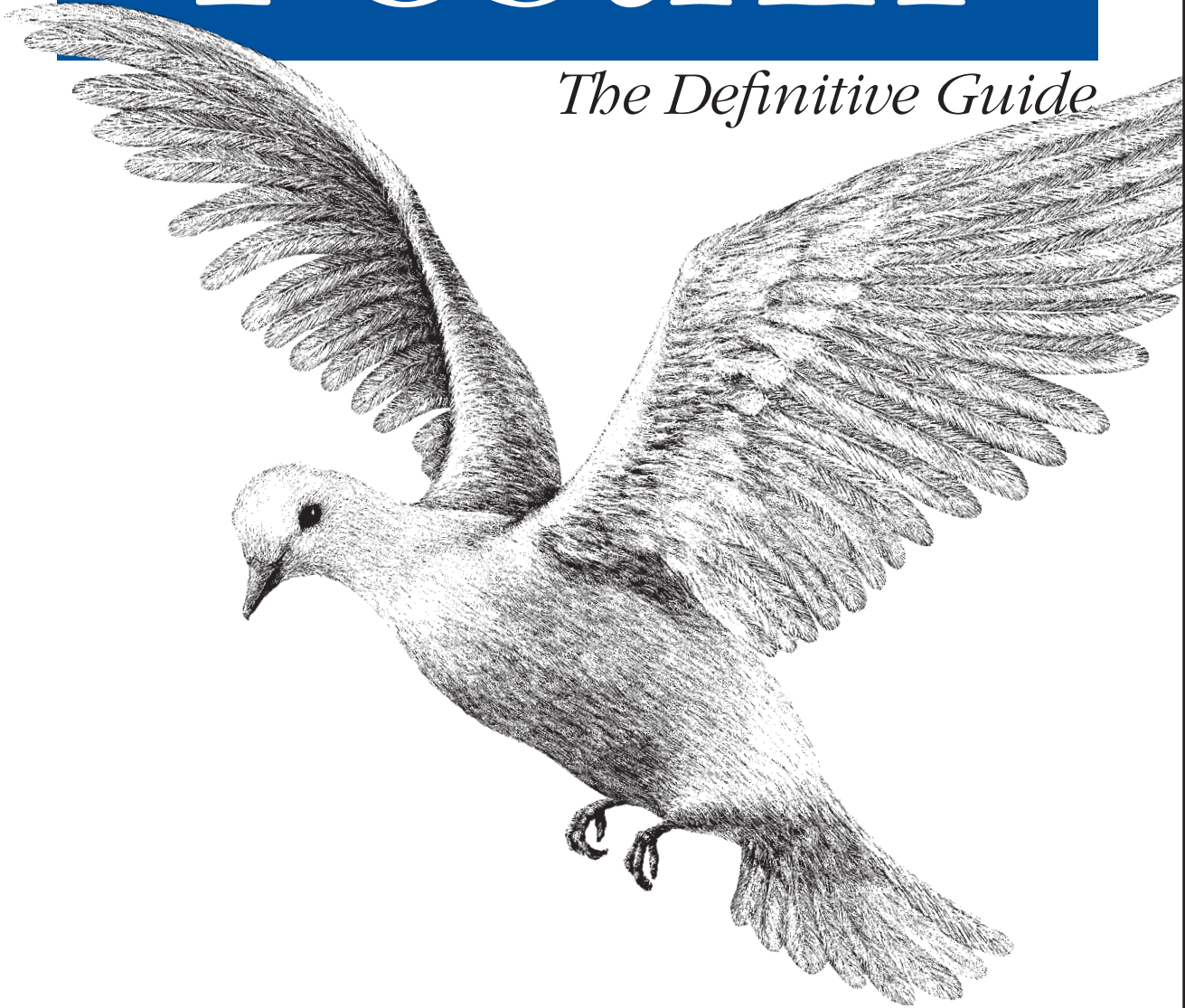


A Secure and Easy-to-Use MTA for Unix

Postfix

The Definitive Guide



O'REILLY®

Kyle D. Dent
Foreword by Wietse Venema

Mail Relaying

Up until now, we've mostly considered Postfix in its role as the end node for email messages. That is, messages that arrive at the Postfix system are, for the most part, delivered to the local system. But it's also common to find Postfix serving as an intermediate node on the path a message follows to its ultimate destination. In this chapter we'll look at some of the configuration options for Postfix as a client in MTA-to-MTA communications.

