Лекция № 7. Электронная почта

Содержание

1. Принципы организации
2. Формат письма
3. Протокол SMTP

История обмена сообщениями: начала

60-е Передача сообщений между пользователями одного мэйнфрейма.

Рост ARPANET взывал появление стандартов обмена сообщениями.

1971 Mail Box Protocol, RFC 196

Ray Tomlinson создал SNDMSG

1973 Network Mail Meeting Summary, RFC 469

A Proposed Mail Protocol, RFC 524

1980 Mail Transfer Protocol, RFC 772, Jon Postel

1981 Simple Mail Transfer Protocol, RFC 772, Jon Postel

Выход 4.1cBSD и Sendmail

История обмена сообщениями

1982 SMTP описан в RFC 881
обновлен 2821 (01 г.), 5321 (08 г.)

1993 RFC 1425 Extended SMTP (ESMTP),
обновлен 1651 (94 г.), 1869 (95 г.)

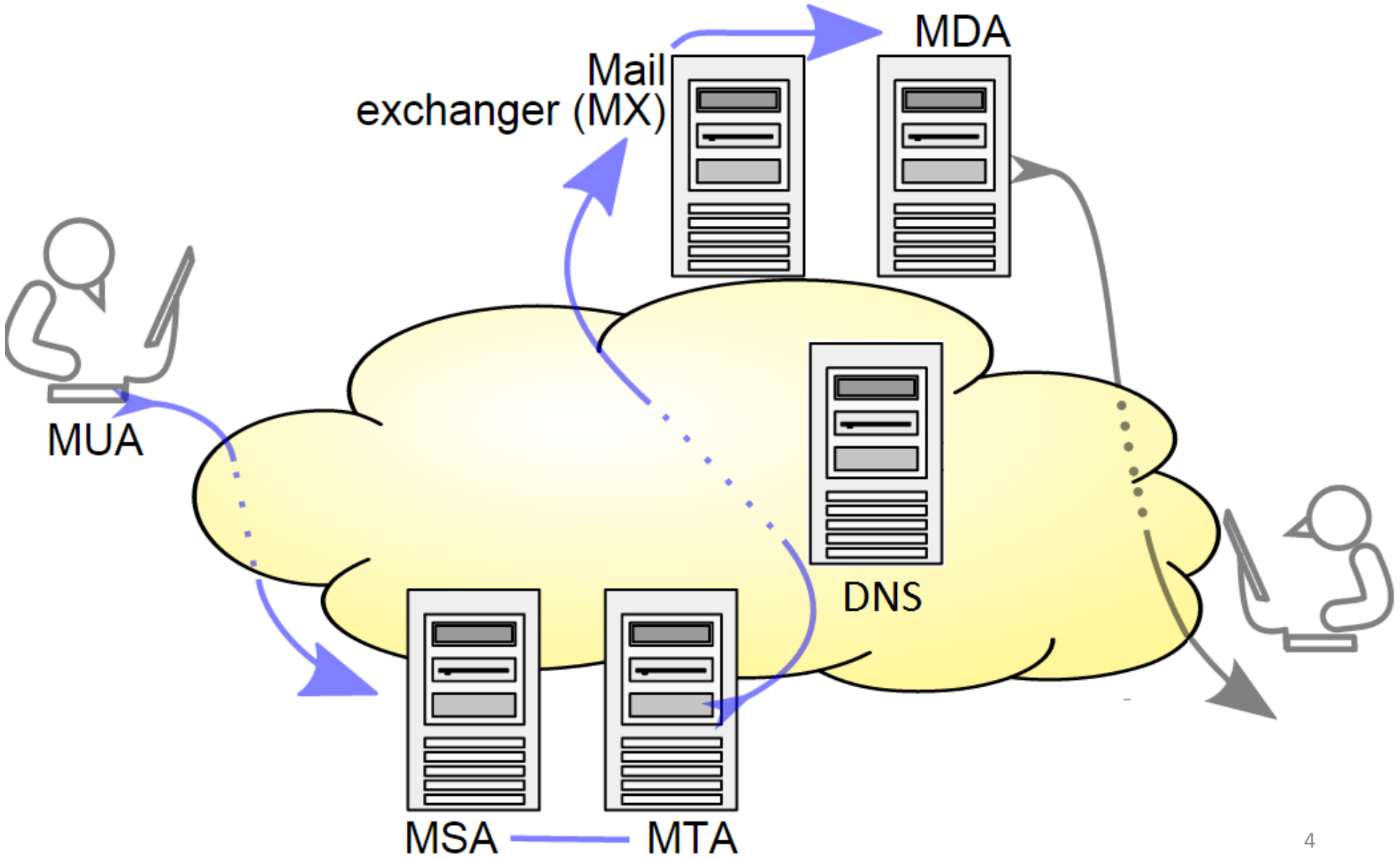
1998 RFC 2476 Message Submission
обновлен 4409 (06 г.), 6409 (11 г.)

