Требовать TLS/SSL и идентифицировать только при пересылке** , если вы хотите, чтобы сервер применял TLS/SSL только для идентификации при пересылке сообщений.
Идентификация	Если вы хотите, чтобы правом входа в систему сервера SMTP обладали только пользователи, включенные в разрешенный список, выберите значение **Проверять ИД при локальной доставке**.
Идентификация	Можно настроить модульные функции среды почтового сервера SMTP на отказ от приема непроверенных электронных сообщений. Для этого выберите значение **Проверять отправителя сообщения**.
Идентификация	Для того, чтобы сервер SMTP проверял, включен ли отправитель в Системный каталог рассылки и совпадает ли адрес электронной почты с адресом, указанным в этом каталоге, выберите значение **Пользователи** или **Пользователи, не включенные в разрешенный список** Пользователи, адреса электронной почты которых не совпадают с указанными в каталоге, будут запрещены.

4. Для сохранения изменений нажмите кнопку **OK**.

Задачи, связанные с данной

“Ограничение пересылки сообщений” на стр. 27
Для того, чтобы ваш почтовый сервер не использовался для рассылки нежелательной почты (спама) или для отправки больших объемов электронной почты, можно воспользоваться функцией ограничения пересылки и указать, кто именно может использовать вашу систему для пересылки сообщений. Тем не менее, при ограничении пересылки сообщений, вы не сможете защитить свою электронную почту путем идентификации.

“Настройка сервера SMTP” на стр. 16
После настройки TCP/IP система автоматически настраивает SMTP. Тем не менее, вам придется изменить некоторые свойства SMTP, чтобы сервер SMTP мог работать с электронной почтой.

Мониторинг отправителя электронной почты

Теперь можно настроить сервер SMTP на запрет приема электронной почты от не идентифицированного отправителя. Кроме того, можно настроить модульные функции среды почтового сервера SMTP на отказ от приема непроверенных электронных сообщений.

Для того, чтобы запретить прием непроверенных сообщений или сообщений от непроверенных отправителей, необходимо включить шифрование транзакции, то есть, протоколы TLS/SSL.

Отказ от приема почты от непроверенного отправителя

Для того, чтобы запретить прием почты от непроверенных отправителей, выполните следующие действия:

1. В Навигаторе System i разверните меню ***система*** **→ Сеть → Серверы → TCP/IP**.
2. Щелкните правой кнопкой на **SMTP** и выберите **Свойства**.
3. Откройте вкладку **Идентификация**.
4. Если необходимо проверять всех отправителей электронной почты, в поле **Проверять почту от пользователя** выберите **Все**. Если нужно проверять только пользователей, не включенных в разрешенный список, выберите опцию проверки **Пользователей, не включенных в список разрешенных**.
5. Нажмите **OK**.

Сервер SMTP проверяет, включен ли отправитель в Системный каталог рассылки и совпадает ли адрес электронной почты с адресом, указанным в этом каталоге. В случае несовпадения, вступает в силу запрет.

Отказ от приема непроверенной почты

Для того, чтобы запретить прием непроверенной почты, выполните следующие действия:

1. В Навигаторе System i разверните меню ***система*** **→ Сеть → Серверы → TCP/IP**.
2. Щелкните правой кнопкой на **SMTP** и выберите **Свойства**.
3. Откройте вкладку **Идентификация**.
4. Выберите значение **Требовать TLS/SSL и идентифицировать ее локально и при пересылке** для поля **Разрешить идентификацию**.
5. Выберите **Проверять отправителя сообщения MSF**.
6. Нажмите **OK**.

Если электронное сообщение поступает не из идентифицированного источника, то пользователь, который вызвал команду API QzmfCrtMailMsg(), должен быть создателем сообщения MSF. Иначе модульные функции SMTP запретят прием таких сообщений.

Ограничение пересылки сообщений

Для того, чтобы ваш почтовый сервер не использовался для рассылки нежелательной почты (спама) или для отправки больших объемов электронной почты, можно воспользоваться функцией ограничения пересылки и указать, кто именно может использовать вашу систему для пересылки сообщений. Тем не менее, при ограничении пересылки сообщений, вы не сможете защитить свою электронную почту путем идентификации.

Существует шесть вариантов управления пересылкой:

- Разрешена пересылка всех сообщений
- Не разрешена пересылка никаких сообщений
- Разрешена пересылка только для получателей, указанных в списке доменов
- Разрешена пересылка только сообщений от указанных адресов
- Разрешена пересылка только сообщений от указанных доменов и адресов
- Разрешена пересылка только сообщений от клиентов POP в течение указанного периода

Теперь ограничить пересылку можно только путем выбора опции **Нет TLS/SSL, идентификация не выполняется**. В System i Navigator эта опция находится на странице Идентификация, где вы указываете свойства SMTP.

Для указания пользователей, которым разрешена отправка почты, выполните следующие действия:

1. В System i Navigator разверните меню ***система*** **→ Сеть → Серверы → TCP/IP**.
2. Щелкните правой кнопкой на **SMTP** и выберите **Свойства**.
3. Перейдите на страницу **Ограничения на пересылку сообщений**.
4. Выберите нужный вариант управления пересылкой из перечисленных выше.

Примечание: При выборе опции **Принимать сообщения только для получателей из соседних доменов** или **Принимать сообщения только из соседних доменов и с адресов, указанных в списке** необходимо на странице **Общие** указать список соседних доменов, которым разрешена пересылка почты.

5. Нажмите **OK**.

Понятия, связанные с данным

“Управление доступом к электронной почте” на стр. 11
Для того чтобы защитить свои данные от разрушительных воздействий, необходимо контролировать, кто имеет доступ к системе через электронную почту.

Задачи, связанные с данной

“Идентификация электронной почты для локальной работы и пересылки” на стр. 26
Рассылку нежелательной почты (спама) можно запретить на сервере, требуя идентификации при отправке электронных сообщений. Требовать идентификации нельзя, если вы хотите ограничить пересылку сообщений. Рекомендуется настроить идентификацию для своего сервера.

Ссылки, связанные с данной

| Команды Изменить атрибуты SMTP (CHGSMTPA)

Разрешение пересылки сообщений от клиентов Почтового протокола POP

Один из вариантов ограничения пересылки разрешает клиентам POP пересылать сообщения посредством SMTP в течение определенного периода после подключения этих клиентов к серверу POP.

Обычно эту функцию называют ″POP перед SMTP″. Она особенно полезна для мобильных сотрудников, пользующихся динамическими IP-адресами, поскольку функции защиты, применяющие фиксированные IP-адреса, не эффективны при проверке динамических IP-адресов. В этом случае мобильный сотрудник после однократной идентификации на сервере POP сможет отправлять электронную почту в течение определенного времени (15-65535 минут) без повторной идентификации.

Например, систему можно настроить таким образом, что удаленным пользователям будет разрешено пересылать сообщения через сервер SMTP в течение четырех часов (240 минут) после их подключения к серверу POP. В данном примере мобильный сотрудник подключается к серверу POP для просмотра своей электронной почты. Сервер POP заносит IP-адрес пользователя и системное время в очередь. Час спустя пользователь решает отправить электронное сообщение. Когда он отправляет это сообщение с помощью сервера SMTP, тот просматривает очередь, чтобы убедиться, что пользователь подключился к серверу POP в течение отведенного периода. После проверки пользователя сервер SMTP пересылает сообщение клиенту SMTP для доставки получателю.

Примечание: Для того чтобы еще лучше контролировать доступ пользователей к почтовому серверу, вы можете применять функцию ограничения пересылки и функцию ограничения соединений одновременно. Например, вы можете запретить определенным группам пользователей подключаться к почтовому серверу, но разрешить некоторым клиентам POP из этой группы применять сервер SMTP для отправки электронных сообщений.

Для того чтобы разрешить клиентам POP пересылать сообщения в течение определенного времени, выполните следующие действия:

1. В System i Navigator разверните меню ***система*** **→ Сеть → Серверы → TCP/IP**.
2. Щелкните правой кнопкой на **SMTP** и выберите **Свойства**.
3. Перейдите на страницу **Ограничения на пересылку сообщений**.
4. В поле **Разрешить пересылку сообщений** выберите **Указанный**.
5. Выберите **От клиента POP в течение следующего периода (15 - 65535)** и введите время в минутах, в течение которого клиенту будет разрешено отправлять почту с помощью сервера SMTP.
6. Нажмите **OK**.

Одновременное применение функций ограничения пересылки и ограничения соединений

Операционная система i5/OS позволяет одновременно применять функцию ограничения пересылки и функцию ограничения соединений для более точного контролирования доступа к почтовому серверу.

Вы можете запретить подключение к почтовому серверу определенным группам пользователей, но разрешить некоторым клиентам POP из этой группы отправлять сообщения с помощью сервера SMTP.

Пусть, например, вам известно, что пользователи с IP-адресами из некоторого диапазона регулярно рассылают спам. По этой причине, вы хотите запретить подключение к почтовому серверу с адресов из этого диапазона. Однако некоторые IP-адреса из этого диапазона выделены надежным пользователям i5/OS, и вы хотите разрешить таким пользователям, имеющим пользовательские профайлы i5/OS, пересылать сообщения в течение заданного периода после их подключения к серверу POP.

К счастью, вы можете воспользоваться функцией ограничения соединений, чтобы запретить подключение с IP-адресов из определенного диапазона, и функцией ограничения пересылки, чтобы разрешить некоторым надежным пользователям (клиентам POP) с адресами из этого диапазона отправлять почту с помощью сервера SMTP. Операционная система i5/OS сначала проверит, настроили ли вы в системе разрешение клиентам POP пересылать сообщения в течение заданного периода. Затем она выяснит, какие соединения запрещены. Эта возможность, предоставляемая i5/OS, позволяет вам в точности определить круг пользователей, которым будет разрешено пересылать сообщения с помощью сервера SMTP и которым будет разрешено подключаться к почтовому серверу.

| В случае одновременного применения функций ограничения пересылки и ограничения соединений
| необходимо задать параметр OVRRJTNNL(*YES) (Переопределять список запретов на соединения) в
| команде CL Изменить атрибуты SMTP (CHGSMTPA). Этот параметр означает, что функция идентификации
| сервера POP будет переопределять конфигурацию ограничения соединений. Впоследствии вам может
| потребоваться удалить ограничение пересылки, позволяющее клиентам POP из запрещенной группы
| пользоваться вашим почтовым сервером. В этом случае в команде CHGSMTPA необходимо задать
| параметр OVRRJTNNL(*NO).

