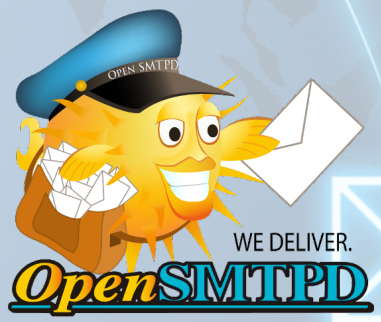
OpenSMTPD: we deliver

Giovanni Bechis
<giovanni@openbsd.org>

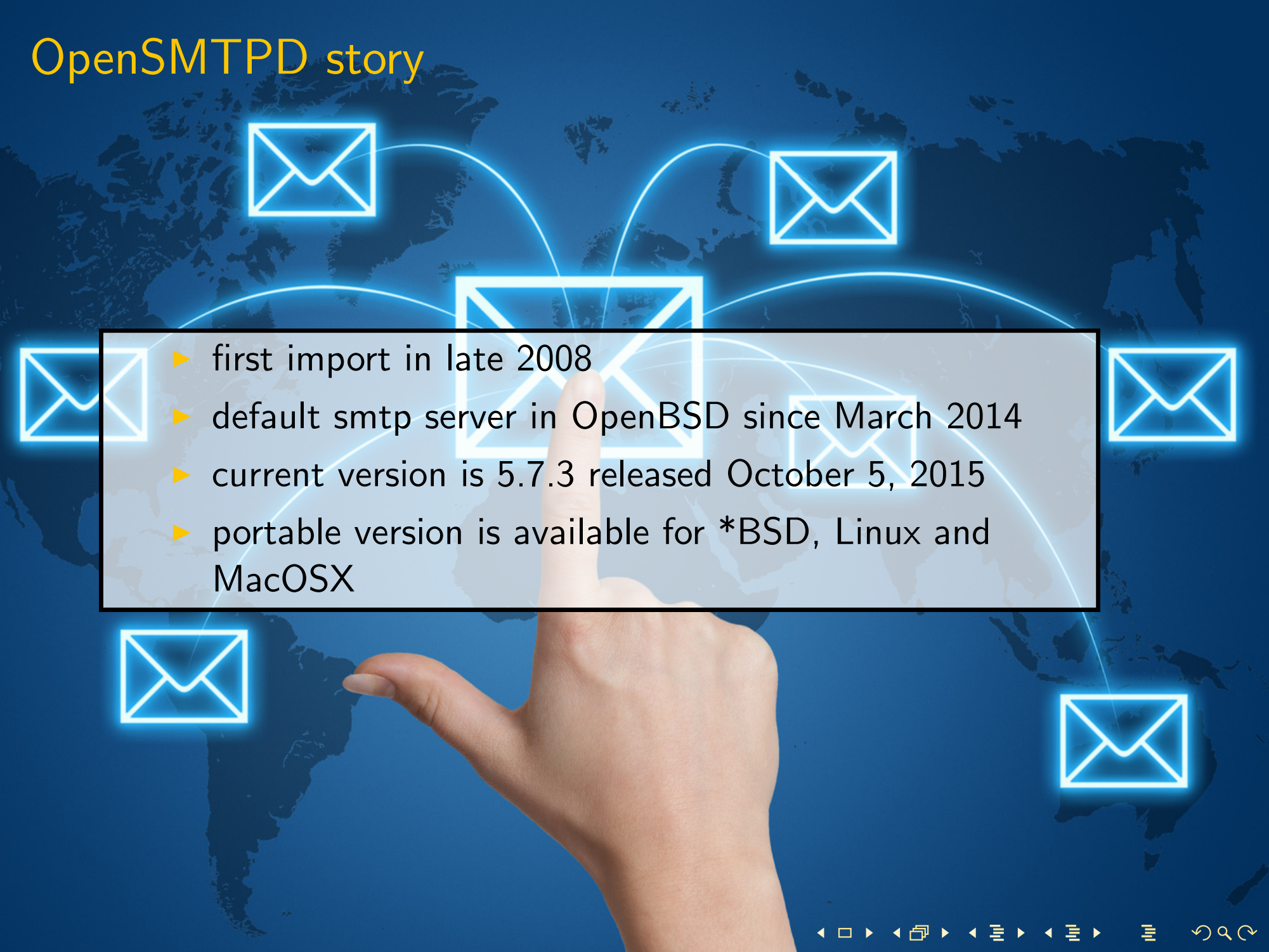
OpenSourceDay 2015



About Me

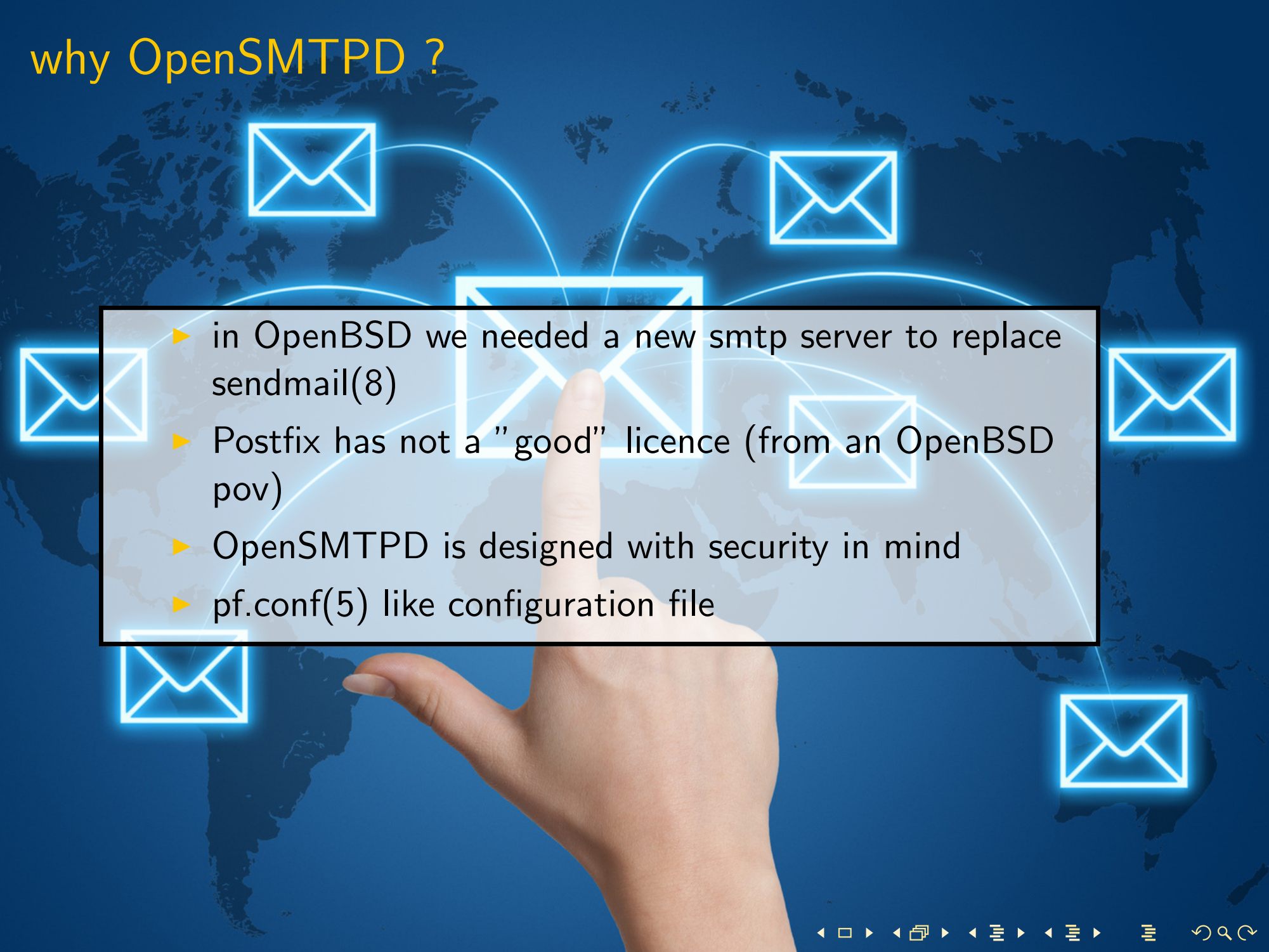
- sys admin and developer @SNB
- OpenBSD developer