1999 RFC 2554 SMTP Service Extension for Authentication
обновлен 4954 (07 г.), 5248 (08 г.)

15 октября 1998. Бесплатная почта от Mail.Ru

01 апреля 2004. Бесплатная почта от Google

Концептуальная схема



Основные участники обмена

Mail User Agent – ПО, устанавливаемое на компьютере пользователя и предназначенное для получения, написания, отправки и хранения сообщений электронной почты.

Mail Submission Agent – ПО, принимающее электронные письма от MUA и работающее совместно с MTA для доставки этого письма.

https://en.wikipedia.org/wiki/Mail_submission_agent

Mail Transfer Agent – ПО, передающее сообщения от одного компьютера к другому.

Mail Delivery Agent – ПО, принимающее входящие электронные письма и доставляющее их на электронный ящик получателя (или перенаправляющее их на другой почтовый сервер, если адрес назначения расположен на другом компьютере)

Простейшая схема отправки почты

Отправитель

SMTP

Почтовый сервер отправителя

DNS сервер отправителя

DNS: корневой сервер + TLD

SMTP

Почтовый сервер получателя

DNS сервер получателя

POP3

Получатель

Формат письма

конверт – заголовок SMTP

Имя отправляющего узла: параметр EHLO, IP
MAIL FROM
RCPT TO

письмо

Date
From
To
Message-ID
Subject

Hello! This is a test message.
It was separated with empty line from header.
Best regards.