Задачи, связанные с данной

“Ограничение соединений”
В целях обеспечения защиты системы, вы можете запретить подключение пользователей, которые излишне загружают сервер.

Ссылки, связанные с данной

| Команда Изменить атрибуты SMTP (CHGSMTPA)

Ограничение соединений

В целях обеспечения защиты системы, вы можете запретить подключение пользователей, которые излишне загружают сервер.

Например, некоторые пользователи используют систему для массовой рассылки рекламных сообщений. Такие почтовые сообщения (″спам″), которые никому не нужны, занимают значительную долю процессорного времени и большой объем памяти. Кроме того, если ваша система разрешает передавать рекламные сообщения, то другие системы могут заблокировать почту, которая приходит с вашей системы.

Вы можете указать IP-адреса известных нежелательных пользователей, а также загрузить с одного из серверов Список блокированных адресов (RBL). Этот список содержит IP-адреса хостов, занимающихся массовой рассылкой.

Для добавления фиксированных IP-адресов или имен хостов, предоставляющих динамические списки блокированных адресов, выполните следующие действия:

1. В System i Navigator разверните меню ***система*** **→ Сеть → Серверы → TCP/IP**.
2. Щелкните правой кнопкой на **SMTP** и выберите **Свойства**.

3. Откройте страницу Ограничения на соединения.
4. Нажмите кнопку **Добавить** для добавления имен серверов списка блокированных адресов.
5. Нажмите кнопку **Добавить** для добавления фиксированных адресов хостов, которым запрещено подключение.
6. Нажмите **OK**.

Понятия, связанные с данным

“Управление доступом к электронной почте” на стр. 11
Для того чтобы защитить свои данные от разрушительных воздействий, необходимо контролировать, кто имеет доступ к системе через электронную почту.

Задачи, связанные с данной

“Одновременное применение функций ограничения пересылки и ограничения соединений” на стр. 29
Операционная система i5/OS позволяет одновременно применять функцию ограничения пересылки и функцию ограничения соединений для более точного контролирования доступа к почтовому серверу.

Фильтрация почты для защиты от вирусов

Для предотвращения распространения вируса, который может проникнуть на серверы электронной почты, можно создать фильтры, реагирующие на определенные темы, типы, имена файлов и адреса отправителей сообщения. Соответствующая почта может отправляться на карантин или удаляться.

Если включена фильтрация вирусов, то сомнительные почтовые сообщения автоматически изолируются либо удаляются, в зависимости от параметров, указанных системным администратором. Ниже перечислены возможные критерии фильтрации электронной почты:

1. **Адрес** - домена или личный
2. **Тема** - ILOVEYOU
3. **Имя вложения** - lovebug.vbs или *.vbs
4. **Тип MIME** - image/* или image/jpg

Значения могут содержать символы подстановки. Один из символов подстановки - звездочка (*), что соответствует произвольным символам. Например, для проверки имен файлов с расширением .vbs можно указать критерий *.vbs. Адрес отправителя *@us.ibm.com означает, что будет отфильтрована вся почта, приходящая из подразделений IBM, расположенных в США, а фильтр image/* отфильтрует почту с изображениями любых типов.

Для создания фильтра выполните следующие действия:

1. В System i Navigator разверните меню ***система*** **→ Сеть → Серверы → TCP/IP**.
2. Щелкните правой кнопкой на **SMTP** и выберите **Свойства**.
3. Откройте страницу Фильтры.
4. Выберите **Сохранить сообщение** или **Удалить сообщение**. Опция **Сохранить сообщения** приводит к сохранению копии сообщения; при этом само сообщение не будет доставлено получателю.
5. Нажмите **Добавить** для указания критерия идентификации опасных сообщений.Сообщения, удовлетворяющие введенному критерию, не будут доставлены получателям.
6. Для сохранения изменений нажмите кнопку **OK**.

Помимо данных фильтров, необходимо также использовать дополнительные средства защиты от вирусов.

Отправка и получение электронной почты

Ваша система может работать как почтовый сервер, на котором зарегистрированы пользователи электронной почты (SNADS, POP или Lotus).Пользователи могут отправлять, получать и читать свою почту с помощью программ-клиентов POP или SNADS.

С помощью API отправки почты MIME (QtmmSendMail) API или API создания и отправки почты MIME (QtmsCreateSendEmail) пользователи могут отправлять почтовые сообщения из программ i5/OS. Работая с API QtmsCreateSendEmail, пользователи могут подписывать и зашифровывать документ MIME с помощью протокола secure/MIME, представляющего собой защищенную версию протокола MIME. API QtmsCreateSendEmail является предпочтительным методом отправки почтовых сообщений программными средствами.

Кроме того, пользователи могут получать и отправлять электронную почту следующими способами.

Понятия, связанные с данным

"Основы электронной почты" на стр. 2
Электронная почта - важный деловой инструмент. Операционная система i5/OS поддерживает протоколы SMTP и POP, позволяющие быстро обмениваться электронной почтой.

Задачи, связанные с данной

"Регистрация пользователей электронной почты" на стр. 20
Для регистрации пользователей электронной почты необходимо создать пользовательские профайлы.

Ссылки, связанные с данной

API Создать и отправить электронное сообщение MIME (QtmsCreateSendEmail)

API Отправить электронное сообщение MIME (QtmmSendMail)

Настройка почтовых клиентов POP

Для получения сообщений с сервера POP сначала требуется настроить почтовый клиент.

В вашей системе для хранения и пересылки электронной почты применяется сервер POP. С сервером POP взаимодействует почтовый клиент, который получает и хранит почту для пользователей. Протокол POP поддерживается различными клиентами, включая такие как Eudora, Outlook Express и Lotus Notes. Для настройки каждой из этих программ-клиентов существует своя процедура. Однако информация, которую вы должны при этом вводить, одинакова для всех программ. В качестве примера рассмотрим процедуру настройки Outlook Express:

1. Соберите информацию для почтового клиента POP.
   - ИД пользователя и полное имя хоста (имя хоста плюс имя домена). Это электронный адрес пользователя, по которому он будет получать почту. Обычно адрес выглядит следующим образом: ИД_пользователя@имя_хоста.имя_домена.

     Примечание: При настройке некоторых клиентов вам придется ввести адрес хоста несколько раз: при определении хоста сервера POP (для приема почты), хоста SMTP (для отправки почты), а также для того, чтобы идентифицировать отправителя почты для получателей.
   - Имя пользователя POP или учетное (регистрационное) имя. Это имя пользовательского профайла i5/OS.
   - Пароль пользователя. Этот пароль должен совпадать с паролем пользовательского профайла i5/OS.
2. Введите регистрационные данные пользователя и параметры. Например, в Outlook Express выберите **Сервис → Учетные записи**, а затем щелкните на вкладке **Почта** для идентификации информации о пользователе и пользовательских параметрах.
   - Имя пользователя. Это имя пользовательского профайла i5/OS.
   - Электронный адрес пользователя. Это ИД пользователя и полное имя хоста.
   - Обратный адрес. Он может совпадать с электронный адрес пользователя, сообщенный ему администратором сети, но пользовательский профайл i5/OS должен существовать в системе.
3. Укажите сервер отправляемой почты (SMTP). Сервер SMTP необходимо задать в почтовом клиенте, поскольку именно с его помощью пользователи программы-клиента будут отправлять почту. Например, в Outlook Express выберите **Сервис → Учетные записи**, выберите соответствующую учетную запись электронной почты и нажмите кнопку **Свойства**. Откройте вкладку **Серверы** и укажите сервер SMTP.

- Имя пользователя POP или учетное (регистрационное) имя. Это ИД пользователя в электронном адресе или имя пользовательского профайла i5/OS.
- Сервер отправляемой почты (SMTP). Это имя хоста системы.

4. Укажите сервер принимаемой почты (POP). Например, в Outlook Express выберите **Сервис → Учетные записи**, выберите соответствующую учетную запись электронной почты и нажмите кнопку **Свойства**. Откройте вкладку **Серверы** и укажите сервер POP.
   - Сервер принимаемой почты. Это имя хоста системы.
5. Настройте клиентскую программу для работы с TLS/SSL. В Outlook Express, к примеру, для настройки выполните следующие действия:
   a. Выберите **Сервис → Учетные записи** и выберите учетную запись электронной почты.
   b. Выберите **Свойства**, а затем щелкните на вкладке **Серверы**.
   c. Выберите **Серверу требуется идентификация** и нажмите кнопку **Параметры**.
   d. Выберите **Аналогично серверу для входящей почты** и нажмите **OK**.
   e. Откройте вкладку **Дополнительно** и выберите **Требуется защищенное подключение (SSL)** для почтовых серверов входящей (POP) и исходящей (SMTP) почты. Нажмите кнопку **OK**.
   f. Нажмите **Применить**, а затем **OK**, чтобы закрыть окно Свойства.

JavaMail

С помощью JavaMail можно разрабатывать клиентских приложений электронной почты.

API JavaMail обеспечивает независимую от операционной системы и протокола среду для создания почтовых клиентских приложений на базе Java. API JavaMail позволяет создать почтовый клиент, поддерживающий отправку почтовых сообщений мультимедиа, а также реализацию Протокола доступа к сообщениям Internet (IMAP) с поддержкой папок, идентификации и обработки вложений.

