GWAVACon

Aaack! They Won’t Accept My Email!

Messaging Security • Unified Archiving • Business Continuity

Version 4 - 9/

www.GWAVACon.com

K I S

Allan Hurst
Partner & Director of Enterprise Strategy
allanh@kiscc.com

Version 5.1 - 2012-01-23

Housekeeping

Cell phones, pagers, Treos, Blackberries, etc., set them all to stun, please. **No noise is good noise**.

If you have a question, **it’s absolutely OK to ask**. It’ll help if you raise your hand first to get my attention. I’ll try to answer on the fly.

It’s OK to **have fun** in here. Honest.

Who is This Guy, Anyway?

Allan Hurst

Works for KIS ("Keep IT Simple")

Partner and Director of Enterprise Strategy

Master CNE^{SM} working with Novell® products since 1988 (2.0a)

One of four partners at KIS, a Novell Platinum Partner and Novell Gold Training Partner in Fremont, CA, Kansas City, MO, Cleveland, Denver, and New Jersey.

Runs the Enterprise Strategy Practice (network planning, migrations, upgrades, moves, re-architecting, and clean-up)

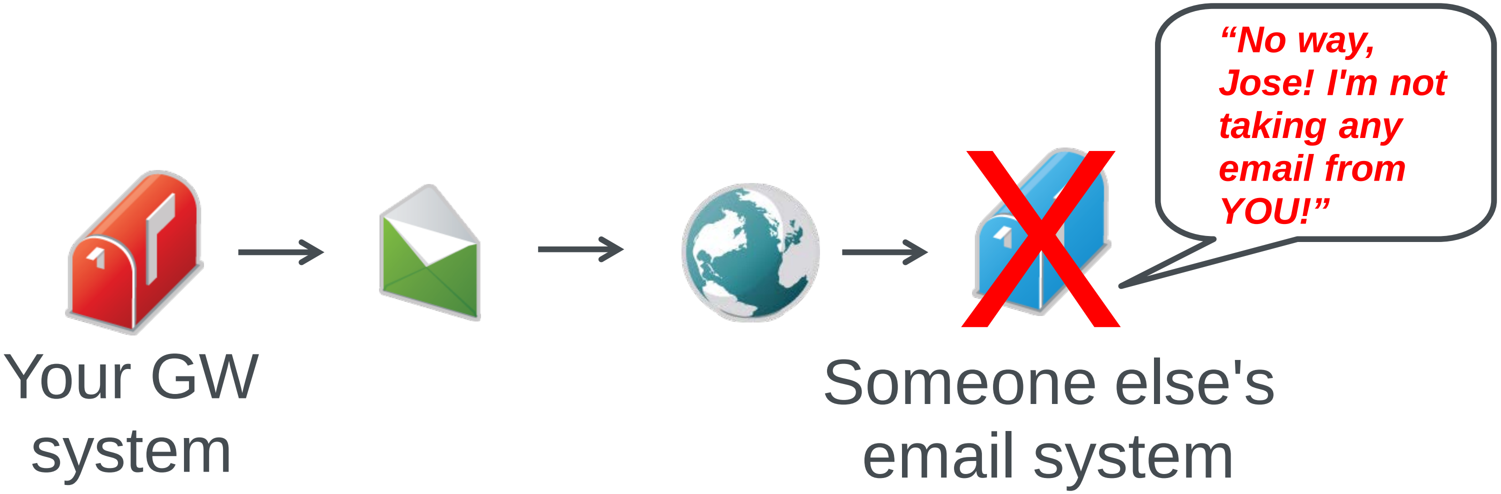
Also runs "The WAP Squad." ("WAP" stands for …)

Who Are You?

Novell® GroupWise® administrator and/or network manager

Some of your end users' correspondents aren't able to send or receive mail to or from your system.

You desperately want to stop your end users from complaining (and chloroform is *not* a good long-term solution).


"No way, Jose! I'm not taking any email from YOU!"
Your GW system
Someone else's email system

Where Did This Session Come From?

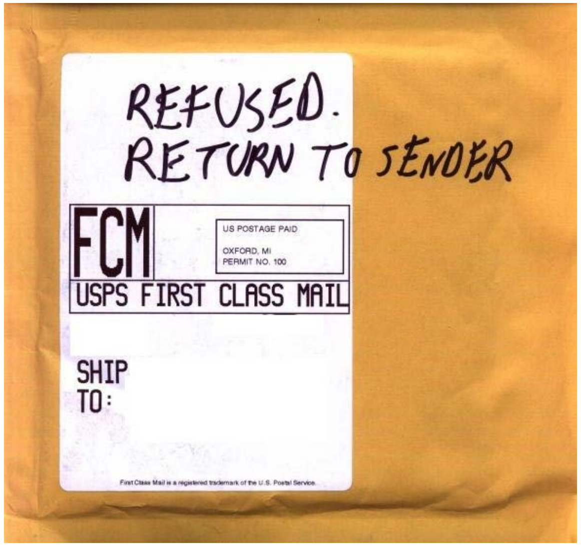
This session is actually yet another follow-up to my session “Demystifying DNS”.

Every year the session was presented, people kept asking more and more questions about how to solve bouncing email problems.