Backup MX

In DNS, MX records refer to *mail exchangers* (see Chapter 6). MX records contain both host and priority (or preference) information for sending mail to a domain. A backup MX server is one that receives mail for a particular domain, but is not the preferred server to receive the mail. If the preferred server or servers are down, the backup MX server receives the mail and queues it until one of the more preferred servers comes back online. Figure 9-1 illustrates delivery to a backup host when the primary host is not available. The backup queues messages until the primary is back online, whereupon the backup can deliver messages to it.

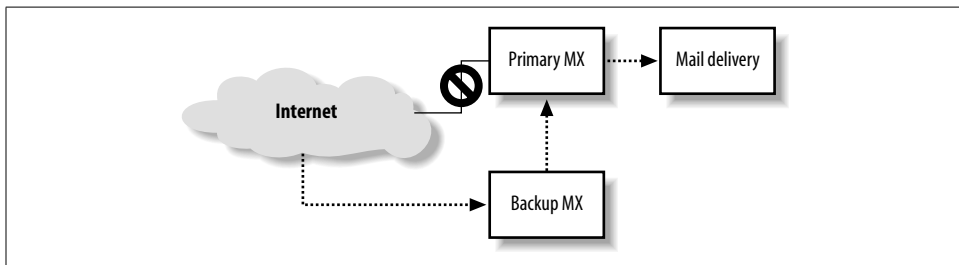


Figure 9-1. Delivery to backup MX host

When your system is configured in DNS as a backup MX host, you don't have to configure any special transport from your system to the primary system. Postfix uses the DNS records to determine how to route mail to the primary MX host. The only

configuration required in Postfix is to indicate that it should receive mail for the domain by adding the domain name to the `relay_domains` parameter. When a sending MTA discovers that the primary mail system for a domain is down, it tries the next preferred one until it finds one that accepts delivery. If your system is a backup MX host, and the destination domain is listed in your `relay_domains` parameter, Postfix accepts the mail and queues it. Postfix periodically scans its queue and checks for a more preferred system to see if any are able to accept the message. Once a higher priority mail exchanger is back online, Postfix can deliver the message to it.

Postfix continues trying to deliver queued messages for the amount of time specified in the `maximal_queue_lifetime` parameter, which determines how long deferred messages stay in the queue before they are bounced back to the sender. The default value is five days. If you provide secondary mail service for primary servers that you know will be down longer than the default, you can extend the time.

Relay Recipients

It is highly recommended that you maintain a list of valid recipients for domains you provide backup MX services to. You should develop a regular process for obtaining an updated user list from your primary MX servers. If your system does not know all of the available mailboxes on the primary mail server, it must accept all messages. It's only when your backup MX server tries to deliver them to the primary server that it discovers that a message cannot be delivered. At that point, your server must bounce the message back to the original sender.

Since spammers often send messages to made-up addresses, if your server does not know all the valid email addresses on the primary server, your server will unnecessarily accept a lot of mail that must be bounced. The bounce problem is exacerbated by the spammer tactic of forging sender addresses by using the real email addresses of innocent bystanders. The forged addresses receive all of the error notices for messages they never sent (see Chapter 11). The `relay_recipient_maps` parameter specifies lookup tables that should contain all of the addresses for domains listed in your `relay_domains` parameter:

```
relay_recipient_maps = hash:/etc/postfix/relay_recipients
```

The `relay_recipients` file should contain entries with the recipient address on the lefthand side. The righthand side is not used by Postfix, but you must specify a value:

```
#
# relay_recipients
#
user1@example.com      any_value
user2@example.com      any_value
user3@example.com      any_value
```

If your system is on the same network as the primary, and the user accounts are stored in some kind of database, you may be able to perform real-time lookups using MySQL or LDAP (see Chapter 15).

A potential problem is that once you set `relay_recipient_maps`, you must include email addresses for all domains you provide backup service to. If not, Postfix will reject messages that don't appear in the lookup table. If you don't know the valid addresses for some domains, you can specify a wildcard entry for that domain:

```
#
# relay_recipients
#
user1@example.com      any_value
user2@example.com      any_value
user3@example.com      any_value
@oreillynet.com        any_value
```

The final entry is a wildcard entry that allows messages for any address at the domain. Obviously, it's better to obtain the list of valid addresses for the reasons mentioned earlier.