Заголовки письма

From

To

CC

BCC

Sender

Reply-To

Return-Path

Received

Message-ID

In-Reply-To

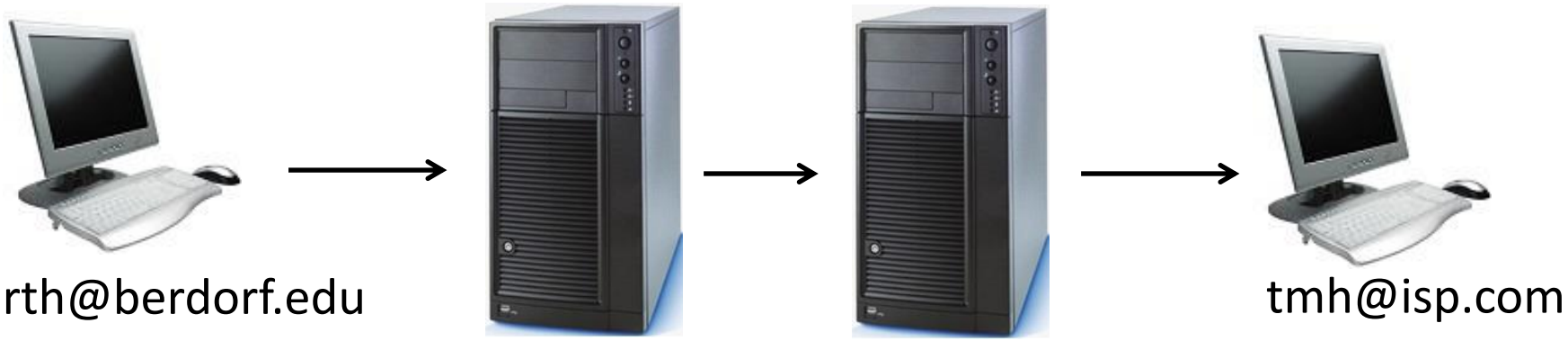
Subject

Date

MIME-Version

Content-Type

Анализ заголовков



rth@berdorf.edu
alpha.berdorf.edu

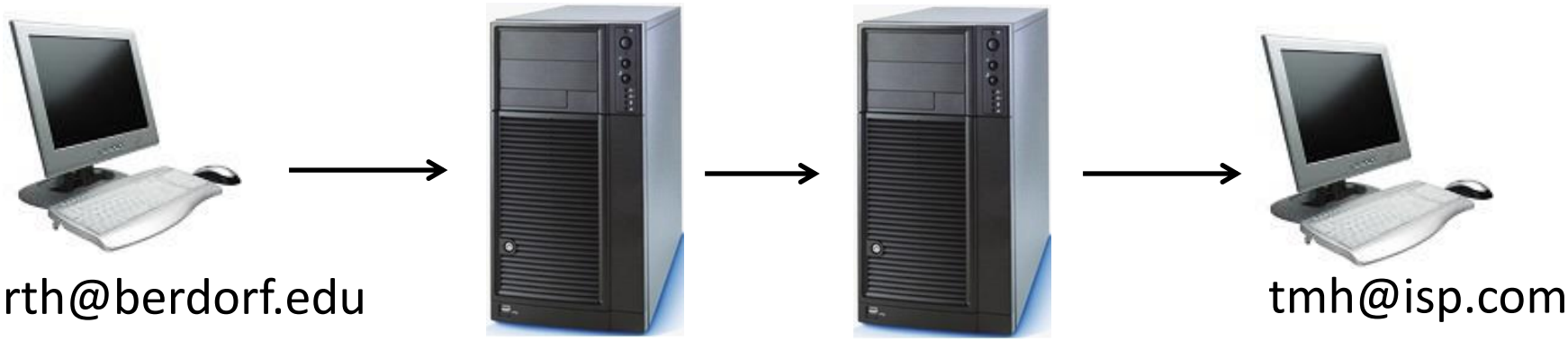
mail.berdorf.edu

mailhost.isp.com

tmh@isp.com

From: rth@berdorf.edu (R.T. Hood)
To: tmh@isp.com
Date: Tue, Mar 18 1997 14:36:14 PST
X-Mailer: Loris v2.32
Subject: Lunch today?

Анализ заголовков



rth@berdorf.edu
alpha.berdorf.edu

mail.berdorf.edu

mailhost.isp.com

tmh@isp.com

Received: from mail.berdorf.edu (mail.berdorf.edu [124.211.3.78]) by mailhost. isp.com (8.8.5/8.7.2) with ESMTP id LAA20869 for ; Tue, 18 Mar 1997 14:39:24 -0800 (PST)

Received: from alpha.berdorf.edu (alpha.berdorf.edu [124.211.3.11]) by mail.berdorf.edu (8.8.5) id 004A21; Tue, Mar 18 1997 14:36:17 -0800 (PST)

Анализ заголовков

Received: from mail.berdorf.edu (mail.berdorf.edu [124.211.3.78]) by mailhost. isp.com (8.8.5/8.7.2) with ESMTP id LAA20869 for <tmh@immense-isp.com>; Tue, 18 Mar 1997 14:39:24 -0800 (PST)

Received: from alpha.berdorf.edu (alpha.berdorf.edu [124.211.3.11]) by mail.berdorf.edu (8.8.5) id 004A21; Tue, Mar 18 1997 14:36:17 -0800 (PST)

From: rth@berdorf.edu (R.T. Hood)

To: tmh@isp.com

Date: Tue, Mar 18 1997 14:36:14 PST

Message-Id: <rth031897143614-00000298@mail.berdorf.edu>

X-Mailer: Loris v2.32

Subject: Lunch today?

Команды SMTP

HELO EHLO:<user@domain.com>

Для идентификации отправителя.

MAIL FROM:<user@domain.com>

Для инициирования почтовой транзакции.

RCPT TO:<user@domain.com>

Для идентификации отдельного получателя почтовых данных.

DATA

Для текста сообщения

QUIT, VRFY, EXPN, NOOP, HELP, REST

220 mailhost.isp.com ESMTP Sendmail 8.8.5/1.4/8.7.2/1.13
HELO mail.berdorf.edu
250 Hello mail.berdorf.edu [124.211.3.78]
MAIL FROM: rth@berdorf.edu
250 rth@berdorf.edu... Sender ok
RCPT TO: tmh@isp.com
250 tmh@isp.com... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
From: rth@berdorf.edu (R.T. Hood)
To: tmh@isp.com
Subject: Lunch today?

Do you have time to meet for lunch?