About This Session

- Top 10 Reasons For Having Your Email Refused
- Downright Sneaky Stuff
- Issues I've Not Run Into Yet
- Best Practices
- Question and Answer

Top 10 Reasons For Having Your Email Refused



10. People Think You're A Spammer

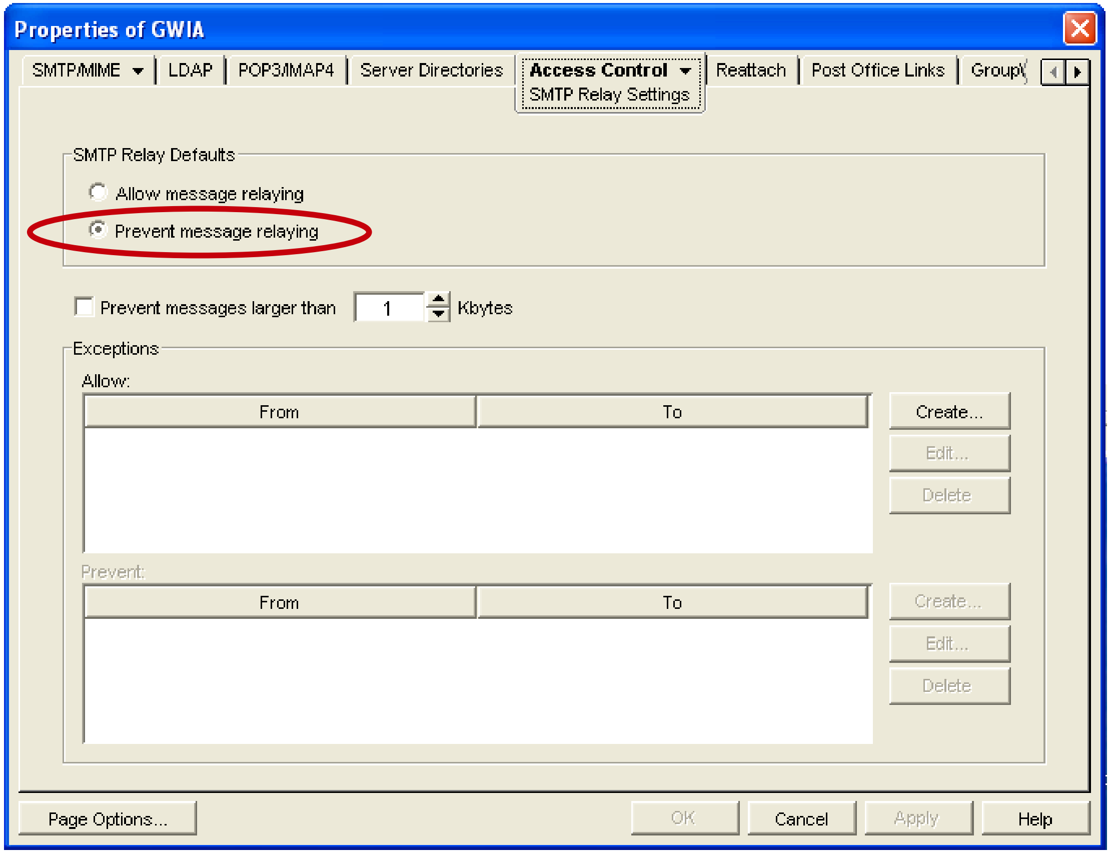
You're blacklisted as a spammer or relay point on one or more Realtime Blackhole Lists (RBLs) because *someone* thinks you have an open relay.

Note: There are many blacklists. Not everyone uses the same set.

See “comparison of dns blacklists" on Wikipedia for a pretty good starting list.

Fixing Open Relay in ConsoleOne

GWIA Object / Access Control / SMTP Relay Settings



SMTP Relay Defaults

○ Allow message relaying

● Prevent message relaying

□ Prevent messages larger than 1 Kbytes

Exceptions

Allow:

From	To

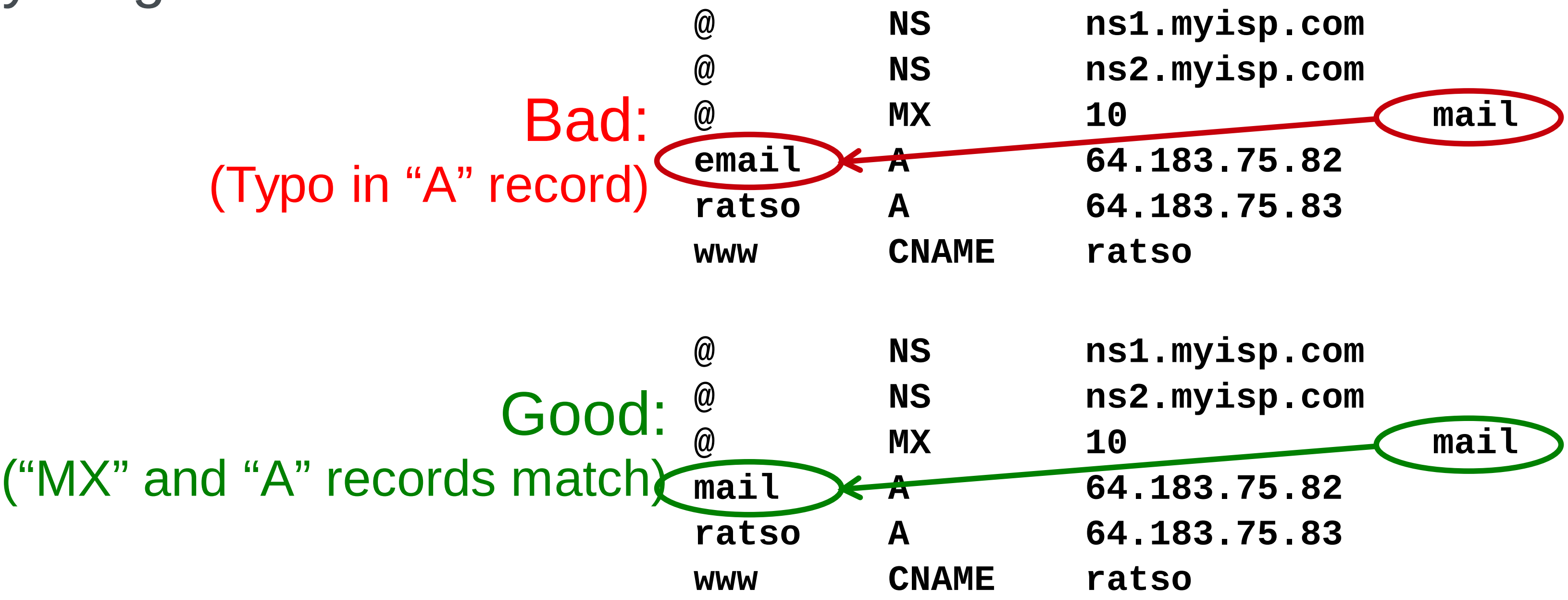
Prevent:

From	To

9. Bad Exernal DNS Records

You don't have valid "A", "MX", and "IN-ADDR-ARPA" records in your *external* DNS for your mail server.

You need *all three* types of records, because many anti-spam systems do a forward/reverse cross-check to see if everything matches.



Bad:

(Typo in “A” record)

```
@         NS       ns1.myisp.com
@         NS       ns2.myisp.com
@         MX       10              mail
email     A        64.183.75.82
ratso     A        64.183.75.83
www       CNAME    ratso
```

Good:

(“MX” and “A” records match)

```
@         NS       ns1.myisp.com
@         NS       ns2.myisp.com
@         MX       10              mail
mail      A        64.183.75.82
ratso     A        64.183.75.83
www       CNAME    ratso
```

8. You're Sending a Virus

It's not unusual to find a site that scans all *incoming* email for viruses, but not *outgoing* email.

With so many nasty viruses (“virii”?) going around, it's possible that an attached file may contain a virus.

Keep in mind that even some *clean* files that are executable may cause a denial of delivery, depending upon how the destination email system's antivirus/ antispam system is configured.

Clean Up Your Act!

Ensure that both inbound and outbound email is scanned for viruses.

If email is denied because of an executable attachment, try renaming the file (this doesn't always work with antivirus products using “file fingerprinting” technology) or putting it into a zipped file.

Last ditch effort: Give up and send the attachment via a third party file transfer service such as http://www.wetransfer.com (or wait for Novell Filr).

7. You Have No SPF Record

While I personally think Sender Protection Framework (SPF) is worthless because it was hacked within *hours* of its initial release, many antispam systems are set up to check for an SPF record.

This means you need to create a SPF record for your system.

The original SPF Wizard at http://www.openspf.org has been retired, but there are similar tools located at:

http://spfwizard.com/

http://www.mtgsy.net/dns/spfwizard.php

http://www.mailradar.com/spf/

```
@               MX     10             mail
mail            A      64.183.75.82
ratso           A      64.183.75.83
www             CNAME  ratso
mail.fubar.com  TXT    "v=spf1 mx ptr ip4:68.178.232.100 mx:mail.fubar.com -all"
```

6. Bad *Reverse* DNS Records

You don't have a reverse DNS (in-addr-arpa) record defined for your mail server.

Bad:

```
@        NS       ns1.myisp.com
@        NS       ns2.myisp.com
@        MX       10              mail
mail     A        64.183.75.82
ratso    A        64.183.75.83
www      CNAME    ratso
```

Good:

```
@        NS       ns1.myisp.com
@        NS       ns2.myisp.com
@        MX       10              mail
mail     A        64.183.75.82
ratso    A        64.183.75.83
www      CNAME    ratso
82.75.183.65.in-addr.arpa PTR 64-183-75-82.myisp.com.
```