Fast Flushing

Networks that receive mail for many sites, such as ISP networks, typically have some customers whose systems aren't always connected to the network. When the customer network is offline, the ISP queues its messages. When the site comes online, it can request immediate delivery of all its queued mail with the ETRN SMTP command:

```
220 mail.ora.com ESMTP Postfix
EHLO mail.example.com
250-auger.seaglass.com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250 8BITMIME
ETRN example.com
250 Queuing started
```

If there are a lot of messages queued when a domain is ready to accept mail, searching every queue file would be time-consuming. Postfix provides a capability called *fast flush* to speed up queue processing for a particular domain. Fast flush is handled by the `flush` daemon, which maintains lists of messages that are queued for specific domains so that Postfix knows which messages to deliver when it receives an ETRN command.

By default, all of the sites listed in `relay_domains` are eligible for the fast flush service. You can include domains in addition to your relay domains by adding them to the `fast_flush_domains` parameter. Add a domain name as follows:

```
fast_flush_domains = $relay_domains, example.com
```

In this case *example.com* is a domain not already listed in `relay_domains`.

You can manually notify Postfix that a fast flush domain is ready to accept messages by issuing the `postqueue -s` command (or its equivalent, `sendmail -qR`) with the site name:

```
$ postqueue -s example.com
```

Transport Maps

Postfix can be configured to relay to any other host, regardless of how DNS MX records are set up. This section discusses the `transport_maps` parameter in general. Later sections and other chapters in the book present specific configurations that use it.

Conceptually, transport maps override default transport types for delivery of messages. The `transport_maps` parameter points to one or more transport lookup tables. The following entry sets up `/etc/postfix/transport` as a transport map lookup table:

```
transport_maps = hash:/etc/postfix/transport
```

The keys in a transport lookup table are either complete email addresses or domains and subdomains. (Email addresses as lookup keys for transport maps require Postfix 2.0 or later.) When a destination address or domain matches a lefthand key it uses the righthand value to determine the delivery method and destination. Example 9-1 lists some possible transport map entries.

Example 9-1. Transport map entries

```
example.com      smtp:[192.168.23.56]:20025
oreilly.com      relay:[gateway.oreilly.com]
oreillynet.com   smtp
ora.com          maildrop
kdent@ora.com    error:no mail accepted for kdent
```

The format of righthand values can differ depending on the transport type, but generally has the form `transport:nexthop`, where *nexthop* often indicates a host and port for delivery. Each of the possible portions of the righthand value are described here:

transport

Refers to an entry from *master.cf*. If you are adding a new transport type, first create an entry for it in *master.cf*.

host

The destination host for delivery of messages. The host is used only with `inet` transports such as SMTP and LMTP. Postfix treats the hostname like any destination domain. It performs an MX lookup to determine where to deliver messages. If there are no MX records, Postfix delivers to the A record IP address. If you know that Postfix should deliver directly to the IP in the A record for the specified host, you can have Postfix skip the check for MX records by enclosing the name in brackets. If you use an IP address, the brackets are required.

port

The destination port for message delivery. The port is used only with `inet` transports such as SMTP and LMTP. The port can be specified using the actual number or its symbolic name from the `/etc/services` file.

Each of the sample entries from Example 9-1 uses a different format in their righthand values, which are explained below:

example.com smtp:[192.168.23.56]:20025

All messages destined for *example.com* are relayed using the `smtp` transport to the host at IP address 192.168.23.56. Messages are delivered over port 20025 instead of the default SMTP port 25. Notice that the IP address is in brackets, as required for IP addresses.

oreilly.com relay:[gateway.oreilly.com]

All messages destined for *oreilly.com* are relayed using the `relay` transport to the host *gateway.oreilly.com*. Since no port is specified, Postfix uses the default port 25. The hostname is in brackets to prevent Postfix from looking up MX records. Instead, it looks up the A record and delivers to the IP address that the hostname resolves to.