Тело письма

.
250 LAA20869 Message accepted for delivery
QUIT
221 mailhost. isp.com closing connection

Пример заголовков письма

Date: 27 Aug 76 0932

From: ivan@inm.ras.ru Mon Mar 25 13:05:04 2013

Subject: Re: The Syntax in the RFC

Sender: dima@inm.ras.ru

Reply-To: sam@mail.ru

To: George Jones <jones@mail.ru>

In-Reply-To: <1364201865.490976316@f306.mail.ru>

Message-ID: <web-6606485@inm.ras.ru>

Received: from [83.149.206.147] (port=57170 helo=inm.ras.ru)
by mx20.mail.ru with esmtp (envelope-from <ivan@inm.ras.ru>)
id 1UK3Ky-0004Qb-FB
for jones@mail.ru; Mon, 25 Mar 2013 13:05:04 +0400

Пример заголовков письма

Received: from smtp32.i.mail.ru (smtp32.i.mail.ru. [94.100.177.92])

by mx.google.com with ESMTPS id c3si6598339lbh.151.2013.03.26.08.32.33

(version=TLSv1 cipher=RC4-SHA bits=128/128);

Tue, 26 Mar 2013 08:32:34 -0700 (PDT)

Received: from mail by f48.mail.ru with local (envelope-from <solodushkin_s@mail.ru>)

id 1UKTw0-0005Oq-2z

for solodushkin_s@mail.ru; Tue, 26 Mar 2013 17:29:12 +0400

Extended SMTP

Механизм расширений протокола SMTP

S: 220 smtp.example.com ESMTP Postfix

C: **EHLO** bob.example.org

S: 250 smtp.example.com Hello bob.example.org [192.0.2.201]

S: 250 8BITMIME

S: 250 SIZE 14680064

S: 250 AUTH LOGIN PLAIN CRAM-MD5 DIGEST-MD5

S: 250 STARTTLS

S: 250 PIPELINING

S: 250 HELP

S: 250 ETRN

S: 250 CHECKPOINT

The ESMTP format was restated in RFC 2821 (superseding RFC 821) and updated to the latest definition in RFC 5321

AUTH – аутентификация и шифрование

S: 220 smtp.server.com Simple Mail Transfer Service Ready

C: EHLO client.example.com

S: 250-smtp.server.com Hello client.example.com

S: 250 AUTH LOGIN PLAIN CRAM-MD5

C: AUTH LOGIN

S: 334 VXNlcm5hbWU6	Base64(Username:)
C: dm92YQ==	Base64(vova)
S: 334 UGFzc3dvcmQ6	Base64(Password:)
C: c2VjcmV0X3Bzd2Q=	Base64(secret_pswd)

S: 235 2.7.0 Authentication successful

AUTH – аутентификация и шифрование

S: 220 smtp.server.com Simple Mail Transfer Service Ready

C: EHLO client.example.com

S: 250-smtp.server.com Hello client.example.com

S: 250 AUTH LOGIN PLAIN CRAM-MD5

C: AUTH CRAM-MD5

S: 334 PDQxOTI5NDIzNDEuMTI4Mjg0NzJAc291cmNlZm91ci5hbmRyZXcuY211LmVkdT4=

C: cmpzMyBlYzNhNTlmZWQzOTVhYmExZWM2MzY3YzRmNGI0MWFjMA==

S: 235 2.7.0 Authentication successful

STARTTLS (Start Transport Layer Security)

C: EHLO client.example.com
S: 250-smtp.server.com Hello client.example.com
S: 250-AUTH LOGIN PLAIN CRAM-MD5
S: 250-STARTTLS
C: STARTTLS
S: 220 TLS go ahead
C: <starts TLS negotiation>

C & S: <negotiate a TLS session and check result of negotiation>

C: EHLO client.example.com *
S: 250-smtp.server.com Hello client.example.com
S: 250-AUTH LOGIN PLAIN CRAM-MD5
C: AUTH LOGIN
S: 334 VXNlcm5hbWU6

C: dm92YQ==

S: 334 UGFzc3dvcmQ6

C: c2VjcmV0X3Bzd2Q= S: 235 2.7.0 Authentication successful

Multipurpose Internet Mail Extension

MIME – стандарт, описывающий передачу различных типов данных по электронной почте.

Спецификация для кодирования информации и форматирования сообщений для передачи разного рода информации внутри текстовых данных.

Определяет набор e-mail-заголовков для определения дополнительных атрибутов сообщения.

Определяет множество кодировок, которые могут быть использованы для представления 8-битных бинарных данных с помощью символов из 7-битного ASCII.