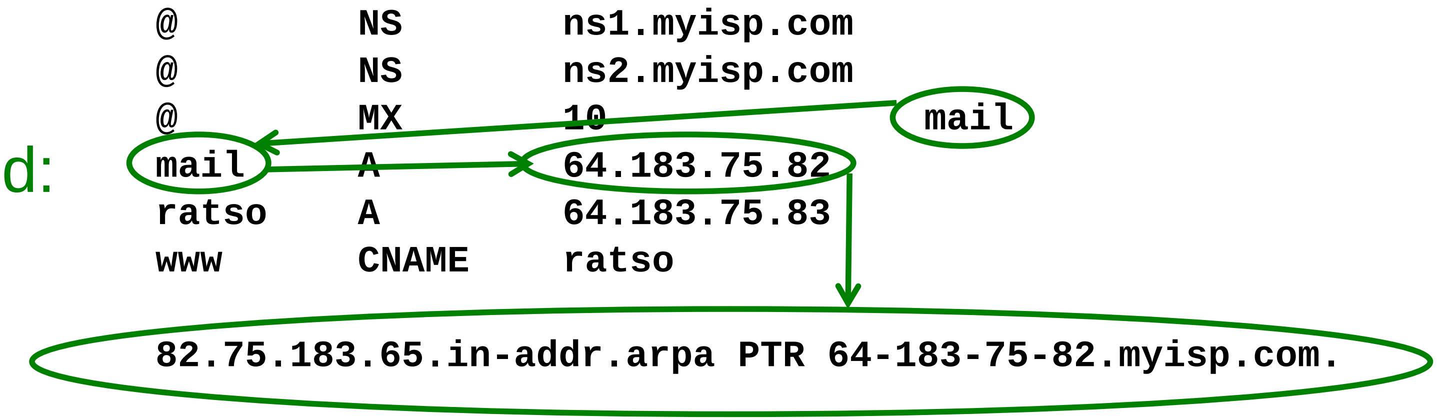
6. Bad *Reverse* DNS Records

You don't have a reverse DNS (in-addr-arpa) record defined for your mail server.

Bad:

```
@         NS        ns1.myisp.com
@         NS        ns2.myisp.com
@         MX        10                mail
mail      A         64.183.75.82
ratso     A         64.183.75.83
www       CNAME     ratso
```

Good:



```
@         NS        ns1.myisp.com
@         NS        ns2.myisp.com
@         MX        10                mail
mail      A         64.183.75.82
ratso     A         64.183.75.83
www       CNAME     ratso
82.75.183.65.in-addr.arpa PTR 64-183-75-82.myisp.com.
```

5. Your GWIA Isn't Up

Laugh if you want, but if your GWIA is down, nothing's going out...and chances are that GWIA will go down late at night *just* as your CEO attempts to send email to an old school chum.

4. Your GWIA Has Weird Timeouts

Your GWIA has a weird configuration or too-short timeouts.

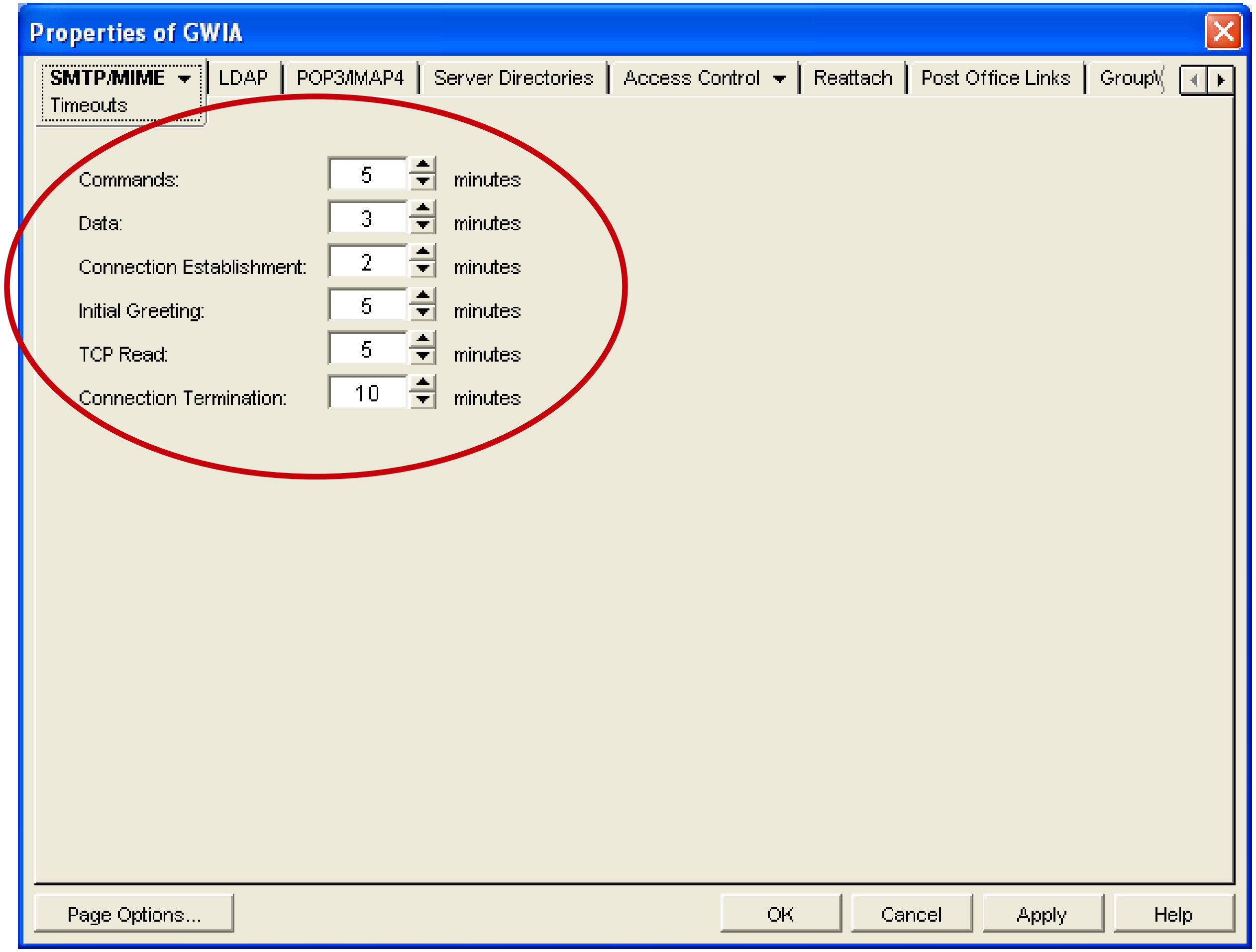
People *love* messing with GWIA timeouts, even if nothing's wrong. This *especially* applies to your predecessor.