The relay transport was introduced in Version 2 of Postfix to fix a potential performance bottleneck with queue scheduling. You should direct inbound messages relayed to internal systems over the relay transport, so that they don't compete with messages destined for many different systems on the Internet.

oreillynet.com smtp

All messages destined for *oreillynet.com* are relayed using the `smtp` transport. Since both the next hop and port are left off, Postfix uses the default port 25 and determines the next hop based on the destination address. Most often, the next hop is determined by performing a DNS lookup, which determines the MX host for the domain. This example is a bit contrived, since simply listing *oreillynet.com* with `relay_hosts` achieves the same thing in this case.

ora.com maildrop

All messages destined for *ora.com* are delivered to the maildrop service. `maildrop` must be an entry in *master.cf*. Since delivery occurs over a pipe rather than an `inet` socket, no host and port are specified.

kdent@ora.com error:no mail accepted for kdent

The special `error` transport causes all mail to be rejected. After the colon, specify a message to report when email is rejected.

Transport maps can also be used for special handling of certain messages on the local system. (Chapter 14 discusses content filters, which provide a good example of configuring special local transports.) Another local use of transport maps is to temporarily defer all of a domain's messages. To demonstrate a simple use of transport maps, the next section describes a procedure to defer all of the messages for a domain.

Postponing Mail Delivery

Under some circumstances you want Postfix to postpone delivery of messages until it has received an explicit command to deliver them. Deferred messages are delivered when you issue the `postqueue -f domain` command or Postfix receives an ETRN SMTP command from a fastflush-eligible domain.

A common scenario for deferring messages is when an ISP receives mail for a customer network that is not always online. The ISP must queue messages until the network is online and can receive them. Similarly, users on the customer network should send messages through a local gateway that queues them until they can be delivered once the network is online. This section presents configurations for both situations.

Deferring mail relay

This procedure sets up a new transport type called “ondemand,” and configures a transport map to defer all messages for the *example.com* domain:

1. Create a new transport in your *master.cf* file called `ondemand`. It should be identical to your `smtp` transport except for the name:

```
ondemand    unix    -    -    n    -    -    smtp
```

2. Tell Postfix that delivery of all messages over your new transport should be deferred automatically. Edit the `defer_transports` parameter in *main.cf* to include your `ondemand` transport:

```
defer_transports = ondemand
```

3. Make sure that the `transport_maps` parameter points to your transport lookup table:

```
transport_maps = hash:/etc/postfix/transport
```

4. Add an entry to your *transport* file for *example.com* that points it to the `ondemand` transport:

```
example.com    ondemand
```

5. Execute `postmap` on the file.

```
# postmap /etc/postfix/transport
```

6. Reload Postfix so that it recognizes the changes in its configuration files:

```
# postfix reload
```

Now any message destined for *example.com* is deferred until there is an explicit command to deliver it.

When you are ready to release the deferred messages, issue the `postqueue -f` command:

```
$ postqueue -f example.com
```

Deferring delivery

A home network or small office network that wants to trigger delivery manually should defer all SMTP deliveries, so that delivery attempts only occur when a connection to the Internet has been established:

1. In *main.cf*, assign the `smtp` transport to the `defer_transports` parameter:

```
defer_transports = smtp
```

2. Reload Postfix so that it recognizes the changes in its configuration file:

```
# postfix reload
```

Once a connection is established, all of the messages can be delivered using `postqueue -f`.

The rest of this chapter describes various scenarios where Postfix must relay mail to other systems. In many cases, transport maps are necessary for configuring the next-hop delivery details.

Inbound Mail Gateway

A mail gateway is an email system that accepts messages and relays them to another system. Gateways might provide a path from one network to another, or from one protocol to another. A common use of a mail gateway is a server that accepts all the mail for a network from the Internet and relays it to internal mail systems. Mail gateways are commonly set up in conjunction with firewall systems to limit the number of servers that need direct access to the Internet.

Imagine a company network such as the one depicted in Figure 9-2. There are subdomains for different workgroups at the company, and each workgroup has its own internal mail server. The gateway system *gw.example.com* receives all the mail for the network. The human resources department gets email addressed as *user@hr.example.com*, and their mail should go to the server *mail1.example.com*. The sales department uses *user@sales.example.com*, and their mail should go to *mail2.example.com*. The client hosts in each subnet retrieve mail from their respective mail servers. Transport maps are required to set up the mail gateway *gw.example.com* to relay messages to the correct internal mail servers.