SMTP поддерживает только символьные данные. Для представления сложных данных, таких как форматированный текст, вложенные файлы (текстовые или двоичные) и мультимедиа, используется MIME. При использовании API Отправка сообщений MIME (QTMMSENDMAIL), преобразование данных в нужный формат должно выполняться соответствующим приложением. В JavaMail преобразование MIME происходит автоматически.

Компоненты JavaMail входят в состав IBM Developer Kit for Java.

Понятия, связанные с данным

JavaMail

Отправка буферных файлов в формате PDF

Буферные файлы можно отправить в формате документов Adobe Portable (PDF) и выполнить их рассылку по электронной почте.

С помощью лицензионной программы IBM Infoprint Server for iSeries (5722-IP1) можно создавать файлы в формате Adobe PDF из любых данных вывода i5/OS. Эти файлы PDF можно отправлять по электронной почте как вложения. Каждый буферный файл можно отправить по своему адресу. Кроме того, буферный файл можно разбить на несколько файлов PDF и отправить эти файлы по разным адресам. Например, вы можете вывести счета-фактуры для покупателей и заказчиков в отдельные файлы PDF и отправить каждому покупателю соответствующий счет по электронной почте. Этот метод является обязательным при пользовании лицензионной программойIBM Infoprint Server for iSeries.

Информация, связанная с данной

PDF Руководство пользователя по InfoPrint Server

IBM eServer iSeries Printing Redbooks VI -- Результаты электронного бизнеса

Адресная книга на сервере LDAP

Простой протокол доступа к каталогам (LDAP) позволяет создать общую адресную книгу на базе системного каталога рассылки.

Для замены функций MAPI можно работать с сервером каталогов IBM Tivoli для i5/OS (который является реализацией LDAP, разработанной IBM). С помощью LDAP создается единая адресная книга, доступная для всех пользователей приложения клиента.

Для настройки адресной книги на сервере LDAP выполните следующие задачи:

1. Запустите сервер каталогов.
2. Опубликуйте информацию на сервере каталогов.
3. Настройте поддержку LDAP на почтовом клиенте. Действия, необходимые для выполнения этой задачи, зависят от применяемого почтового клиента (например, Netscape или Eudora). В параметрах почтового клиента укажите сервер LDAP в качестве Сервера каталогов для адресации почты.

Задачи, связанные с данной

Сервер каталогов - Введение

Публикация информации на сервере LDAP

Ссылки, связанные с данной

Сервер каталогов IBM Tivoli для i5/OS (LDAP)

Отправка электронной почты с помощью служб рассылки Системной сетевой архитектуры (SNADS)

Почту можно отправлять с помощью клиента SNADS. Отправитель сообщения должен быть локальным пользователем SNADS.

Предварительные требования

Необходим профайл локального пользователя SNADS, то есть, пользователь должен быть зарегистрирован в каталоге рассылки локальной системы. Инструкции по регистрации локальных пользователей электронной почты SNADS приведены в разделе Регистрация пользователей электронной почты.

Для отправки почты выполните следующие действия:

1. В командной строке i5/OS введите команду SNDDST (Отправить рассылку) и нажмите Enter.
2. Для просмотра полного списка параметров нажмите клавишу F10.
3. В первом поле, *Отправляемая информация*, введите *LMSG и нажмите клавишу Enter.
4. Введите ИД получателя и имя или IP-адрес сервера.
5. В поле *Описание* введите описание сообщения.
6. Нажмите клавишу Page Down, а в поле *Длинное сообщение* введите текст вашего сообщения.
7. Для отправки сообщения нажмите Enter.

Примечание: Команда SNDDST позволяет также задавать адреса отправки в формате IP-адреса.

Задачи, связанные с данной

“Регистрация пользователей электронной почты” на стр. 20
Для регистрации пользователей электронной почты необходимо создать пользовательские профайлы.

“Получение электронной почты с помощью служб рассылки Системной сетевой архитектуры (SNADS)” на стр. 36
Почту можно получать с помощью клиента SNADS. Получатель сообщения должен быть локальным пользователем SNADS.

Изменение заголовков для разделения получателей

Команда Изменить атрибуты рассылки (CHGDSTA) изменяет содержимое атрибутов службы сообщений (X.400) для почтовых рассылок.

Параметр Сохранить получателя (KEEPRCP) указывает, какая информация о получателе должна сохраняться и передаваться в каждой рассылке. Значение этого параметра влияет на способ создания заголовков MIME для сообщений SNDDST.

Для включения в заголовки MIME тегов CC и BCC необходимо указать в параметре KEEPRCP значение *ALL. Получатели BCC не будут показаны независимо от значения данного параметра. Получатели TO и CC будут показаны в тексте сообщения SNDDST.

Типы содержимого MIME

Документы Internet состоят из заголовка и тела сообщения. Документы MIME, кроме того, могут состоять из нескольких частей, что позволяет включать в текст объекты мультимедиа.

Если в общем заголовке указан тип содержимого `Multipart/Mixed`, за ним следуют один или несколько вложенных объектов.Для каждого вложенного объекта обозначена граница начала и конца. Идентификатор границы указан в параметре *boundary*=, следующем за заголовком Content-Type. Пример сообщения MIME с вложенными объектами приведен на Рисунке 1. Для каждого вложенного объекта указывается собственный тип содержимого и (необязательно) набор символов.

```
     From
@SYSNAM6.CITY.COMPANY.COM:popct08@SYSNAM6.city.company.com Wed
Jan 10
11:33:18 1996 Return-Path:
<@SYSNAM6.CITY.COMPANY.COM:popct08@SYSNAM6.city.company.com> Received: from
SYSNAM6.city.company.com by
fakeps2.city.company.com (COMPANY
          OS/2 SENDMAIL VERSION 1.3.2)/1.0) id AA0329; Wed, 10
Jan 96 11:33:18 -0500 Date: Wed, 10
Jan 96
11:33:18 -0500 Message-Id: <9601101633.AA0329@fakeps2.city.company.com> Received:
  from endmail9 by SYSNAM6.CITY.COMPANY. (IBM i5/OS SMTP V03R02M00) with TCP;
Wed, 10
Jan 1996 10:23:42
+0000. X-Sender: popct08@SYSNAM6.city.ibm.com (Unverified) X-Mailer: Windows
Eudora Pro
Version 2.1.2
Mime-Version:1.0Content-Type:multipart/mixed;boundary="====================_821301929==
 _"
To: fake@fakeps2.city.company.com From:
endmail9 <popct08@SYSNAM6.city.company.com> Subject:
eudora attachments
X-Attachments:C:\EUDORA\ARGYLE.BMP;--====================_821301929==_
Content-Type: text/plain; charset=

 "us-ascii" Пример использования Eudora для отправки текста
и изображения.--====================_821301929==_
Content-Type: application/octet-stream; name="ARGYLE.BMP";
x-mac-type="424D5070"; x-mac-creator="4A565752"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=


"ARGYLE.BMP"
Qk12AgAAAAAAAHYAAAAoAAAAIAAAACAAAAABAAQAAAAAAAACAAAAAAAAAAAAAAAAAAAQAAAAAAAA
AAAAgAAAgAAAAICAAIAAAACAAIAAgIAAAICAgADAwMAAAAD/AAD/AAAA//8A/wAAAP8A/wD//wAA
////AE1EREREREZEREREREE1E1EREREERsZEREREETURE1EREREGxsZEREREERNRERE1ERE
REbGxsZERERE1ERERE1ERERsbGxsZERETURERERE1ERGxsbGxsZERNRERERERE1EbGxsbGxsZE1E
RERERERE1sbGxsbGxsbURERERERERG1sbGxsbGxtZEREREREREbG1sbGxsbG1sZEREREREREbG1s
bGxsbWxsZERERERGxsbG1sbGxtbGxsZERERERbGxsbG1sbGxsZERERERbGxsbG1sbWxsbGxsZE
RGxsbGxsbG1tbGxsbGxsZEbGxsbGxsbG1sbGxsbGxsZEbGxsbGxsbW1sbGxsbGxkREbGxsbGxtbG
1sbGxsbGRERERbGxsbG1sbG1sbGxsZERERERbGxsbGxkRERERERbGxtbGxsbG1sbGRERERE
REbG1sbGxsbG1sZEREREREREbWxsbGxsbG1kRERERERERNbGxsbGxsbG1EREREREREE1EbGxsbGxs
ZE1EREREREETUREbGxsbGxkRE1EREREERNRERERERbGxsbGRERERE1ERERE1ERERERbGxsZERERE1ERETURE
RERERbGxkRERERE1ERNRERERERERbGRERERERE1E1EREREREREZEREREREREE3URERERERERERERERERERE--====================_821301929==_--
```

Рисунок 2. Пример сообщения MIME с вложенными объектами

Поддержка IP-адресов в команде SNDDST

Почту в Internet можно отправлять с помощью команды SNDDST, указывая в ней IP-адрес получателя (в поле *Получатель почты Internet*).

Если в вашей сети для отправки и получения электронной почты применяются Службы рассылок SNA (SNADS) и офисные приложения, настройте в почтовой системе поддержку IP-адресов для команды Отправить рассылку (SNDDST).

Для настройки системы доставки почты выполните следующие действия:

1. В командной строке i5/OS введите: `ADDDIRE USRID(INTERNET GATEWAY) USRD('Allow SNDDST to send INTERNET Mail') SYSNAME(INTERNET) MSFSRVLVL(*USRIDX) PREFADR(NETUSRID *IBM ATCONTXT)`
2. Введите `CHGDSTA SMTPRTE(INTERNET GATEWAY)` и нажмите клавишу Enter.

Теперь пользователи SNADS могут отправлять почту в Internet с помощью команды SNDDST, указывая в ней IP-адрес получателя (в поле*Получатель почты Internet*).

Информация, связанная с данной

Справочник по функциям электронной почты AS/400

Вложение файлов

При отправке электронной почты с помощью команды SNDDST может потребоваться отправить вместе с сообщением какой-либо файл или документ.

Для отправки электронной почты с прикрепленным файлом можно использовать команду Отправить рассылку (SNDDST). SNDDST позволяет отправлять в одном сообщении только один документ или файл. Для отправки нескольких вложений воспользуйтесь API Отправка почты MIME (QtmmSendMail).