If in doubt, *increase* GWIA SMTP timeouts *slightly*.

Food for thought: I’ve *never* needed to change the installation default timeouts. (I have, however, needed to *restore* the installation default timeouts.)

Changing Timeouts in ConsoleOne

GWIA Object - **SMTP/MIME** - Timeouts



Commands: 5 minutes

Data: 3 minutes

Connection Establishment: 2 minutes

Initial Greeting: 5 minutes

TCP Read: 5 minutes

Connection Termination: 10 minutes

3. Your GWIA Has An Identity Crisis

Whether you use GWIA or an antispam appliance to send and receive email, it needs to answer up *exactly* the same as your MX record.

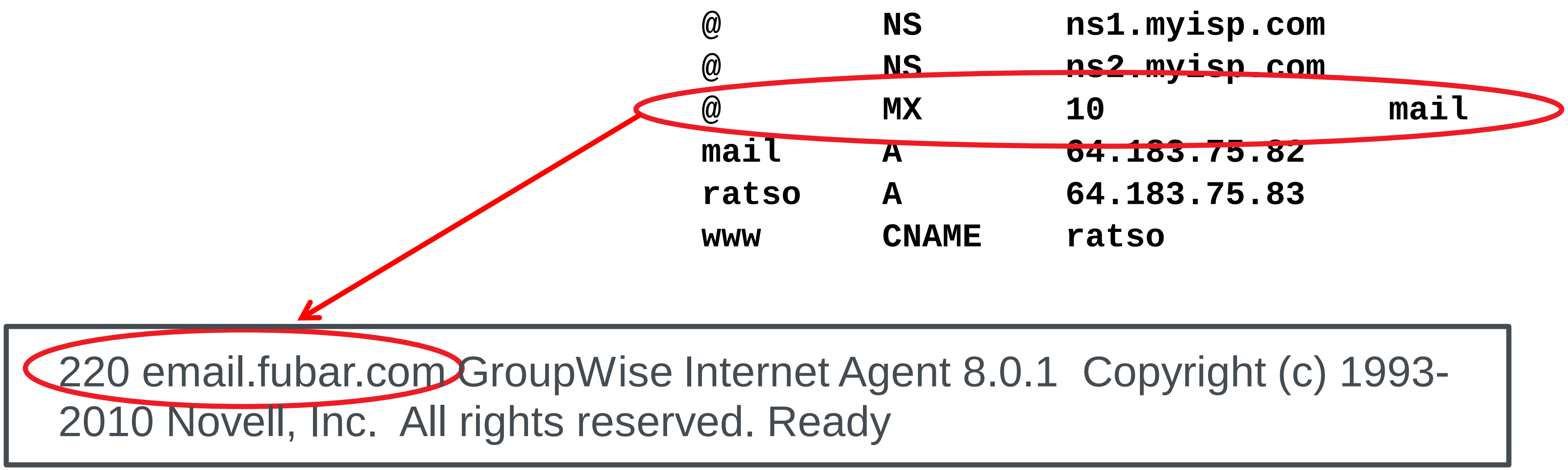
```
@         NS        ns1.myisp.com
@         NS        ns2.myisp.com
@         MX        10                mail
mail      A         64.183.75.82
ratso     A         64.183.75.83
www       CNAME     ratso
```

```
220 email.fubar.com GroupWise Internet Agent 8.0.1  Copyright (c) 1993-
2010 Novell, Inc.  All rights reserved. Ready
```

What's wrong with this picture?

3. Your GWIA Has An Identity Crisis

Whether you use GWIA or an antispam appliance to send and receive email, it needs to answer up *exactly* the same as your MX record.