- Open Source developer in several other projects

OpenSMTPD story



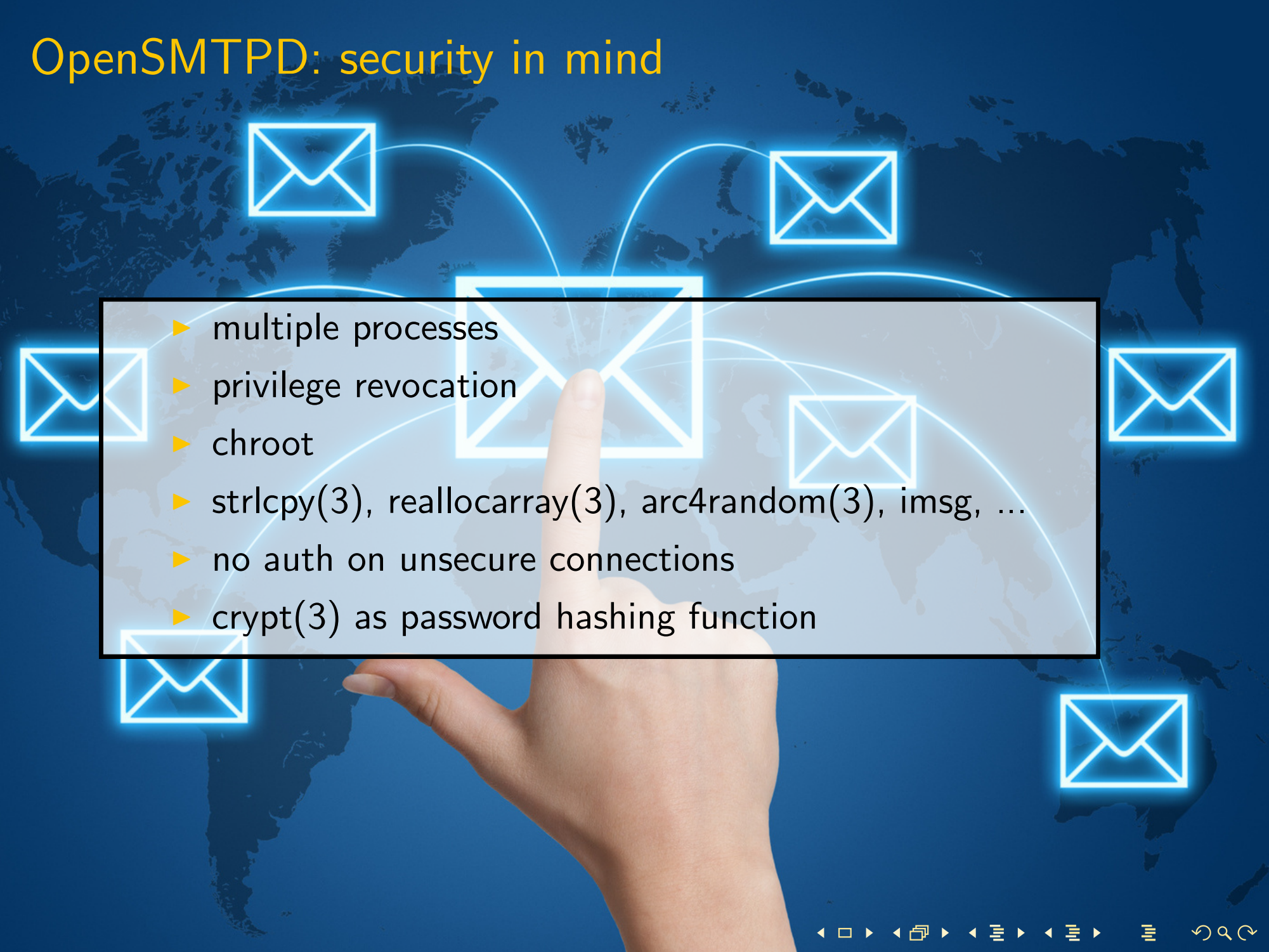
- first import in late 2008
- default smtp server in OpenBSD since March 2014
- current version is 5.7.3 released October 5, 2015
- portable version is available for *BSD, Linux and MacOSX

why OpenSMTPD ?