Примеры заголовков MIME

Mime-Version – версия MIME.

```
Mime-Version: 1.0
MIME-Version: 1.0 (Generated by GBD 3.7)
```

Content-Type – тип сообщения.

```
Content-Type: text/plain; charset=KOI-8
application: octet-stream
```

Content-Transfer-Encoding – тип транспортного кодирования

```
Content-Transfer-Encoding: base64
```

Заголовок multipart

Содержимое письма состоит из некоторого множества частей, содержащих данные различных взаимонезависимых типов.

mixed	основной подтип;
alternative	представление одних и тех же данных в разных форматах;
parallel	одновременный просмотр разных частей документа;
digest	объединение в одном письме частей, каждая из которых имеет тип message.

Пример multipart/alternative

Content-Type: multipart/alternative; boundary=boundary42

--boundary42
Content-Type: text/plain; charset=us-ascii

... Здесь содержится версия простым текстом ....
--boundary42
Content-Type: text/richtext

.... Здесь содержится версия с разметкой RFC 1341 ...
--boundary42
Content-Type: text/x-whatever

.... Здесь содержится версия в гипотетическом формате ...
--boundary42--

Base64

Схема преобразования произвольной последовательности байт в последовательность печатных ASCII символов.

символы (A—Z, a—z),

цифры (0—9),

символы «+» и «/»,

с символ «=» в качестве специального кода суффикса.

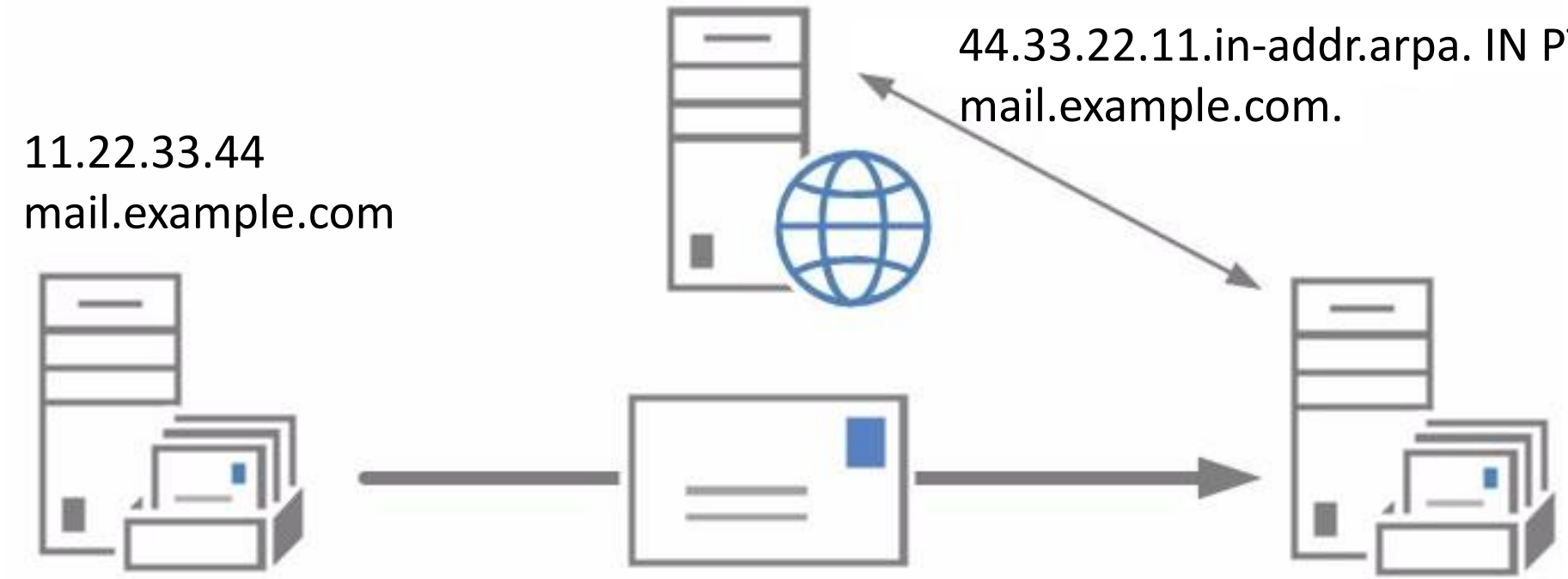
Hello, World

SGVsbG8sIFdvcmxk

Настройка зоны DNS: PTR запись

44.33.22.11.in-addr.arpa. IN PTR mail.example.com.