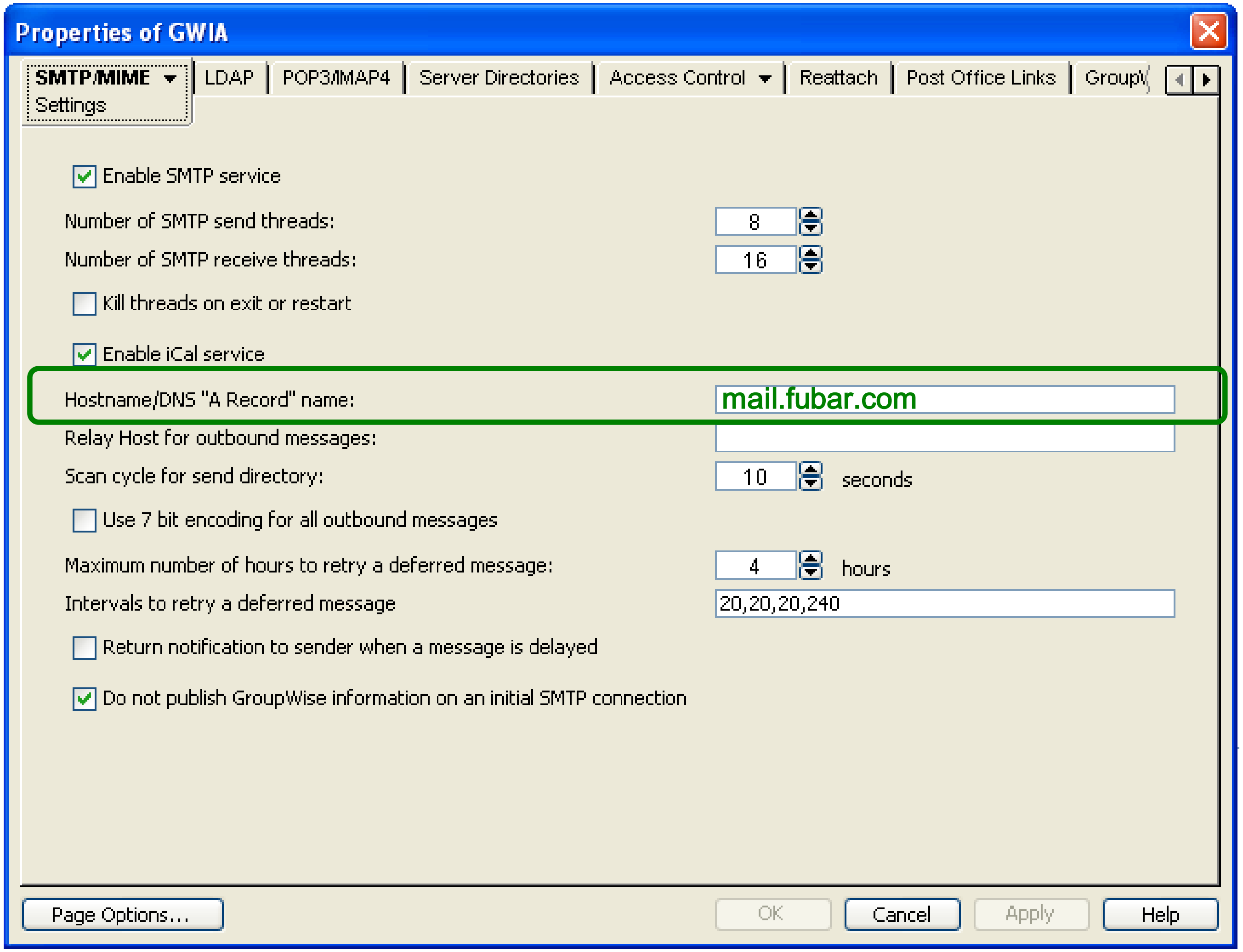
```
@        NS       ns1.myisp.com
@        NS       ns2.myisp.com
@        MX       10                mail
mail     A        64.183.75.82
ratso    A        64.183.75.83
www      CNAME    ratso
```

```
220 email.fubar.com GroupWise Internet Agent 8.0.1  Copyright (c) 1993-
2010 Novell, Inc.  All rights reserved. Ready
```

Bad GWIA; No Email! This GWIA answers up as “email.fubar.com”, when the external DNS “MX” record says it should be answering up as “mail.fubar.com”

Fixing GWIA's Identity Crisis

This must match your external DNS "MX" record.



☑ Enable SMTP service

Number of SMTP send threads: 8

Number of SMTP receive threads: 16

□ Kill threads on exit or restart

☑ Enable iCal service

Hostname/DNS "A Record" name: mail.fubar.com

Relay Host for outbound messages:

Scan cycle for send directory: 10 seconds

□ Use 7 bit encoding for all outbound messages

Maximum number of hours to retry a deferred message: 4 hours

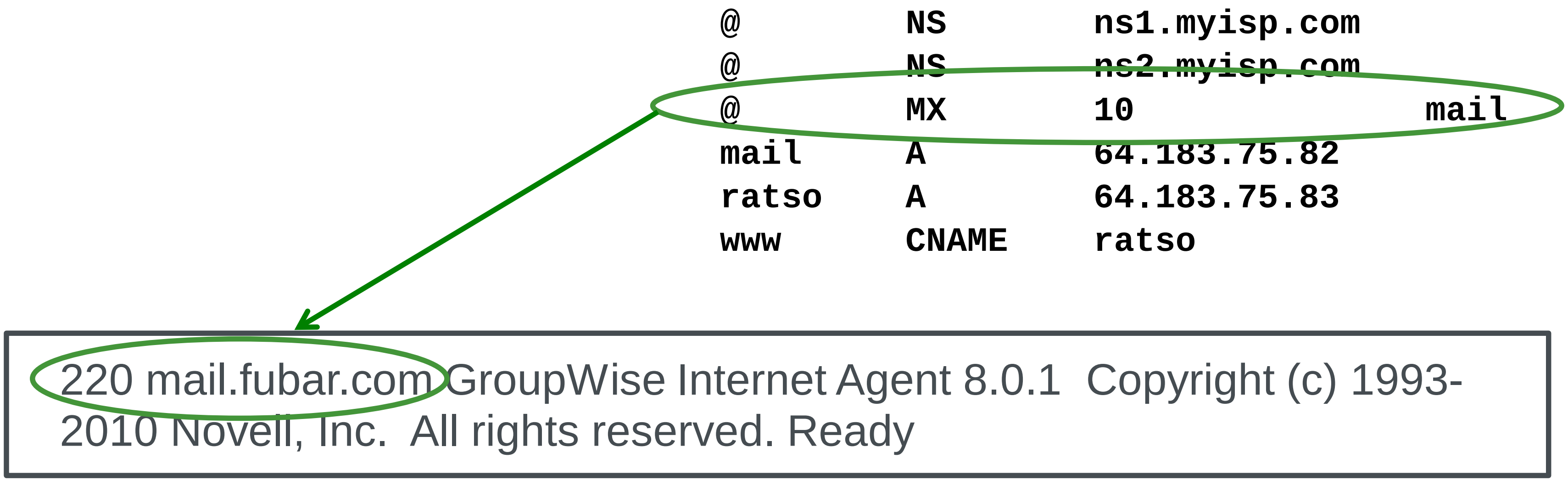
Intervals to retry a deferred message 20,20,20,240

□ Return notification to sender when a message is delayed

☑ Do not publish GroupWise information on an initial SMTP connection

Fixing GWIA's Identity Crisis

Here's how this configuration *should* look:



```
@         NS      ns1.myisp.com
@         NS      ns2.myisp.com
@         MX      10              mail
mail      A       64.183.75.82
ratso     A       64.183.75.83
www       CNAME   ratso
```

```
220 mail.fubar.com GroupWise Internet Agent 8.0.1  Copyright (c) 1993-
2010 Novell, Inc.  All rights reserved. Ready
```

Good GWIA; We Have Email! This GWIA answers up correctly, matching the external DNS “MX” record of “mail.fubar.com”.

2. End User Mistypes Email Address

Laugh if you want, but a large number of email problems we're called on to troubleshoot involve end users who just aren't spelling their intended recipient's email address correctly.

This is *not* something we can fix.

(Unless you know of a way that we don’t to get all new end users.)

1. Something Sneaky Is Going On

We couldn't fit everything into just 10 items, so we're lumping together all of the *non*-obvious problems we run into on a frequent basis.

Downright *Sneaky* Stuff

You've Been Blacklisted By Mistake!

It's not uncommon for an end user to mistakenly mark incoming mail as spam, *especially* on systems such as AOL or Comcast.

When that happens, all you can do is jump through the necessary hoops that the destination ISP requires:

AOL:
http://postmaster.aol.com/

Comcast:
http://www.comcastsupport.com/sdcxuser/asp/comcast_blockedprovider.asp

Others:
http://www.rackaid.com/resources/spam-blacklist-removal/
(Covers AT&T, Earthlink, Gmail, Godaddy, Hotmail and Yahoo.)

Non-GW Issues: RFC Compliance

These haven't been problems for us with GWIA, but if you're using an anti spam appliance or service...be aware!

Your server won't accept mail from "<>"

You are *required* by RFC 1123 section 5.2.9 to receive mail with a blank reverse path. This typically includes reject/bounce messages and return receipts.

Your server won't accept domain literal format

“Domain literal format” means an email address in the form of ***user@[0.0.0.0]***. Technically speaking, mail servers are required by RFC1123 section 5.2.17 to accept mail to domain literals for any of its IP addresses.

“Dummy” Accounts.

Yes, it's very, very picky of *some* people, but some mail systems get ticked off if they can't send email to one of these accounts:

postmaster@_________

abuse@_____________

Point both of these to your admin mailbox, or to some other mailbox that you check daily.

Issues I've Not Run Into Yet

Other Validation Technologies

I haven't run into or used these, so I'm not qualified to talk about them. However, in the event that you run into them, here are some resources:

DKIM (DomainKeys Identified Mail)

http://www.dkim.org/

ADSP (Author Domain Signing Practices)

http://tools.ietf.org/html/rfc5617

SMIME (Secure MIME)

(Note: GroupWise® 8 handles SMIME in the Windows client *only*. See the GW8 documentation for details.

Best Practices

BP #1: Install A Front-End System

It's not reasonable to expect Novell® to continually upgrade GroupWise® to fight spam and viruses all on its own.

Place your GWIA behind a software scanner*, front-end appliance or cloud-based service which scans for spam and viruses.