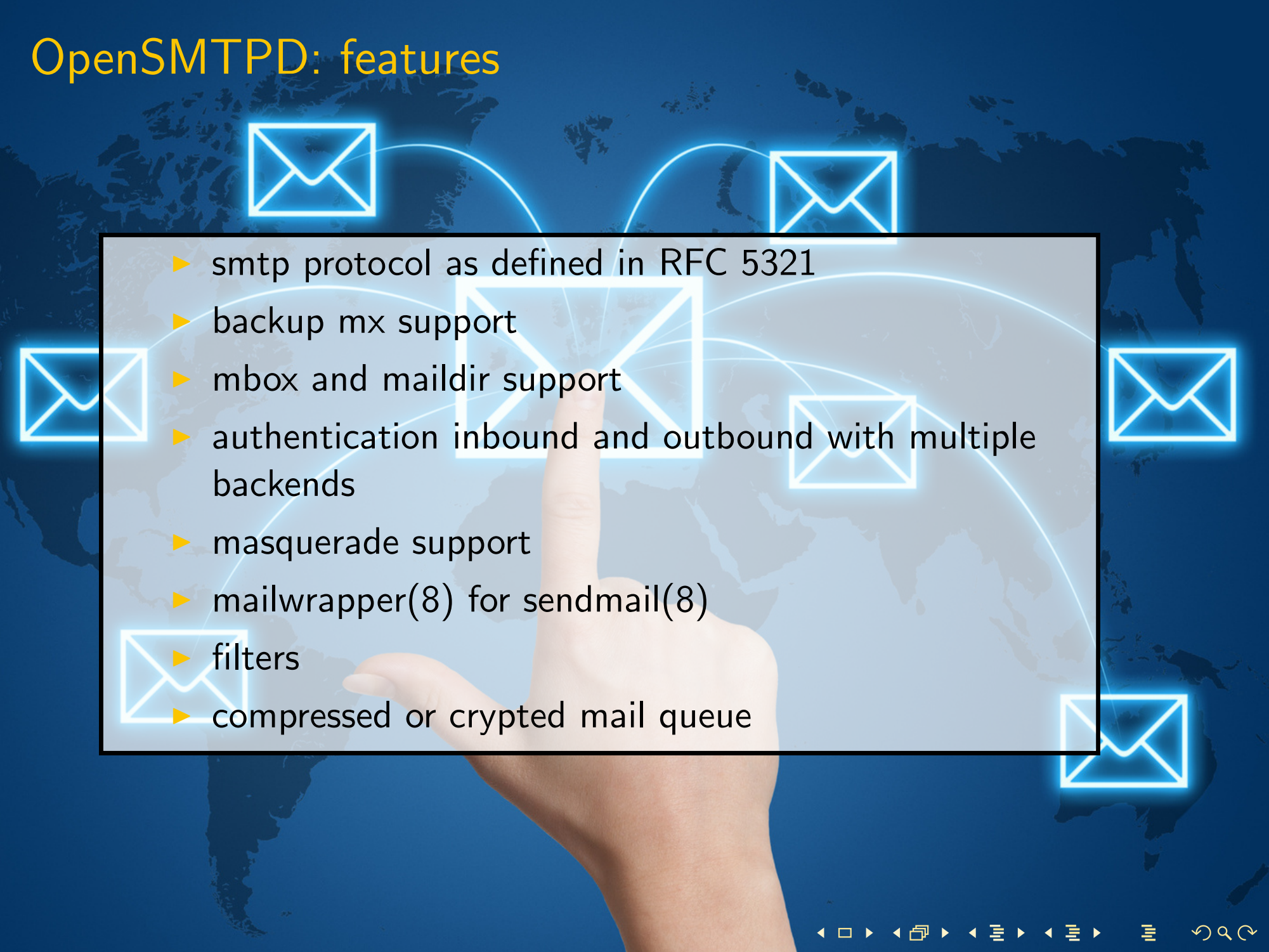
- in OpenBSD we needed a new smtp server to replace sendmail(8)
- Postfix has not a "good" licence (from an OpenBSD pov)
- OpenSMTPD is designed with security in mind
- pf.conf(5) like configuration file