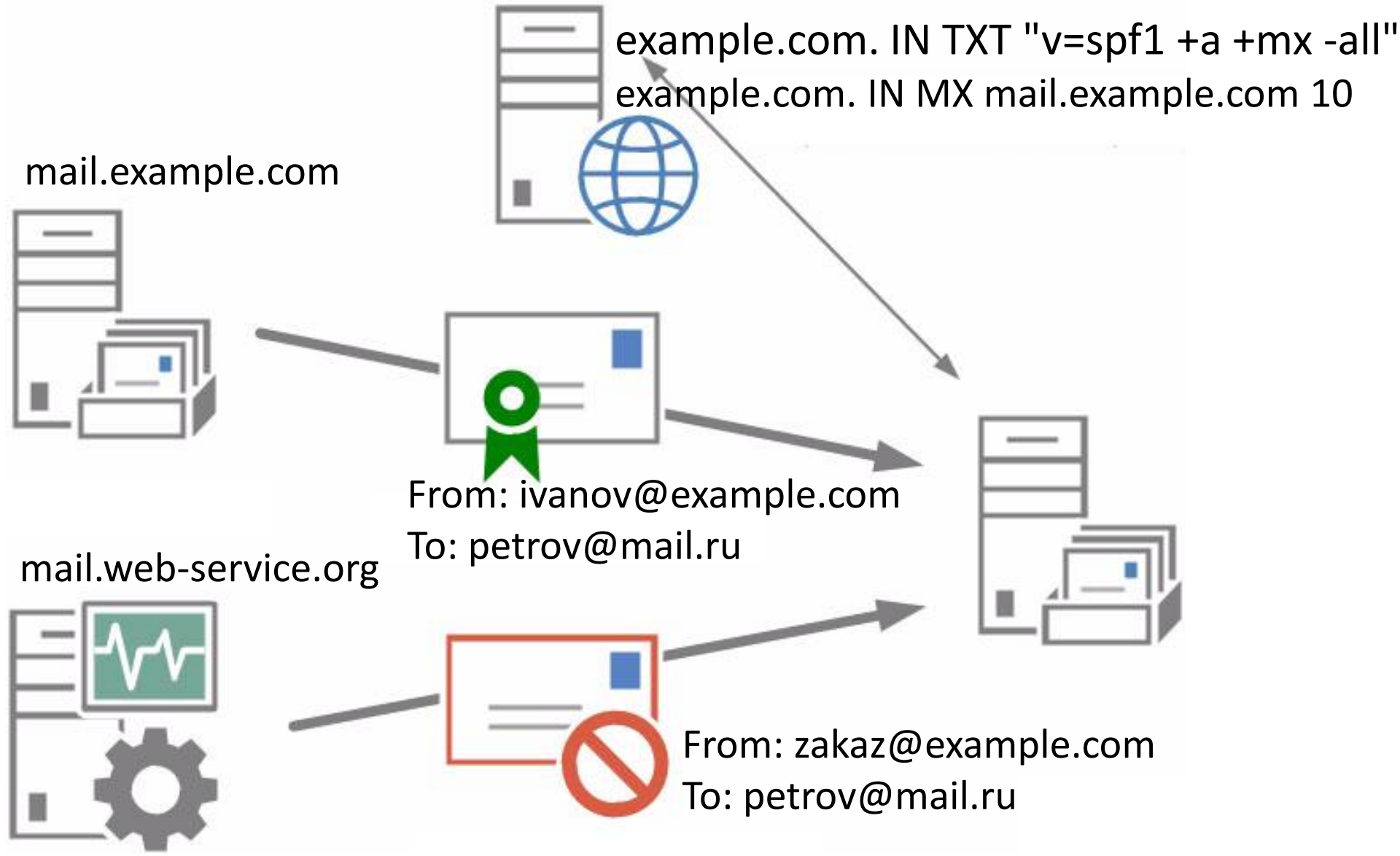
Mail сервер для двух доменов: PTR запись