Для того чтобы отправить *документ* по электронной почте как вложение, введите следующую команду:

```
SNDDST TYPE(*DOC) DSTD(описание) TOUSRID(пользователь) DOC(документ) FLR(папка)
```

Для того чтобы отправить *файл* по электронной почте как вложение, введите следующую команду:

```
SNDDST TYPE(*FILE) DSTD(описание) TOUSRID(пользователь)
MSG(сообщение) DOCFILE(библиотека/файл) DOCMBR(элемент)
```

Если появится сообщение об ошибке, это может означать, что вы попытались отправить файл или документ, формат которого несовместим с командой Отправить рассылку (SNDDST). В этом случае с помощью команд CL CPY i5/OS преобразуйте файл в документ или файл, совместимый с командой SNDDST.

Преобразование типов файлов для отправки с помощью команды SNDDST

Для отправки буферного файла по электронной почте его необходимо преобразовать в соответствующий формат. Предположим, что буферный файл, физический файл и папка уже существуют.

1. Переместить буферный файл в файл базы данных:
   ```
   CPYSPLF   FILE(splfile)  TOFILE(dbfile)  JOB(job3/job2/job1) SPLNBR(splnbr) TOMBR(mbr)
   ```
2. Переместить файл базы данных в папку:
   ```
   CPYTOPCD   FROMFILE(lib/dbfile)  TOFLR(папка) FROMMBR(mbr)  REPLACE(*YES)
   ```
3. Отправка документа:
   ```
   SNDDST   TYPE(*DOC)  TOUSRID(адрес пользователя) DSTD(MAIL) DOC(mbr)  FLR(папка)
   ```

   Ссылки, связанные с данной

   API Отправить электронное сообщение MIME (QtmmSendMail)

Получение электронной почты с помощью служб рассылки Системной сетевой архитектуры (SNADS)

Почту можно получать с помощью клиента SNADS. Получатель сообщения должен быть локальным пользователем SNADS.

Для получения электронной почты выполните следующие действия.

1. В командной строке введите команду QRYDST (Запросить рассылку) и нажмите клавишу F4. Появится список рассылок.
2. Для просмотра дополнительных параметров нажмите клавишу F10.
3. В поле **Файл для получения вывода** укажите любое легко запоминающееся имя библиотеки и файла и нажмите клавишу Enter. Система создает эти физические файлы.
4. Введите команду WRKF (Работа с файлами) и нажмите клавишу Enter. Появится окно Работа с файлами.
5. Введите имена файла и библиотеки, которые вы указали на шаге 3, и нажмите клавишу F4.
6. На экране появится список всех ваших почтовых рассылок. Введите 5 напротив рассылки, которую необходимо просмотреть, и нажмите клавишу Enter.
7. В меню Показать элемент физического файла (DSPPFM) нажмите клавишу Enter.
8. Будет показано меню, в котором каждому почтовому сообщению соответствует длинная строка чисел. Скопируйте в буфер символы с седьмого по двадцать шестой.
9. Дважды нажмите клавишу F3 для выхода.
10. Введите команду RCVDST (Получить рассылку) и нажмите клавишу Enter.
11. В поле **Идентификатор рассылки** вставьте символы с седьмого по двадцать шестой, которые вы ранее скопировали в буфер.
12. В поле **Файл для получения вывода** укажите новое имя файла и заданное ранее имя библиотеки, затем нажмите клавишу Enter.
13. Введите команду DSPPFM (показать элемент физического файла) чтобы просмотреть только что созданный файл.
14. Для прокрутки списка влево нажмите клавишу F20 (Shift + F8) и прочтите сообщение (или сообщения).

Задачи, связанные с данной

“Отправка электронной почты с помощью служб рассылки Системной сетевой архитектуры (SNADS)” на стр. 33
Почту можно отправлять с помощью клиента SNADS. Отправитель сообщения должен быть локальным пользователем SNADS.

Управление электронной почтой

Опытный пользователь или администратор может управлять почтовыми серверами, другими пользователями и сообщениями для надежной доставки почты в сети.

Проверка серверов электронной почты

Наиболее часто проблемы с почтой возникают из-за того, что не запущены нужные серверы. Проверьте состояние почтовых серверов и убедитесь, что все они запущены, прежде чем начать их использовать.

Для проверки состояния серверов выполните следующие действия:

1. В System i Navigator разверните меню ***система*** → **Управление заданиями** → **Задания сервера**.
2. Убедитесь в том, что сервер SMTP запущен. Найдите в списке ″Активные задания сервера″ строки, у которых в столбце ″Имя задания″ показано значение **Qtsmtp**.
3. Если заданий с именем **Qtsmtp** не существует, запустите серверы SMTP.
4. Проверьте, работает ли Среда почтового сервера. Найдите в списке ″Активные задания сервера″ строки, у которых в столбце ″Имя задания″ указано значение **Qmsf**.

5. Если в показанном списке нет ни одного задания Qmsf, введите команду STRMSF (Запустить Среду почтового сервера).
6. Убедитесь в том, что сервер POP запущен. Найдите в списке ″Активные задания сервера″ строки, у которых в столбце ″Имя задания″ указано значение **Qtpop**.
7. Если заданий с именем **Qtpop** не существует, запустите серверы POP.
8. Убедитесь в том, что сервер SNADS запущен. Найдите в списке ″Активные задания сервера″ строки, у которых в столбце ″Имя задания″ указано значение **Qsnads**.
9. Если в списке нет заданий QSNADS, запустите SNADS. Введите в командной строке STRSBS QSNADS.

Для того чтобы электронная почта работала, все почтовые серверы должны быть запущены.

Понятия, связанные с данным

“Запуск и остановка серверов электронной почты” на стр. 21
Запустите необходимые серверы. Это позволит гарантировать, что все серверы работают правильно и что внесенные в их конфигурацию изменения вступили в силу. В некоторых случаях возникает необходимость перезапуска серверов. Для этого необходимо остановить их, а затем снова запустить.

“Определение неполадок электронной почты” на стр. 48
Здесь описаны действия, которые помогут в анализе неполадок электронной почты.

Удаление пользователей электронной почты протокола POP

Удалить пользователей электронной почты POP можно с помощью System i Navigator.

Для удаления пользователя электронной почты из операционной системы необходимо удалить его запись из системного каталога рассылки.

1. В командной строке введите команду WRKDIRE (Работа с записями каталога).
2. С помощью клавиши табуляции перейдите в поле *Опц* для пользователя, которого вы собираетесь удалить.
3. Введите 4 (Удалить) и нажмите клавишу Enter. Нажмите клавишу Enter еще раз для подтверждения. Почта больше не будет доставляться в почтовый ящик POP этого пользователя.
4. Войдите в почтовый клиент POP под именем и с паролем этого пользователя. Получите и удалите все почтовые сообщения.

Предотвращение разбиения длинных почтовых сообщений на блоки

Может потребоваться запретить автоматическое разбиение длинных почтовых сообщений на блоки меньшего размера.

В SMTP можно настроить разбиение больших сообщений на несколько частей. Однако многие почтовые клиенты не могут восстанавливать сообщения из отдельных частей и в результате выдают нечитаемые сообщения. В этом случае функцию разбиения сообщений SMTP необходимо отключить.

Для отключения разбиения длинных почтовых сообщений на блоки в SMTP выполните следующие действия:

1. В System i Navigator разверните меню ***система*** **→ Сеть → Серверы → TCP/IP**.
2. Дважды щелкните на **POP**. Появится окно диалога Свойства POP.
3. Перейдите на страницу **Конфигурация**.
4. В поле **Размер блоков сообщений** выберите значение **Не ограничен**.

Примечание: Отключение разбиения почтовых сообщений на блоки может привести к возникновению ошибок при отправке длинных почтовых сообщений в сети, которые не поддерживают обработку таких сообщений.

Понятия, связанные с данным

“Устранение неполадок в электронной почте” на стр. 48
Здесь приведена информация об устранении возможных неполадок с электронной почтой.

Получение уведомления о состоянии доставки электронной почты

Функция уведомления о состоянии доставки позволяет пользователям запрашивать состояние доставки (DSN) исходящей почты.

Уведомление о доставке позволяет почтовым клиентам получать информацию о состоянии отправленных сообщений: доставлено, переслано или не доставлено. Для поддержки таких запросов необходимо включить функцию Уведомление о состоянии доставки.

Вы всего лишь включаете функцию уведомления о состоянии доставки, делая ее доступной для пользователей, а они должны самостоятельно установить необходимые параметры на своих почтовых клиентах, если пожелают воспользоваться этой функцией. Название и расположение этого параметра зависит от применяемого клиента.

Для включения функции уведомления о состоянии доставки выполните следующие действия:

1. В System i Navigator разверните меню ***система*** → **Сеть** → **Серверы** → **TCP/IP**.
2. Щелкните правой кнопкой на **SMTP** и выберите **Свойства**.
3. Перейдите на страницу Дополнительные параметры.
4. Включите переключатель **Поддержка уведомлений о состоянии доставки (DSN)** и укажите `Адрес ответственного за DSN`.
5. Нажмите **OK**.

Использование функции уведомления о состоянии доставки требует дополнительных ресурсов, что может повлиять на максимальное число получателей почтового сообщения.

Размещение серверов Domino и SMTP в одной системе

Если серверы Domino SMTP работают в одной системе, рекомендуется связать их с разными IP-адресами.

Если серверы Domino иSMTP работают в одной системе, рекомендуется связать их с разными IP-адресами. Почта отправляется пользователям Domino или SMTP по соответствующему IP-адресу, и хотя серверы применяют общий порт, почтовые сообщения обрабатываются только той системой, для которой они предназначены.