If using a cloud-based service, make sure that your firewall is set to only allow traffic from the cloud-based service to hit your GWIA's IP address.

*Gee, *who* at GWAVAcon could you talk to about an email scanner...?

BP #2: Redirect Incoming Mail

To avoid loss of email service during the transition to a front-end appliance (or cloud-based service provider):

1. Add an MX record (with a *lower* number than your existing GWIA's MX record) to direct all incoming mail to that system.

2. Let that sync up for a day or so. (I like doing this on a Friday morning or afternoon.)

3. Once you see mail starting to come into the new MX record, *then* remove your old MX record(s) pointing to GWIA.

BP #3: Revamp External DNS

Don't forget to change your external “A”, “MX”, and reverse DNS (“IN-ADDR-ARPA”) records to point to the new front-end system.

BP #4: Create an SPF Record

As we said earlier...even if you don't believe in SPF, create an SPF record for your system anyway.

(It might not help, but it certainly won't hurt.)

BP #5: What If It Goes Down?

Decide what you want to do if your primary front-end mail system goes down. *Have a written plan, even if it's only one page long!*

We strongly recommend that you *not* pass through mail directly to GWIA by using a secondary MX record. (Spammers will often start hacking away at secondary MX records before primary MX records.)

So what *should* you do? Keep reading...

BP #6: Protect Your Front End!

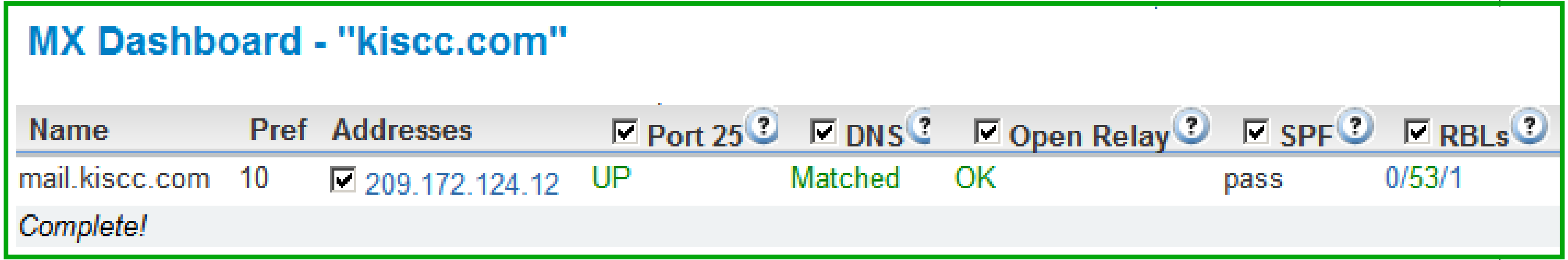
Here are some options to consider:

1. Don't create a secondary MX record. *If email's down, then it's down.*
2. If using an appliance, buy a pair and configure them for fault-tolerance/failover mode. In some cases you won't need a secondary MX record, in other cases you will. This is vendor-dependent.
3. If using a cloud-based front end, make sure that they'll “spool” incoming email in case your GWIA goes down.

BP #7: Test Your Email!

There are a number of email testing services that will whack your email servers upside the head to see what happens.

I happen to use a service from http://www.dnsstuff.com, but there are many others, such as http://www.mxtoolbox.com



MX Dashboard - "kiscc.com"

Name	Pref	Addresses	☑ Port 25	☑ DNS	☑ Open Relay	☑ SPF	☑ RBLs
mail.kiscc.com	10	☑ 209.172.124.12	UP	Matched	OK	pass	0/53/1

Complete!

GWAVA

BP #7: Test Your Email! (Part 2)

telnet IP-address-or-DNS-name-of-the-smtp-gateway 25

If you can’t see what you’re typing on the screen, enable echo in Terminal, Preferences.

Each correct command should be answered with a "220" or "250 Ok" statement.

```
220 mail.fubar.com Brand-X SMTP Gateway Ready
helo company.com [enter]
250 mail.fubar.com Hello company.com [11.138.75.25], pleased to meet you
mail from:john_doe@company.com [enter]
250 Sender <john_doe@company.com> OK
rcpt to:user@company.com  [enter]
250 Sender <john_doe@company.com> OK
rcpt to:joeuser@fubar.com
250 Recipient <allanh@kiscc.com> OK
data
354 Start mail input; end with <CRLF>.<CRLF>
This is a test message.
.
250 Ok: queued as 9F2D43BEA69
quit
```

BP #8: Teach Your Users To Spell

Specifically, to spell destination email addresses correctly.

Yeah, that'll happen...*not*.

Questions?

Got Reference?

If you would like an updated copy of this presentation, please pass me your business card. You will also receive copies of the presentations:

- **Demystifying DNS**
- **More Demystifying DNS**
- **SLP Made Easy**
- **Migrations Without Tears**
- **Avoiding Lumps & Bumps In Virtualization**

(Also pass your card in if you want to be in the drawing for a USB stick!)

Thank You!

Allan Hurst
Director of Enterprise Strategy
510.933.7555
allanh@kiscc.com
http://www.kiscc.com