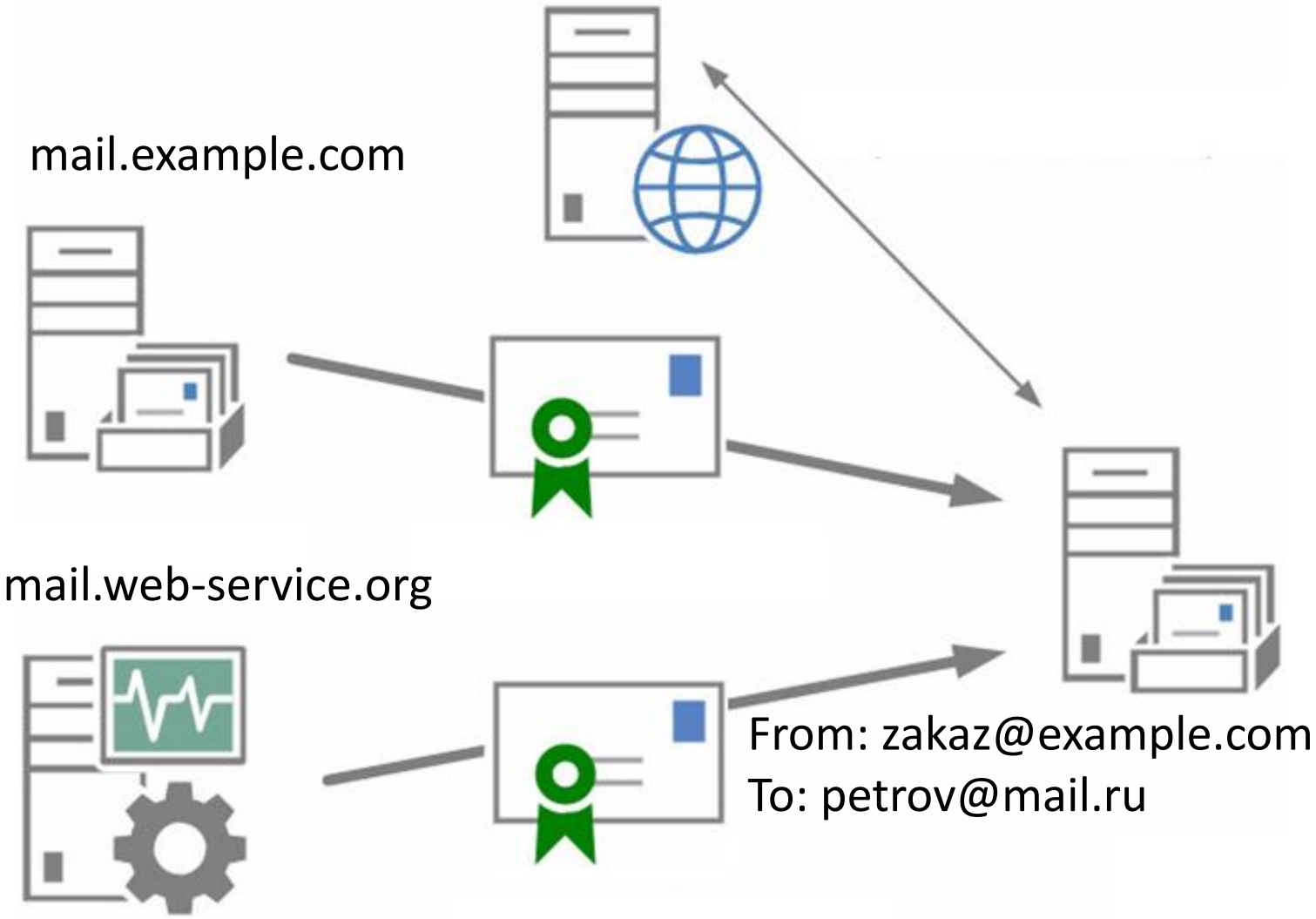
44.33.22.11.in-addr.arpa. IN PTR mail.example.com.

В этом случае PTR-запись должна указывать на имя почтового хоста (которое он передает в рамках SMTP-сессии), даже если он расположен в другом домене.

Настройка зоны DNS: SPF



Настройка зоны DNS: SPF



example.org. IN TXT "v=spf1 +a +mx +mx:web-service.com -all"

example.org. IN TXT "v=spf1 +a +mx +a:mail.web-service.com -all"

DomainKeys Identified Mail

```
DKIM-Signature: v=1; a=rsa-sha256; d=example.net;
s=brisbane;   c=relaxed/simple; q=dns/txt; l=1234;
t=1117574938; x=1118006938;
h=from:to:subject:date:keywords:keywords;


bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;


b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVoG4
ZHRNiYzR
```