The following procedure demonstrates how to configure *gw.example.com* to relay messages to the correct internal systems:

1. Make sure that the DNS has been configured correctly with MX records for *hr.example.com* and *sales.example.com* pointing to the gateway *gw.example.com*.
2. In your *main.cf* file, set `relay_domains` to include the two internal domains:

```
relay_domains = hr.example.com, sales.example.com
```

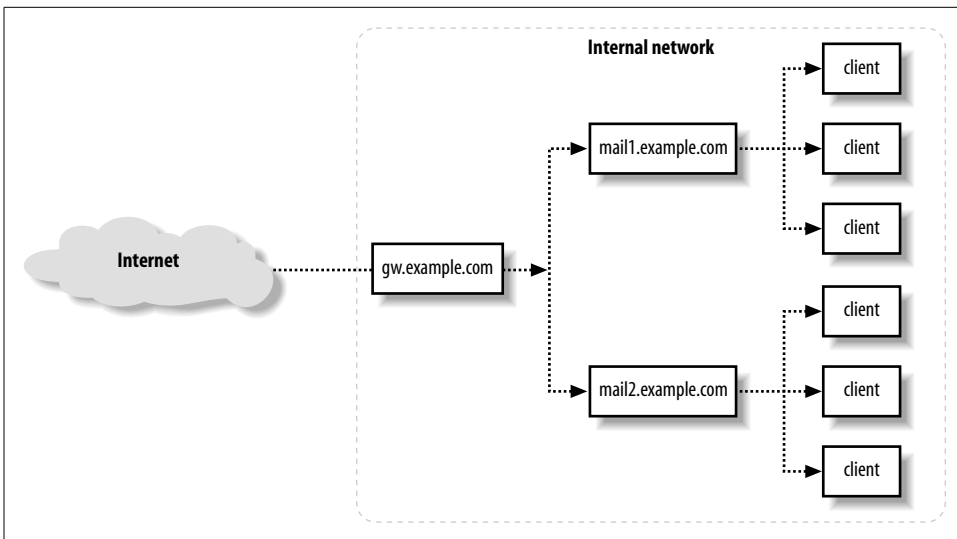


Figure 9-2. Email gateway to internal systems

3. Make sure that the `transport_maps` parameter points to your transport lookup table:

```
transport_maps = hash:/etc/postfix/transport
```

4. Add entries to your `transport` file for each domain pointing to the correct internal mail systems:

```
#
# transport maps
#
hr.example.com      relay:[mail1.example.com]
sales.example.com   relay:[mail2.example.com]
```

We've used brackets around the internal mail system host names to disable MX lookups for those systems.

5. Reload Postfix so that it recognizes the changes in its configuration files:

```
# postfix reload
```

It is highly recommended that you maintain a list of valid recipients for all of your internal users with the `relay_recipient_maps` parameter. See “Relay Recipients” earlier in the chapter.

Outbound Mail Relay

When a mail system does not have adequate connectivity or all of the information it needs to relay messages, it can forward them to another system that is in a better position for relaying. Consider the network in Figure 9-2 again. If the internal mail systems don't have direct access to the Internet, they can't deliver messages sent by

the users in their subnets. They can, however, pass along all messages to the gateway mail system, which can make the deliveries for them. The following procedure demonstrates setting up Postfix on *mail1.example.com* to relay all messages it receives to *gw.example.com*, which can then make the outbound deliveries.

Before configuring the internal mail systems, make sure that the mail gateway is set up to permit relaying from the internal mail systems. The `mynetworks` parameter (see Chapter 4) should encompass the IP addresses of the internal mail systems, and if you use SMTP UBE restrictions (see Chapter 11), be sure to include `permit_mynetworks` among the rules to allow relaying:

1. Check the `mynetworks` (or `mynetworks_style`) parameter to make sure it includes the client systems.
2. Have the users in the workgroup configure their various mail clients to use *mail1.example.com* as their SMTP server.
3. In *main.cf*, set the parameter `relayhost` to point to the gateway system:

```
relayhost = [gw.example.com]
```

4. Reload Postfix so that it recognizes the changes in its configuration file:

```
# postfix reload
```

Now all messages delivered to *mail1.example.com* are relayed through *gw.example.com*.

UUCP, Fax, and Other Deliveries

The Postfix online documentation describes configuring Postfix for delivery to a FAX system and setting up a gateway for UUCP. These provide good examples for configuring Postfix to work with all kinds of special devices. If you need to create a gateway between different types of systems or different networks, transport maps provide the mechanism for directing mail to the other systems or devices.