OpenSMTPD: security in mind



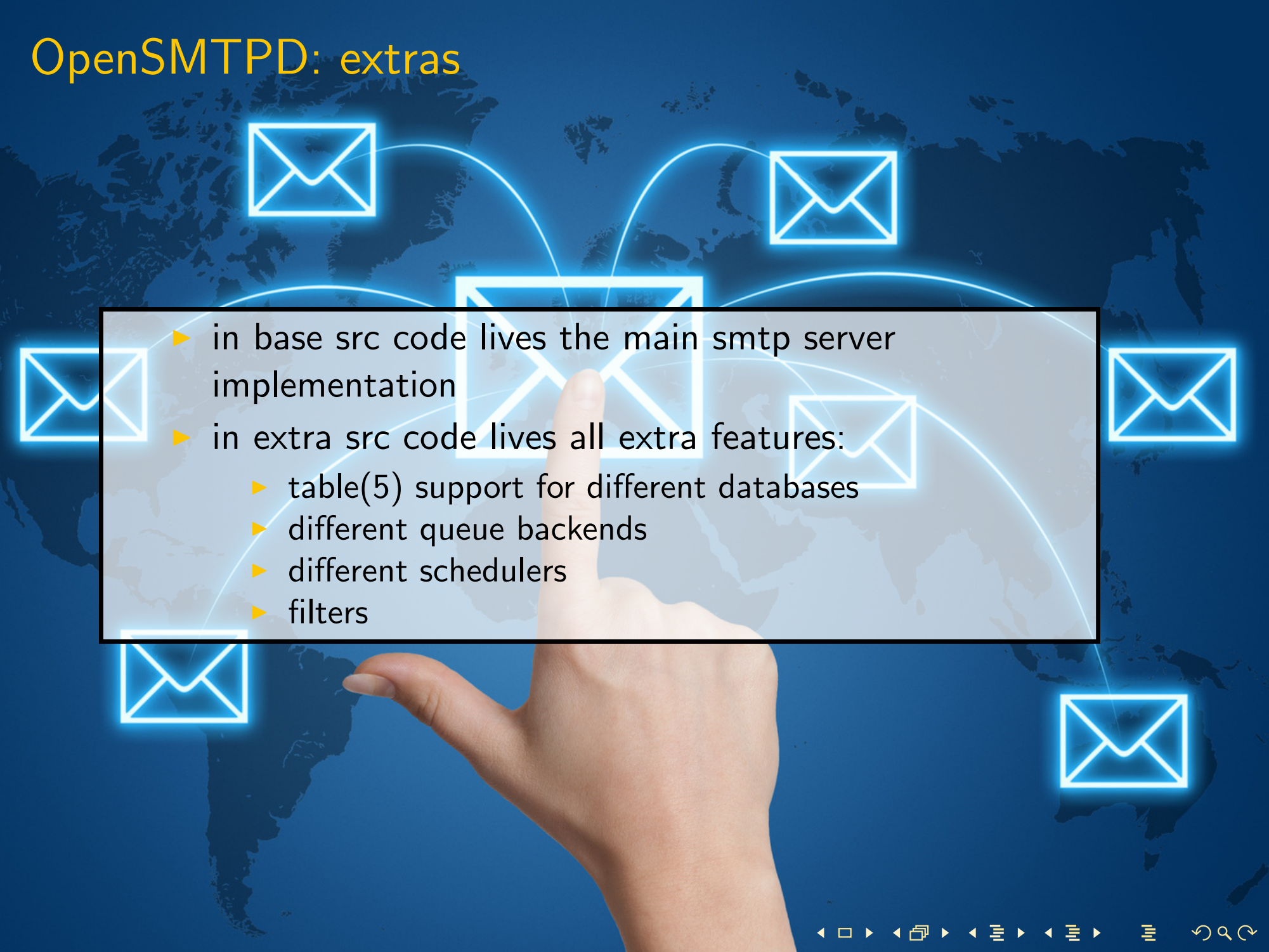
- multiple processes
- privilege revocation
- chroot
- strlcpy(3), reallocarray(3), arc4random(3), imsg, ...
- no auth on unsecure connections
- crypt(3) as password hashing function

OpenSMTPD: features



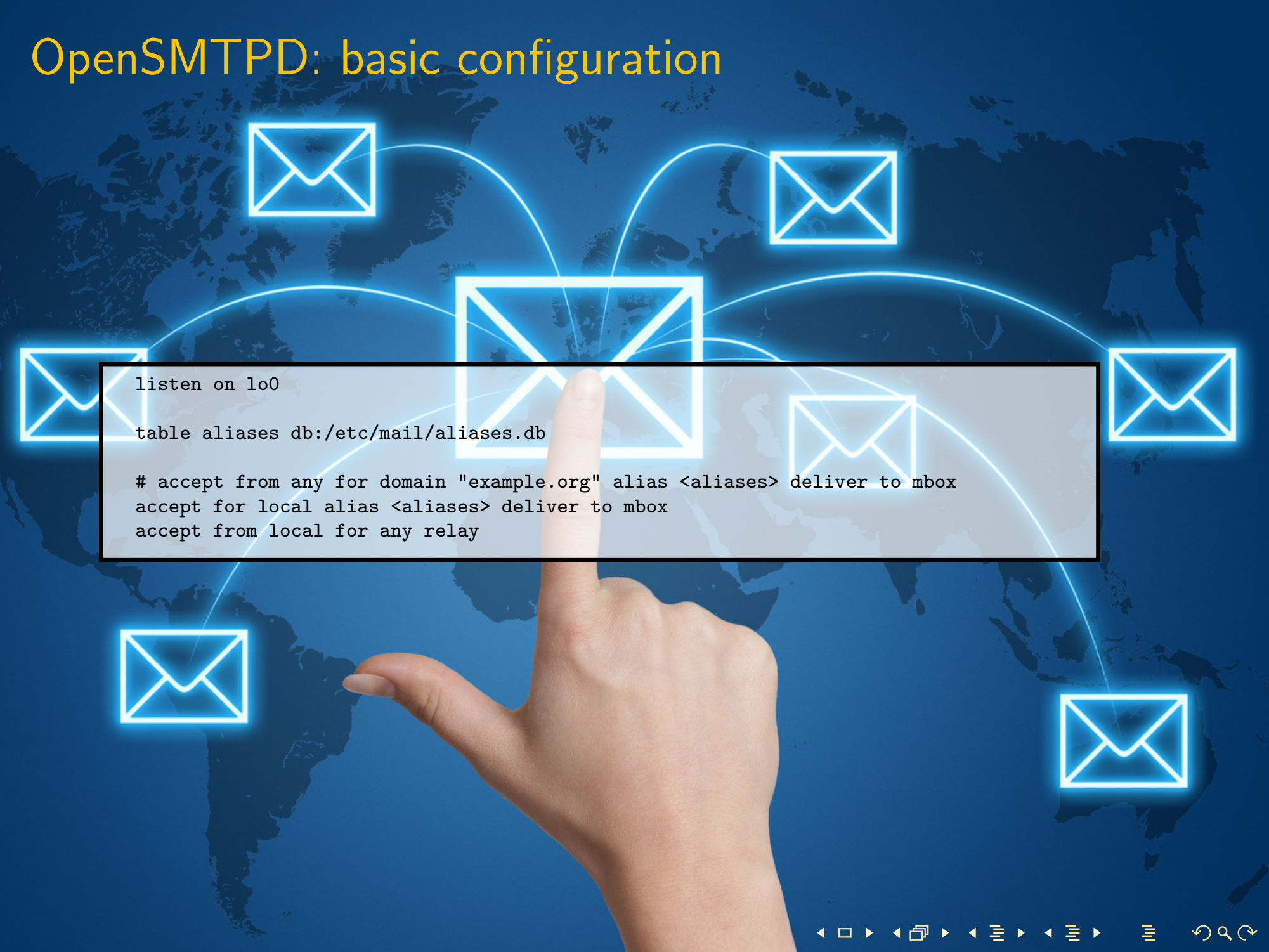
- smtp protocol as defined in RFC 5321
- backup mx support
- mbox and maildir support
- authentication inbound and outbound with multiple backends
- masquerade support
- mailwrapper(8) for sendmail(8)
- filters
- compressed or crypted mail queue