Для принудительного указания IP-адреса, с которым должен работать сервер SMTP, выполните следующие действия:

1. В System i Navigator разверните меню ***система*** → **Сеть** → **Серверы** → **TCP/IP**.
2. Щелкните правой кнопкой на **SMTP** и выберите **Свойства**.
3. Перейдите на страницу **Подключения**.
4. Выберите переключатель **Применять все интерфейсы** для подключения к порту 25 всех интерфейсов.
5. Выберите переключатель **Выбрать интерфейс** для указания конкретных интерфейсов клиента и сервера.

   Примечание: Если в системе или в брандмауэре выполняется Преобразование сетевых адресов(NAT), необходимо указать для клиента SMTP i5/OS один определенный IP-адрес.
6. Нажмите **OK**.

Теперь сервер SMTP будет принимать почтовые сообщения, адресованные только указанному IP-адресу. Проверьте, существует ли этот адрес на сервере DNS, в локальной таблице хостов и в системном каталоге рассылки.

Ознакомьтесь с инструкциями. приведенными в справочной библиотеке Lotus Domino по привязке сервера Domino SMTP к конкретному адресу TCP/IP.

Понятия, связанные с данным

“Планирование работы с электронной почтой” на стр. 10
Прежде чем приступить к настройке электронной почты, вы должны определиться с планом использования электронной почты в своей системе.

Фильтрация IP-пакетов и преобразование сетевых адресов (NAT)

Применение хоста Domino LDAP и сервера каталогов в одной системе

Если серверы Domino LDAP и IBM Tivoli Directory Server for i5/OS (Сервер каталогов) работают в одной системе, рекомендуется связать их с разными IP-адресами.

При размещении Domino LDAP и сервера каталогов в одной системе, можно либо задать для каждого сервера отдельный номер порта, либо связать серверы с разными IP-адресами. Изменений номера порта может отрицательно сказаться на работе клиентов, поэтому рекомендуется указывать отдельные IP-адреса. Для адресации электронной почты серверы Domino и SMTP применяют соответствующие серверы LDAP.

Для принудительного указания IP-адреса, с которым должен работать сервер каталогов, выполните следующие действия:

1. В System i Navigator выберите ***система*** → **Сеть** → **Серверы** → **TCP/IP**.
2. Щелкните правой кнопкой на значке **Каталог** и выберите пункт **Свойства**.
3. Перейдите на страницу **Сеть**.
4. Нажмите **IP-адреса**.
5. Выберите опцию **Применять выбранные IP-адреса** и укажите в списке необходимые интерфейсы для связывания.
6. Нажмите кнопку **OK**, чтобы закрыть страницу Каталог - IP-адреса.
7. Нажмите кнопку **OK**, чтобы закрыть страницу Свойства каталога.
8. Необязательно: При работе с Domino LDAP ознакомьтесь с материалами справочной библиотеки Lotus Domino, в которой содержатся инструкции по привязке Domino LDAP к определенному адресу TCP/IP.
9. Запустите серверы для работы с электронной почтой.

Информация, связанная с данной

Библиотека по Lotus Domino

Управление производительностью сервера SMTP

Советы по управлению загруженным многозадачным сервером SMTP.

Это может быть связано с тем, что сервер SMTP все свои ресурсы тратит на добавление и завершение предварительных заданий для каждого почтового запроса.

Если вы обнаружили, что число предварительных заданий слишком велико и это снижает производительность системы, вы можете уменьшить пороговое значение. Если требуется запускать больше предварительных заданий, то пороговое значение можно, наоборот, увеличить.

При использовании предварительных заданий каждый почтовый запрос запускается как отдельное задание. При этом каждое задание обслуживает только своего клиента или сервера. Задание может установить для вызова более продолжительный тайм-аут, чтобы избежать приема ненужных рекламных объявлений (защититься от ″спама″).

Для управления загрузкой сервера SMTP можно изменять следующие параметры:

- Число заданий, запускаемых при инициализации
- Пороговое число заданий
- Число заданий, добавляемых при достижении системой порогового значения
- Максимальное число выполняемых заданий
- Подсистема заданий

При высоком уровне загруженности системы необходимо изменять параметры настройки и сервера, и клиента SMTP.

Сервер SMTP работает со следующим демоном и предварительными заданиями: QTSMTPSRVD и QTMSMTPSRVP. Клиент SMTP работает со следующим демоном и предварительными заданиями: QTSMTPCLTD и QTSMTPCLTP.

Для изменения значений на сервере SMTP выполните следующие действия:

1. В командной строке введите команду CHGPJE (Изменить записи заданий).
2. В полях этого меню введите следующие значения, затем нажмите клавишу Enter.

Приглашение	**Значение**
Подсистема	QSYSWRK
Библиотека	QSYS
Программа	QTMSSRCP
Библиотека	QTCP
Запуск заданий	*SAME
Начальное число заданий	4
Порог	2
Дополнительное число заданий	2
Максимальное число заданий	20

Система с такими параметрами будет первоначально запускать четыре предварительных задания, а при снижении числа доступных заданий до двух будет запускать еще по два дополнительных задания, но общее число предварительных заданий не будет превышать 20.

Изменение значений сервера SMTP

Для изменения значений на сервере SMTP выполните следующие действия.

1. В командной строке введите команду CHGPJE (Изменить записи заданий).
2. В полях этого меню введите следующие значения, затем нажмите клавишу Enter.

Приглашение	**Значение**
Подсистема	QSYSWRK
Библиотека	QSYS
Программа	QTMSSRCP
Библиотека	QTCP
Запуск заданий	*SAME
Начальное число заданий	4
Порог	2
Дополнительное число заданий	2
Максимальное число заданий	20

Система с такими параметрами будет первоначально запускать четыре предварительных задания, а при снижении числа доступных заданий до двух будет запускать еще по два дополнительных задания, но общее число предварительных заданий не будет превышать 20.

Изменение значений клиента SMTP

Для изменения значений на клиенте SMTP выполните следующие действия.

1. В командной строке введите команду CHGPIE (Изменить записи заданий).
2. В полях этого меню введите следующие значения, затем нажмите клавишу Enter.

Приглашение	**Значение**
Подсистема	QSYSWRK
Библиотека	QSYS
Программа	QTMSCLCP
Библиотека	QTCP
Запуск заданий	*SAME
Начальное число заданий	4
Порог	2
Дополнительное число заданий	2
Максимальное число заданий	20

Клиент SMTP с такими параметрами будет первоначально запускать четыре предварительных задания, а при снижении числа доступных заданий до двух будет запускать еще по два дополнительных задания, но общее число предварительных заданий не будет превышать 20.

Выбор новой подсистемы для заданий сервера SMTP

Для того, чтобы выбрать новую подсистему для заданий сервера SMTP, выполните следующие действия.

1. Сервер SMTP можно запускать в отдельной подсистеме. Это повысит производительность, поскольку исключит совместное использование ресурсов.
2. Для указания отдельной подсистемы выполните следующие действия:
   a. В System i Navigator разверните меню ***система*** → **Сеть** → **Серверы** → **TCP/IP**.
   b. Щелкните правой кнопкой на **SMTP** и выберите **Свойства**.
   c. Перейдите на страницу **Дополнительные параметры**.
   d. Выберите опцию **Описание подсистемы**.
   e. Укажите имя и библиотеку описания и очереди заданий новой подсистемы.

Программа проверит существование указанной подсистемы. Если подсистема не существует, то программа создаст новую подсистему, а также записи таблицы выполнения, записи автоматических и предварительных заданий и описания заданий. Даже если подсистема не существует, указанная библиотека должна существовать. При следующем выполнении задания запуска сервера ему будет передано имя новой подсистемы, после чего в пакетном режиме будут запущены задания сервера.

Справочная информация по электронной почте

Справочная информация о записях в журналах почтовых серверов, командах протокола SMTP, а также о командах и параметрах протокола POP.

Журнал почтового сервера

Приведенная в этом разделе информация поможет вам разобраться в кодах и сообщениях, используемых в записях журнала.

Приведенные ниже таблицы содержат дополнительную информацию о записях журналов.

Аббревиатуры в записях журнала

Аббревиатура	Значение
LIN	Получено сообщение для локальной доставки. Следующий за этим IP адрес - это адрес хоста, отправившего сообщение.
RIN	Получено сообщение для пересылки другому демону SMTP. За аббревиатурой следует IP-адрес, с которого было отправлено это сообщение.
R	Получатель
O	Отправитель
U	Получатель недоставленной почты
QTMSINQ	Входящая очередь SMTP
QTMSOUTQ	Исходящая очередь SMTP
QTMSBSSQ	Очередь для временного хранения, в которую помещаются сообщения, если превышен предельный объем системной памяти.
QTMSRTQ1	Очередь повторов первого уровня
QTMSRTQ2	Очередь повторов второго уровня
RRSL	Получатель обработан

Каждая запись журнала начинается с двух символов, обозначающих Подтип или код. Первый символ Подтипа или кода - идентификатор функции записи. Второй символ Подтипа или кода обозначает задокументированное в этой записи журнала действие. Ниже приведен список идентификаторов функций.

Идентификатор функции	Описание
7	Запись сервера комплексной сети
8	Клиент SMTP
9	Сервер SMTP
A	MSF Не доставлено
B	MSF Локальная доставка
C	MSF Пересылка сообщения
D	POP Создать сообщение
E	API Отправить сообщение
F	Domino MTA
G	Подключаемая программа поддержки туннеля
H	SNADS (Переключатель)
I	Анализатор MIME (подключаемая программа локальной доставки)

Идентификатор функции	Описание
L	FAX (Локальная доставка)
M	SNADS
O	Фильтрация
P	MSF Программа выхода SMTP для преобразования адресов

Все приведенные здесь записи журнала относятся к типу LG (запись журнала).

Записи журнала клиента SMTP

Тип	Действие	Подтип или код	Комментарии
LG	Выборка из очереди для обработки	8B	Выборка почты непосредственно после установки тега floater.
LG	Успешная доставка почты	88 82	Запись об успешной отправке почты. Запись о каждом получателе.
LG	Невозможность доставки почты	83	Запись о том, что почта не доставлена
LG	Тайм-аут первого уровня	8C	Добавление в очередь повторов первого уровня.
LG	Тайм-аут второго уровня	8D	Добавление в очередь повторов второго уровня.
LG	Почта готова к повторной передаче	8E 8F	Повторное помещение почты в QTMSOUTQ.
LG	Отправка COD отправителю	87	Запись о помещении сообщения, подтверждающего доставку (COD), в очередь BRSR.
LG	Обработка невозможна, ресурс занят	86	Помещение почты обратно в QTMSOUTQ из-за переполнения метрики соединения.
LG	Проверка записей получателя	86	Помещение почты обратно в QTMSOUTQ из-за изменения состояния получателя, например, запись MS показала готовность к доставке сообщения.
LG	Невозможность доставки	87	Передача сообщения о невозможности доставки в QTMSINQ
LG	Запрос MX	8K	Сбой res_send с указанием errno причины и буфера запроса

Записи журнала сервера SMTP

Тип	Действие	Подтип или код	Комментарии
LG	Прием почты	94 91 92 9T 99	Непосредственно после получения завершающей последовательности CRLF <.> CRLF (при локальной отправке). Записываются отправитель и получатель. Размер сообщения в формате *nnnnn* (с учетом вложений). MSGID
LG	Получение переданной почты	95 91 92	Записать MAIL непосредственно после получения завершающей последовательности <.> CRLF (при пересылке). Записываются отправитель и получатель.
LG	Передача почты серверу комплексной сети	97	Запись MAIL в QTMSINQ (входящая почта).
LG	Передача почты клиенту для удаленной доставки	96	Запись MAIL в QTMSOUTQ (пересылаемая почта).
LG	В СОЕДИНЕНИИ ОТКАЗАНО 1.2.3.4....	9S	Запись об отказе в соединении на основе параметров, запрещающих соединение. 1.2.3.4 - отклоненный IP-адрес.
LG	В ПЕРЕСЫЛКЕ ОТКАЗАНО 1.2.3.4....	9V	Запись об отказе в пересылке на основе параметров, запрещающих пересылку. 1.2.3.4 - отклоненный IP-адрес.
LG	Отклонено сервером SMTP	9W	Сообщение было отклонено сервером SMTP.

Записи журнала мостового сервера

Тип	Действие	Подтип или код	Комментарии
LG	Получение почты из очереди IN	7A	Запись о получении почты из очереди QTMSINQ.
LG	Передача почты в SNADS	7O	Запись об успешной передаче в QSNADS.
LG	Помещение контейнера в очередь BUSY из-за нехватки памяти	7L	Запись о помещении почты в очередь QTMSBSSQ при превышении порога
LG	Получение почты из очереди IN	7M	Запись о получении почты из очереди QTMSBSSQ. Память была освобождена, и теперь почту можно доставить.

Тип	Действие	Подтип или код	Комментарии
LG	Передача сообщения в MSF	7H 71 72	Запись о передаче сообщения в рабочую среду.
LG	Создание сообщения COD	7R 7G	Запись о передаче сообщения COD в рабочую среду. Запись MSGID MSF в связи с созданием нового сообщения COD.
LG	Не удается доставить почтовое сообщение получателю	7P 7G	Запись о факте создания уведомления о невозможности доставки. Запись MSGID о новом уведомлении о невозможности доставки сообщения.

MSF завершает работу и создает функции

Тип	Действие	Подтип или код	Комментарии
LG	Создание сообщения о невозможности доставки	AP A1 A2	Запись о помещении сообщения о невозможности доставки в MSF.
LG	Почта доставлена в почтовый ящик POP	B8 B2	Запись о доставке почты в локальный почтовый ящик, IP-адрес обозначает каталог почтового ящика POP. Также указан получатель.
LG	Отправка сообщения COD в MSF	BR B1 B2	Запись о помещении сообщения COD в MSF.
LG	Проверка готовности	CN	Программа выхода MSF пересылки сообщения SMTP. Запись MSGID возвращена в очередь QMSF, так как сервер SMTP не запущен.
LG	Помещение почты в очередь	C6 C1 C2	Запись о помещении почты в очередь QTMSOUTQ
LG	Вызов API Sendmail	EH E1 E2 ET	апись о создании сообщения API SendMail. Размер сообщения в формате *nnnnn* (с учетом вложений).
LG	Почта направляется в удаленную систему SNADS	G8 G2	Запись об отправке сообщения через туннель. Включить запись о системе, отправленной получателю.
LG	Получено сообщение через туннель SNADS.	GQ G2	Запись о получении сообщения через туннель для локальной доставки.
LG	Преобразование адресов SNADS для адреса отправителя/получателя	H1	Служба SNADS поместила сообщение в MSF.

Тип	Действие	Подтип или код	Комментарии
LG	Повторное помещение проанализированного уведомления MIME в рабочую среду	IH I1 I2 IG	Запись о повторном помещении проанализированного сообщения MIME в MSF.
LG	Отклонено функцией фильтрации	OW	Сообщение отклонено. Указано, было ли оно отброшено или сохранено. Если сообщение было перезаписано и доставлено, то это также отмечено.
LG	Помечено программой выхода MSF преобразования адресов SMTP	P2	Сообщение помечено следующим образом: • **POP LclDel:** Помечено для доставки программой выхода POP, выполняющей локальную доставку. • **SMTP MsgFwd:**Помечено для пересылки на SMTP для последующей отправки. • **SMTP NonDel:**Помечено для уведомления о невозможности доставки. • **Parse:** Отправлено в программу синтаксического анализа. • **PutBk:** Помещено обратно в рабочую среду для обработки другой программой выхода (например, Domino или SNADS) • **chg to SNADS:** Тип адреса изменен на SNADS.

Задачи, связанные с данной

“Проверка журналов компонентов” на стр. 50
Для того чтобы определить, как устранить неполадки электронной почты, просмотрите журналы, содержащие записи ошибок.

Простой протокол передачи почты (SMTP)

Простой протокол передачи почты (SMTP) основан на TCP/IP и позволяет отправлять и принимать почтовые сообщения. Обычно он применяется вместе с POP3 или IMAP для сохранения сообщений в почтовом ящике на сервере и периодического запроса почты с сервера пользователем.

Команды SMTP

В таблице перечислены команды SMTP, их функции, и указано, поддерживает ли их сервер SMTP i5/OS/

Команда SMTP	Функция	Поддержка System i
AUTH (Идентификация)	Указывает механизм идентификации для сервера SMTP. Поддерживаются значения PLAIN и LOGIN.	Да

Команда SMTP	Функция	Поддержка System i
DATA (Данные)	Указывает, что начинается содержимое почтового сообщения.	Да
EHLO (Расширенное приветствие)	Включить расширения SMTP.	Да
EXPN (Развернуть)	Запрашивает у получателя подтверждение идентификации списка рассылки.	Нет
HELO (Приветствие)	Идентифицирует отправителя сообщения SMTP.	Да
HELP (Справка)	Запрашивает у получателя справочную информацию для отправителя.	Да
MAIL (Почта)	Начинает почтовую транзакцию для доставки почтового сообщения одному или нескольким получателям.	Да
NOOP (Нет операции)	Запрашивает у получателя допустимый ответ (не указывая никакого другого действия).	Да
QUIT (Завершить)	Указывает, что получатель должен отправить допустимый ответ, а затем закрыть канал передачи.	Да
RCPT (Получатель)	Идентифицирует получателя почтового сообщения.	Да
RSET (Сброс)	Завершает текущую почтовую транзакцию.	Да
SAML (Отправить и передать почту)	Доставляет почту на одну или несколько рабочих станций, либо получателям, если пользователь неактивен.	Нет
SEND (Отправить)	Доставляет почту на одну или несколько рабочих станций.	Нет
SOML (Отправить или передать почту)	Доставляет почту на одну или несколько рабочих станций, либо получателям, если пользователь неактивен.	Нет
STARTTLS (Запустить TLS)	Обращается к серверу SMTP с командой запустить согласование Secure Sockets Layer (SSL) или TLS с клиентом SMTP для установления сеанса SSL или TLS.	Да
TURN (Переключить)	Указывает, что получатель должен либо отправить допустимый ответ и переключиться в режим отправки SMTP, либо отправить отказ и остаться в режиме приема SMTP.	Нет
VRFY (Проверить)	Запрашивает у получателя подтверждение идентификации пользователя.	Да

Понятия, связанные с данным

“Сценарий: Отправка и получение почтовых сообщений в локальной системе” на стр. 5
В этом сценарии показана передача электронной почты между локальными пользователями.

Протокол POP

Почтовый протокол POP версии 3 описан в RFC 1939 (POP3), RFC 2449 (Механизм расширения POP3) и RFC 2595 (Использование TLS с IMAP, POP3 и ACAP). RFC - это разрабатываемые стандарты Internet.

Для взаимодействия с сервером клиент протокола POP передает ему команды, называемые также *глагольными командами*.Сервер POP системы i5/OS поддерживает следующие команды.

Команда и параметры	Описание
USER <id>	Идентификатор пользователя
PASS <password>	Пароль
STAT	Опросить почтовый ящик
LIST <opt msg #>	Информация о сообщениях
RETR <msg #>	Получить сообщение
DELE <msg #>	Удалить сообщение
RSET	Сбросить состояние удаления сообщения
TOP <msg #> <lines>	Получить заголовок и данные сообщения
UIDL <opt msg #>	Список уникальных идентификаторов сообщений
NOOP	Пустая операция
QUIT	Закрыть сеанс клиента
CAPA	Вывести список функций
STLS	Запустить TLS

Понятия, связанные с данным

“Сценарий: Отправка и получение почтовых сообщений в локальной системе” на стр. 5
В этом сценарии показана передача электронной почты между локальными пользователями.

“Почтовый протокол POP в i5/OS” на стр. 4
Сервер Почтового протокола (POP) - это реализация интерфейса протокола POP версии 3 на сервере i5/OS.

Устранение неполадок в электронной почте

Здесь приведена информация об устранении возможных неполадок с электронной почтой.