OpenSMTPD: extras



- in base src code lives the main smtp server implementation
- in extra src code lives all extra features:
  - table(5) support for different databases
  - different queue backends
  - different schedulers
  - filters

OpenSMTPD: basic configuration



```
listen on lo0

table aliases db:/etc/mail/aliases.db

# accept from any for domain "example.org" alias <aliases> deliver to mbox
accept for local alias <aliases> deliver to mbox
accept from local for any relay
```

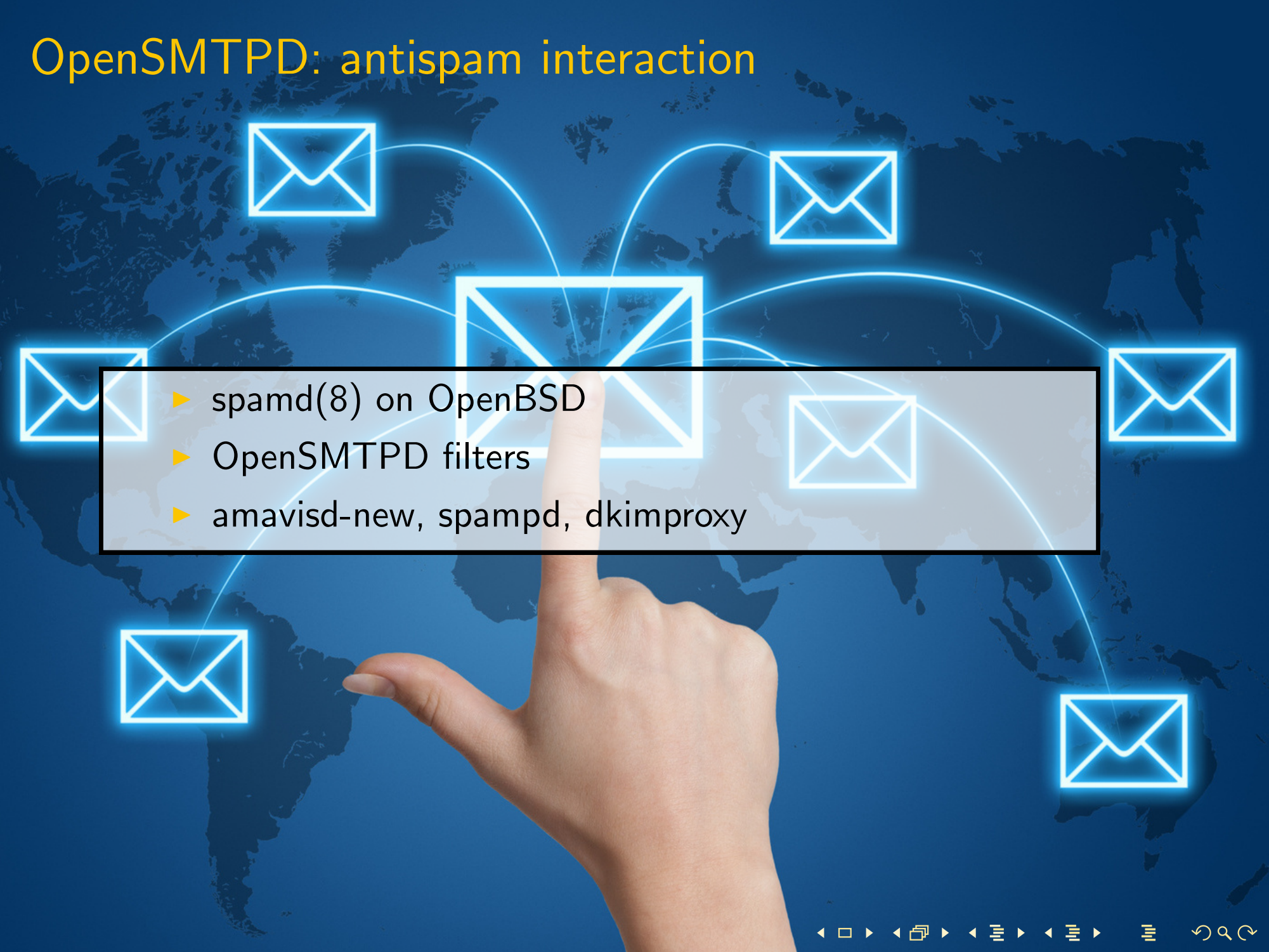
OpenSMTPD: advanced configuration

```
pki mail.example.org certificate "/etc/ssl/mail.example.org.crt"
pki mail.example.org key "/etc/ssl/private/mail.example.org.key"

filter myregex regex
filter mydnsbl dnsbl
filter myperl perl /usr/libexec/smtpd/spamfilter.pl
filter mychain chain myregex mydnsbl myperl

table aliases db:/etc/mail/aliases.db

table vusers mysql:/etc/mail/mysql.conf
table vdomains mysql:/etc/mail/mysql.conf
table valiases mysql:/etc/mail/mysql.conf
table credentials mysql:/etc/mail/mysql.conf

listen on eth0 secure auth-optional <credentials> pki mail.example.org filter mychain
listen on eth0 port submission tls auth <credentials> pki mail.example.org

listen on lo0 port 10025 tag Filtered
listen on lo0 port 10027 tag Signed

accept tagged Filtered for domain <vdomains> userbase <vusers> virtual <valiases> \
deliver to lmtp "/var/dovecot/lmtp"

accept from any for domain <vdomains> relay via "smtp://127.0.0.1:10024"

# Local emails
accept tagged Filtered for local alias <aliases> deliver to mbox
accept tagged Signed for any relay pki mail.example.org
accept for any relay via "smtp://127.0.0.1:10026"
```