Задачи, связанные с данной

“Предотвращение разбиения длинных почтовых сообщений на блоки” на стр. 37
Может потребоваться запретить автоматическое разбиение длинных почтовых сообщений на блоки меньшего размера.

Определение неполадок электронной почты

Здесь описаны действия, которые помогут в анализе неполадок электронной почты.

Для определения возможных причин неполадок SMTP выполните следующие действия:

1. Убедитесь, что протокол TCP/IP настроен для работы с электронной почтой.
   a. Убедитесь в том, что установлены все необходимые PTF.
   b. Убедитесь, что работают все необходимые почтовые серверы.
2. Проверьте имя локального домена.
   a. В System i Navigator разверните меню ***система*** → **Сеть**.
   b. Щелкните правой кнопкой на значке **Конфигурация TCP/IP** и выберите **Свойства**.

c. Щелкните на вкладке **Информация о домене хоста** и проверьте имя локального домена.

3. Установите меньшие значения для параметров повтора SMTP.
   a. В System i Navigator разверните меню ***система*** **→ Сеть → Серверы → TCP/IP**.
   b. Дважды щелкните на **SMTP**.
   c. Откройте страницу **Интервал повторной отправки сообщений**.
4. Проверьте, правильно ли указан ИД пользователя и адрес получателя в системном каталоге рассылки.
   a. В System i Navigator разверните меню ***система*** **→ Пользователи и группы → Все пользователи**.
   b. Щелкните правой кнопкой на значке **Профайл** и выберите **Свойства**.
   c. Выберите **Личные**, перейдите на страницу **Почта** и проверьте указанный адрес.
5. Проверьте, требуется ли для доставки почтового сообщения по целевому адресу запись таблицы хостов.
   a. В командной строке введите команду CHGTCPHTE (Изменить запись таблицы хостов TCP/IP) и IP-адрес почтового сервера.
   b. Если запись таблицы хостов не появится, введите имя хоста для этого IP-адреса.
6. Убедитесь, что не превышен порог памяти.
   a. В System i Navigator выберите ***система*** **→ Настройка и обслуживание → Аппаратное обеспечение → Дисковые накопители → Дисковые пулы**.
   b. Щелкните правой кнопкой мыши на исходном пуле дисков, который необходимо просмотреть, и выберите пункт **Свойства**.
   c. Перейдите на страницу **Емкость**.

      Если пороговое значение превышено, электронная почта может не работать.
7. Убедитесь, что функция разбиения почтовых сообщений на блоки отключена.
   a. В System i Navigator разверните меню ***система*** **→ Сеть → Серверы → TCP/IP**.
   b. Дважды щелкните на **POP**.Появится окно диалога Свойства POP.
   c. Перейдите на страницу **Конфигурация**.
   d. Убедитесь, что в поле **Размер блоков сообщений** выбрано значение **Не ограничен**.
8. Вызовите команду Трассировать приложения TCP/IP. Для этого введите TRCTCPAPP в командной строке.
9. Проверьте журналы компонентов и найдите информацию о неполадке.

Понятия, связанные с данным

“Управление доступом к электронной почте” на стр. 11
Для того чтобы защитить свои данные от разрушительных воздействий, необходимо контролировать, кто имеет доступ к системе через электронную почту.

Примеры независимых пулов дисков

“Управление доступом POP” на стр. 12
Для защиты системы необходимо управлять доступом к ней по протоколу POP.

“Устранение неполадок в API QtmmSendMail” на стр. 51
Процедура устранения неполадок API Отправить сообщение MIME (QtmmSendMail).

Задачи, связанные с данной

“Проверка серверов электронной почты” на стр. 36
Наиболее часто проблемы с почтой возникают из-за того, что не запущены нужные серверы. Проверьте состояние почтовых серверов и убедитесь, что все они запущены, прежде чем начать их использовать.

“Настройка TCP/IP для работы с электронной почтой” на стр. 15
Прежде чем настраивать электронную почту в системе, нужно настроить TCP/IP.

“Проверка заданий среды почтового сервера” на стр. 52
Проверьте состояние заданий Среды почтового сервера в системе QSYSWRK, чтобы определить возможную причину ошибки в API QtmmSendMail.

“Проверка журналов компонентов” на стр. 50
Для того чтобы определить, как устранить неполадки электронной почты, просмотрите журналы, содержащие записи ошибок.

“Отслеживание недоставленных сообщений” на стр. 51
Для отслеживания неполадок, связанных с доставкой почты, можно применить шаблон ИД пользователя. Это может оказаться полезным при устранении неполадок, связанных как с доставкой электронной почты, так и с настройкой почтовых программ.

Информация, связанная с данной

Поддержка для IBM System i

Проверка журналов компонентов

Для того чтобы определить, как устранить неполадки электронной почты, просмотрите журналы, содержащие записи ошибок.

Операционная система работает с очередями, программами и журналами, которые позволяют определить возможную причину сбоя при отправке почты. Ведение журнала позволяет отслеживать неполадки в системе электронной почты. Для ведения журнала используются ресурсы процессора, поэтому система работает быстрее, если эта функция отключена.

Функция ведения журнала регистрирует следующие элементы:

- Переходы - перемещение почты между программами и очередями.
- События - получение почты сервером, доставка почты клиенту, помещение почты в очереди повторов и очереди, применяемые при занятых ресурсах.
- Статистические и дополнительные данные- идентификаторы сообщений стандарта 822 и MSF, размер сообщений, отправителей и получателей.

Записи журналов хранятся в получателях журналов. Этими журналами управляют пользователи. При заполнении журнала введите команду Изменить журнал (CHGJRN), чтобы сменить получатель журнала. Новая функция ведения журнала SMTP применяет журнал QZMF.

Для включения функции ведения журнала и просмотра его содержимого выполните следующие действия:

1. В System i Navigator разверните меню ***система*** → **Сеть** → **Серверы** → **TCP/IP**.
2. Дважды щелкните на **SMTP**.
3. Перейдите на страницу **Общие**.
4. Отметьте переключатель **Разрешить ведение журнала**.
5. Откройте сеанс эмуляции.
6. Для преобразования записей журнала SMTP к читаемому виду введите в командной строке: `DSPJRN JRN(QZMF) OUTPUT(*OUTFILE) OUTFILE(jrnlib/zmfstuff) OUTMBR(MAR2) ENTDTALEN(512)`, где *jrnlib* - имя библиотеки, а *zmfstuff* - имя физического файла.
7. Для просмотра записей журнала SMTP введите в командной строке: `DSPPFM FILE(jrnlib/zmfstuff) MBR(MAR2)`
8. Для просмотра информации в журнале нажмите F20 (Shift + F8).

Понятия, связанные с данным

“Определение неполадок электронной почты” на стр. 48
Здесь описаны действия, которые помогут в анализе неполадок электронной почты.

Ссылки, связанные с данной

“Журнал почтового сервера” на стр. 41
Приведенная в этом разделе информация поможет вам разобраться в кодах и сообщениях, используемых в записях журнала.

Отслеживание недоставленных сообщений

Для отслеживания неполадок, связанных с доставкой почты, можно применить шаблон ИД пользователя. Это может оказаться полезным при устранении неполадок, связанных как с доставкой электронной почты, так и с настройкой почтовых программ.

1. Выберите или создайте новый идентификатор пользователя для получения уведомлений. В командной строке введите команду CRTUSRPRF (Создать пользовательский профайл) и нажмите Enter.
2. Введите команду WRKDIRE (Работа с записями каталога) и нажмите клавишу Enter.
3. Для добавления пользователя в системный каталог рассылки введите 1.
4. Убедитесь, что в поле Хранилище почты задано значение 2, а в поле Предпочитаемый адрес - значение 3.
5. Нажмите PF19 (Добавить имя для SMTP).
6. В качестве адреса SMTP для пользователя POP введите NONDELIVERY@локальный_хост.домен.

Этот пользователь будет получать копию каждого недоставленного почтового сообщения.

Примечание: Заданный вами идентификатор пользователя должен быть фактическим идентификатором пользователя, чтобы можно было эффективно отслеживать недоставленные сообщения. Отправитель получает копию недоставленного сообщения вместе со списком адресатов, которые не смогли получить это сообщение.

Понятия, связанные с данным

“Определение неполадок электронной почты” на стр. 48
Здесь описаны действия, которые помогут в анализе неполадок электронной почты.

Устранение неполадок в API QtmmSendMail

Процедура устранения неполадок API Отправить сообщение MIME (QtmmSendMail).

При вызове API QtmmSendMail могут возникать ошибки. Описания сообщений об ошибках, которые выдает API, содержатся в разделе по QtmmSendMail API.

Понятия, связанные с данным

“Определение неполадок электронной почты” на стр. 48
Здесь описаны действия, которые помогут в анализе неполадок электронной почты.

Ссылки, связанные с данной

API Отправить электронное сообщение MIME (QtmmSendMail)

Проверка вызова API

Для того чтобы восстановить работу после ошибки API QtmmSendMail, убедитесь в том, что сообщения об ошибках, отправляемые API, выдаются на дисплей вашей рабочей станции.

Если вы предусмотрите в программе операцию возврата ошибки, то программа будет возвращать информацию об ошибке в вызывающую программу. Однако, если установить это значение равным нулю (как это сделано в приведенном ниже примере), то сообщения об ошибках будут выдаваться на дисплей вашей рабочей станции.

Пример программы на C

```
Qus_EC_t         Snd_Error_Code;
Snd_Error_Code.Bytes_Provided=0;
```

Пример программы на RPG

```
DAPIError     DS
D APIBytes          1     4B 0
D CPFId             9    15
C              Eval    APIBytes   = 0
```

Проверка файла Многоцелевых расширений почты Internet (MIME)

Возможно, что ошибки в API QtmmSendMail возникают из-за файла MIME. Проверьте файл MIME, чтобы исправить ошибки.