OpenSMTPD: table(5)

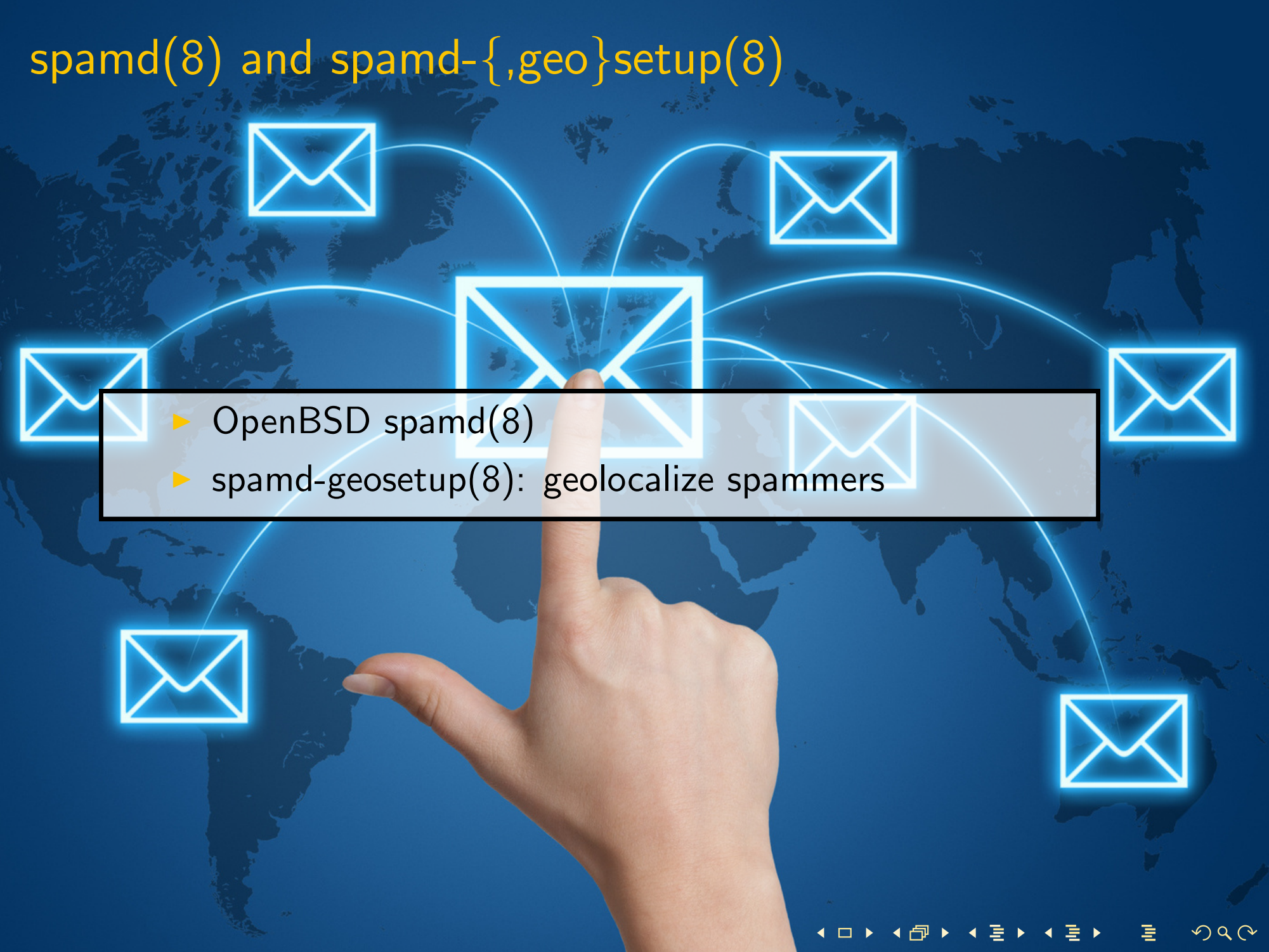
```
# smtpd.conf: table vusers mysql:/etc/mail/mysql.conf

host localhost
username user
password passwd
database db

# Alias lookup query
#
query_alias select destination from mail_valias where source=?


# Domain lookup query
#
query_domain                select domain from mail_domain where domain=?;

# User lookup query
#
query_userinfo                select uid,gid,maildir from mail_user where login=?;

# Credentials lookup query
#
query_credentials        select login, password from mail_user where login=?;
```

OpenSMTPD: antispam interaction



- spamd(8) on OpenBSD
- OpenSMTPD filters
- amavisd-new, spampd, dkimproxy

spamd(8) and spamd-{,geo}setup(8)



- OpenBSD spamd(8)
- spamd-geosetup(8): geolocalize spammers

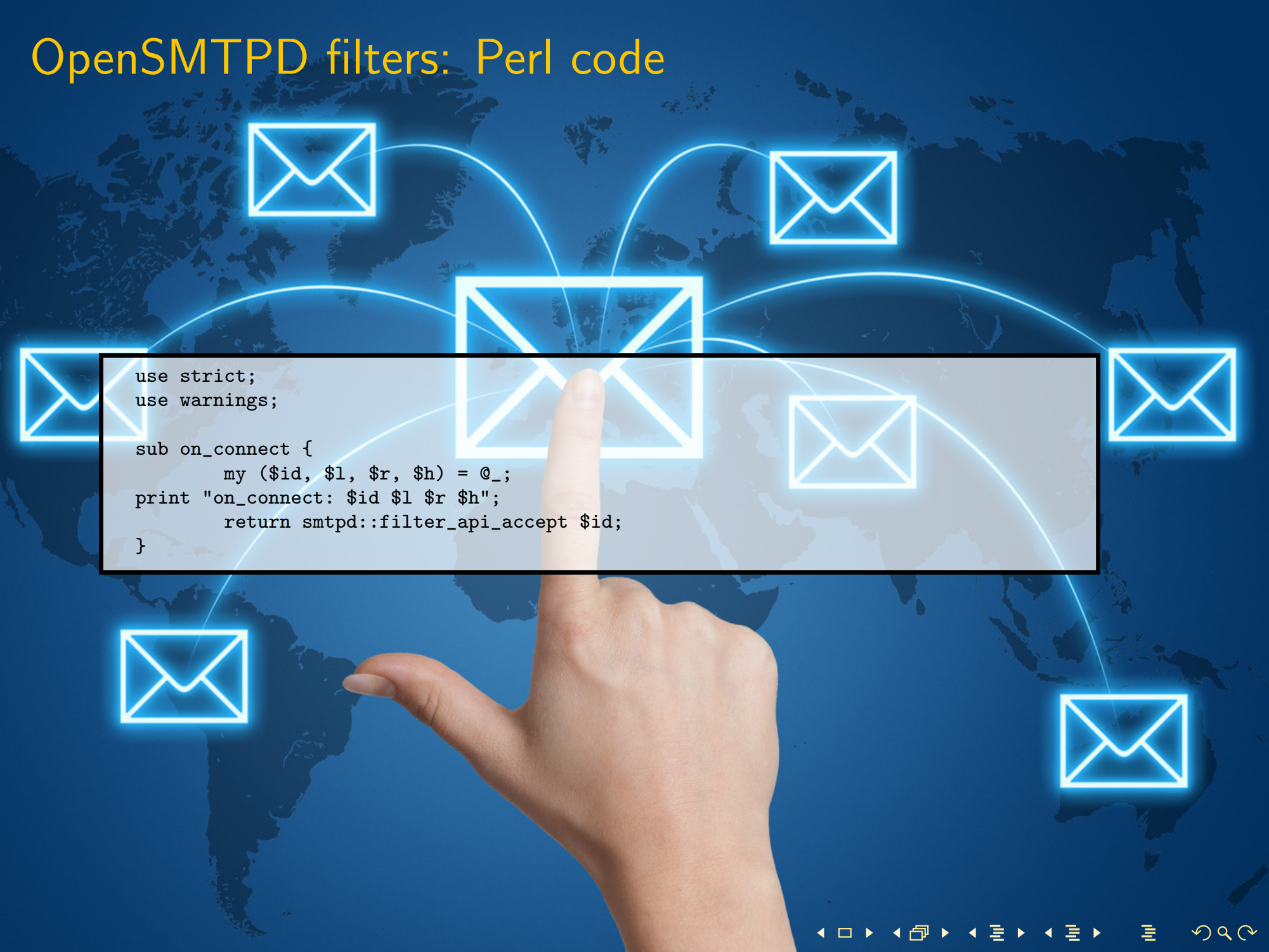
OpenSMTPD filters

- OpenSMTPD filters
- standalone programs written in C, Lua, Perl or Python
- the filter accepts or rejects the email
- talk to the main process via imsg_read(3) and friends
- fork(2) and imsg are managed by internals, writing a new filter is easy
- there are filters available for dnsbl, regex matching, SpamAssassin and Clamav integration and much more

OpenSMTPD filters: C code

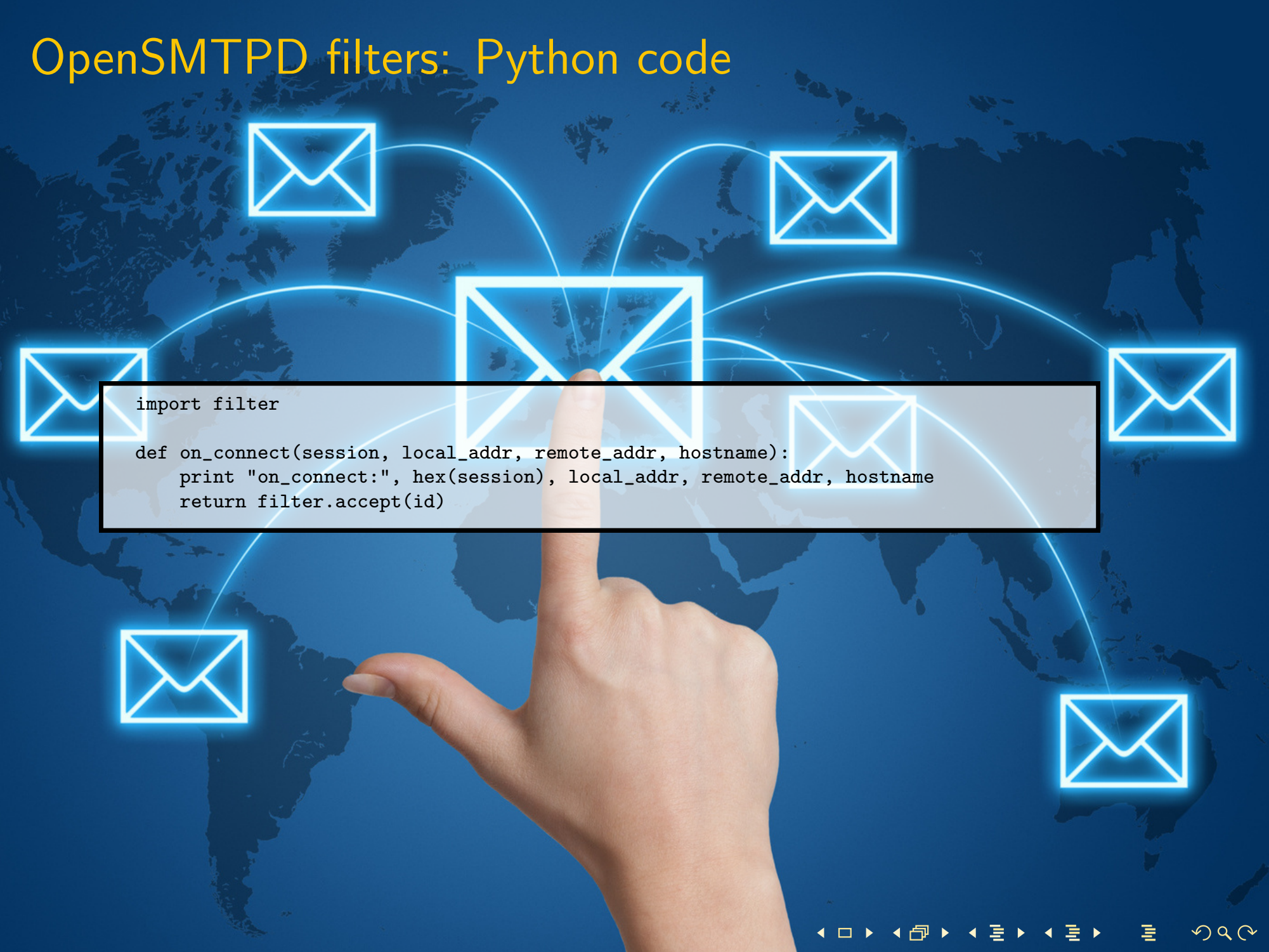
```
static int
on_connect(uint64_t id, struct filter_connect *conn) {
        log_warnx("filter-stub: ALOHA, WELCOME TO MY MAIL SERVER !");
        return (1);
}

int
main(int argc, char **argv) {
        int              ch;

        log_init(-1);
        while ((ch = getopt(argc, argv, "")) != -1) {
                switch (ch) {
                default:
                        log_warnx("warn: filter-stub: bad option");
                        return (1);
                        /* NOTREACHED */
                }
        }
        argc -= optind;
        argv += optind;

        /* register a callback for "on_connect" event */
        filter_api_on_connect(on_connect);

        /* start doing stuff */
        filter_api_loop();

        log_warnx("warn: filter-stub: exiting");
        return (1);
}
```