1. Проверьте расположение файла MIME. Файл MIME должен находиться в файловой системе root и начинаться с косой черты ″/″, например /myfile.txt, а имя файла должно содержать путь: /mydirectory/myfile.mime.
2. Проверьте уровень доступа. Для профайлов QMSF и QTCP должны быть заданы права на чтение и удаление файла MIME.
   a. В командной строке введите команду WRKLNK (Работа со связями объекта).
   b. Для работы с правами доступа QMST и QTCP введите 9 (Показать). Появится окно Работа с правами доступа.
3. Убедитесь, что в файле MIME между заголовком и телом сообщения есть оператор конца заголовка (CRLFCRLF).
4. Убедитесь в том, что файл MIME соответствует требованиям MIME Request for Comments (RFC).

Примечание: Дополнительная информация об операторах конца заголовка содержится в разделе 2.1 RFC2822 (http://rfc.net/rfc2822.html).

Проверка заданий среды почтового сервера

Проверьте состояние заданий Среды почтового сервера в системе QSYSWRK, чтобы определить возможную причину ошибки в API QtmmSendMail.

1. Если обработка сообщения была прекращена Средой почтового сервера (MSF), проверьте, нет ли сообщений об ошибках от заданий MSF.
2. Если задание MSF завершилось, файл MIME должен быть удален. Это означает, что MSF обработала файл MIME. Проблема связана не с API, а с конфигурацией SMTP.

Понятия, связанные с данным

“Определение неполадок электронной почты” на стр. 48
Здесь описаны действия, которые помогут в анализе неполадок электронной почты.

Связанная информация по работе с электронной почтой

В инструкциях к продуктам, публикациях IBM Redbooks, на Web-сайтах и в других сборниках разделов информационного центра содержится информация, связанная с разделами о работе с электронной почтой. Файлы PDF можно и просматривать, и печатать.

Руководства

AnyMail/400 Mail Server Framework Support (около 622 Кб)

Информация о среде, управляющей почтовым сервером i5/OS.

IBM Redbooks (Руководства по выполнению задач)

- AS/400 Electronic-Mail Capabilities (около 3593 Кб)

  Популярное руководство по выполнению задач IBM Redbooks. Содержит подробную информацию об электронной почте и SMTP.

- AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet (около 2160 Кб)

  В этом руководстве Redbooks приведена информация о защите, включая описание действий по очистке операционной системы i5/OS, если ваша система стала жертвой лавинной атаки.

Web-сайты

- Поддержка для IBM System i

  Вы можете загрузить текущие PDF для операционной системы i5/OS, спользуя свою рабочую станцию в качестве шлюза, соединяющего со страницей PTF Internet, а также просмотреть варианты конфигурации i5/OS, хранящиеся в базах данных технической информации.

- RFC Index

  Протоколы электронной почты определены в документах RFC. Так называются разрабатываемые стандарты Internet. Дополнительная информация о SMTP приводится в RFC 1939 (POP3), RFC 2449 (Механизм расширения POP3) и RFC 2595 (Использование TLS с IMAP, POP3 и ACAP).

- Lotus Domino for i5/OS

  На этой Web-странице представлен продукт Lotus Domino для i5/OS и решения, предоставляемые этой лицензионной программой.

- Lotus Справочная библиотека Domino

  Информация о Domino из информационных бюллетеней, книг, презентаций и т.д.

- Документация по Lotus

  На страницах документации по Lotus содержатся ссылки на ресурсы, например, на документацию по продуктам, информационные бюллетени, публикации Redbooks и т.д.

Прочая информация

Защита системы System i при работе с Internet

В этом разделе information center приведена информация о защите сети System i.

Ссылки, связанные с данной

“Файл PDF об электронной почте” на стр. 2
Файл PDF этой информации можно просмотреть и напечатать.

Приложение. Примечания

Настоящая документация была разработана для продуктов и услуг, предлагаемых на территории США.

IBM может не предлагать продукты и услуги, упомянутые в этом документе, в других странах. Информацию о продуктах и услугах, предлагаемых в вашей стране, вы можете получить в местном представительстве IBM. Ссылка на продукт, программу или услугу IBM не означает, что может применяться только этот продукт, программа или услуга IBM. Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако в этом случае ответственность за проверку работы этих продуктов, программ и услуг возлагается на пользователя.

IBM могут принадлежать патенты или заявки на патенты, относящиеся к материалам этого документа. Предоставление вам настоящего документа не означает предоставления каких-либо лицензий на эти патенты. Запросы на приобретение лицензий можно отправлять по следующему адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Запросы на лицензии, связанные с информацией DBCS, следует направлять в отдел интеллектуальной собственности в местном представительстве IBM или в письменном виде по следующему адресу:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Следующий абзац не относится к Великобритании, а также к другим странам, в которых это заявление противоречит местному законодательству: INTERNATIONAL BUSINESS MACHINES CORPORATION ПРЕДОСТАВЛЯЕТ НАСТОЯЩУЮ ПУБЛИКАЦИЮ НА УСЛОВИЯХ “КАК ЕСТЬ”, БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, НЕЯВНЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ ПРАВ, КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КАКОЙ-ЛИБО ЦЕЛИ. В некоторых странах запрещается отказ от каких-либо явных и подразумеваемых гарантий при заключении определенных договоров, поэтому данное заявление может не действовать в вашем случае.

В данной публикации могут встретиться технические неточности и типографские опечатки. В информацию периодически вносятся изменения, которые будут учтены во всех последующих изданиях настоящей публикации. IBM оставляет за собой право в любое время и без дополнительного уведомления исправлять и обновлять продукты и программы, упоминаемые в настоящей публикации.

Все встречающиеся в данной документации ссылки на Web-сайты других компаний предоставлены исключительно для удобства пользователей и не являются рекламой этих Web-сайтов. Материалы, размещенные на этих Web-сайтах, не являются частью информации по данному продукту IBM и ответственность за применение этих материалов лежит на пользователе.

IBM может использовать и распространять любую предоставленную вами информацию на свое усмотрение без каких-либо обязательств перед вами.

© Copyright IBM Corp. 1998, 2008

Для получения информации об этой программе для обеспечения: (i) обмена информацией между независимо созданными программами и другими программами (включая данную) и (ii) взаимного использования информации, полученной в ходе обмена, пользователи данной программы могут обращаться по адресу:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Такая информация может предоставляться на определенных условиях, включая, в некоторых случаях, уплату вознаграждения.

Описанная в этом документе лицензионная программа и все связанные с ней лицензионные материалы предоставляются IBM в соответствии с условиями Соглашения с заказчиком IBM, Международного соглашения о лицензии на программу IBM, Соглашения о лицензии на машинный код или любого другого эквивалентного соглашения.

Все приведенные показатели производительности были получены в управляемой среде. В связи с этим результаты, полученные в реальной среде, могут существенно отличаться от приведенных. Некоторые измерения могли быть выполнены в системах, находящихся на этапе разработки, поэтому результаты измерений, полученные в серийных системах, могут отличаться от приведенных. Более того, некоторые значения могли быть получены в результате экстраполяции. Реальные результаты могут отличаться от указанных. Пользователи, работающие с этим документом, должны удостовериться, что используемые ими данные применимы в имеющейся среде.

Информация о продуктах других изготовителей получена от поставщиков этих продуктов, из их официальных сообщений и других общедоступных источников. IBM не выполняла тестирование этих продуктов других фирм и не может подтвердить точность заявленной информации об их производительности, совместимости и других свойствах. Запросы на получение дополнительной информации об этих продуктах должны направляться их поставщикам.

Все заявления, касающиеся намерений и планов IBM, могут изменяться и отзываться без предварительного уведомления, и отражают только текущие цели и задачи.

Эта информация содержит примеры данных и отчетов, применяемых в повседневной работе. Для того чтобы примеры были максимально наглядными, в них указаны имена людей, а также названия компаний, товарных знаков и продуктов. Все они являются вымышленными, и любое совпадение с реально существующими именами и названиями случайно.

Лицензия на продукты, защищенные авторским правом:

В настоящей документации приведены примеры исходных текстов прикладных программ, иллюстрирующие некоторые приемы программирования в различных операционных платформах. Вы можете копировать, изменять и распространять эти примеры бесплатно в целях разработки, использования, маркетинга и распространения программ, согласованных с программным интерфейсом соответствующих платформ. Работа примеров не была проверена во всех возможных условиях. По этой причине, IBM не может гарантировать их надежность и пригодность.

Любая копия или часть этих примеров программ, а также произведений, созданных на их основе, должна содержать следующее заявление об авторских правах:

© (название вашей компании) (год). Этот код частично создан на основе примеров программ фирмы IBM Corp. (IBM Corp. Sample Programs). © Copyright IBM Corp. _введите год или годы_. Все права защищены.

В электронной версии данной документации фотографии и цветные иллюстрации могут отсутствовать.

Информация об интерфейсе программирования

В настоящей электронной документации приведена информация об интерфейсах программирования, которые позволяют заказчикам создавать программы, использующие службы IBM i5/OS.

Товарные знаки

Ниже перечислены товарные знаки International Business Machines Corporation в Соединенных Штатах и/или других странах:

AIX
AS/400
Domino
eServer
i5/OS
IBM
IBM (эмблема)
Infoprint
iSeries
Lotus
Lotus Notes
Redbooks
System i
The Output of e-business
Tivoli

Adobe, логотип Adobe, PostScript и логотип PostScript являются либо зарегистрированными товарными знаками, либо товарными знаками Adobe Systems Incorporated в США и/или других странах.

Linux является зарегистрированным товарным знаком Линуса Торвальдса (Linus Torvalds) в США и/или других странах.

Microsoft, Windows, Windows NT и эмблема Windows являются товарными знаками корпорации Microsoft в Соединенных Штатах и/или других странах.

Java и все товарные знаки Java-based являются товарными знаками корпорации Sun в Соединенных Штатах и/или других странах.

Другие названия фирм, продуктов и услуг могут являться товарными знаками или знаками обслуживания других фирм.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED ″AS-IS″ AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Напечатано в Дании