OpenSMTPD filters: Perl code



```
use strict;
use warnings;

sub on_connect {
        my ($id, $l, $r, $h) = @_;
print "on_connect: $id $l $r $h";
        return smtpd::filter_api_accept $id;
}
```

OpenSMTPD filters: Python code

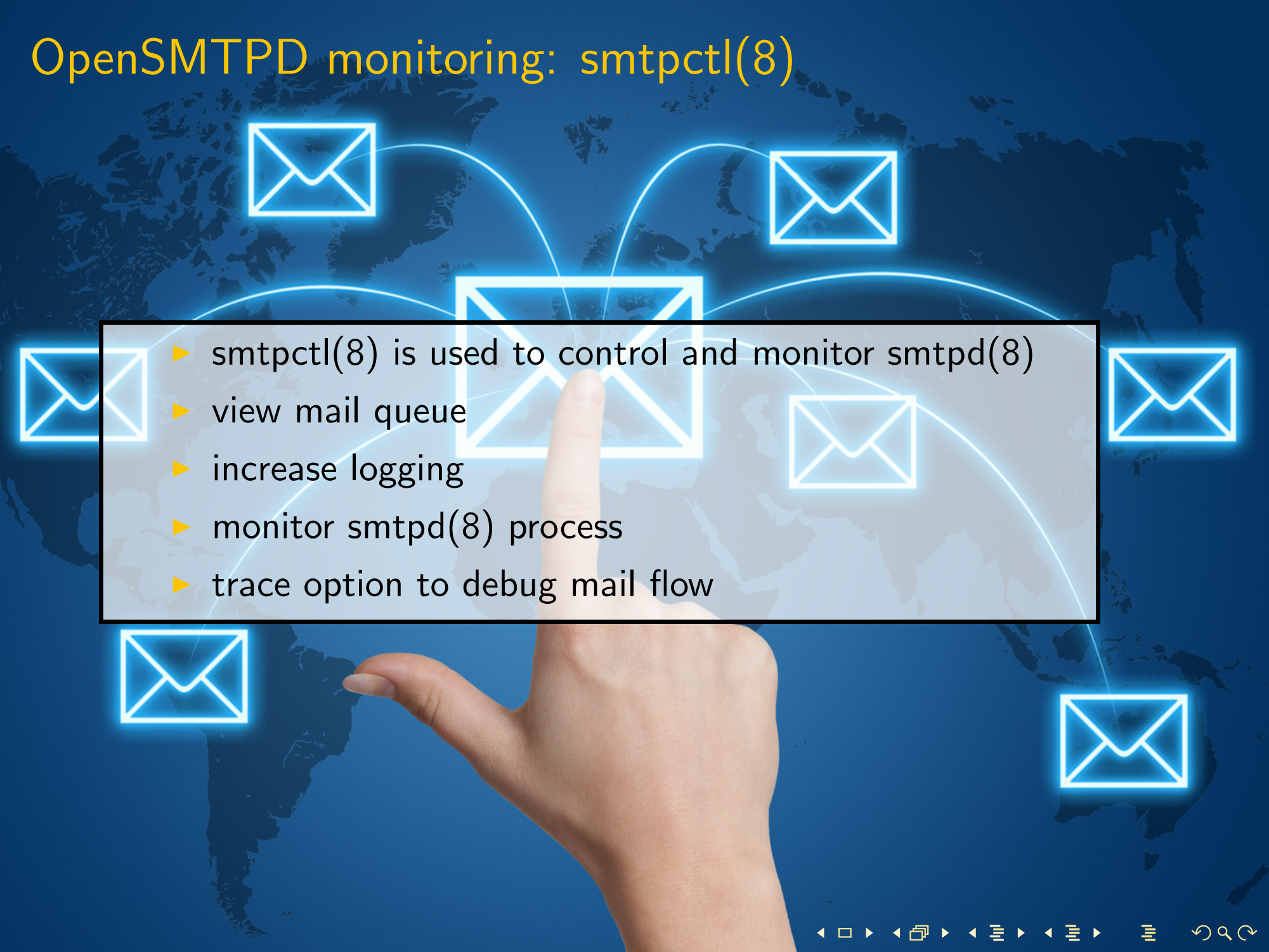


```
import filter

def on_connect(session, local_addr, remote_addr, hostname):
    print "on_connect:", hex(session), local_addr, remote_addr, hostname
    return filter.accept(id)
```

OpenSMTPD monitoring: log files

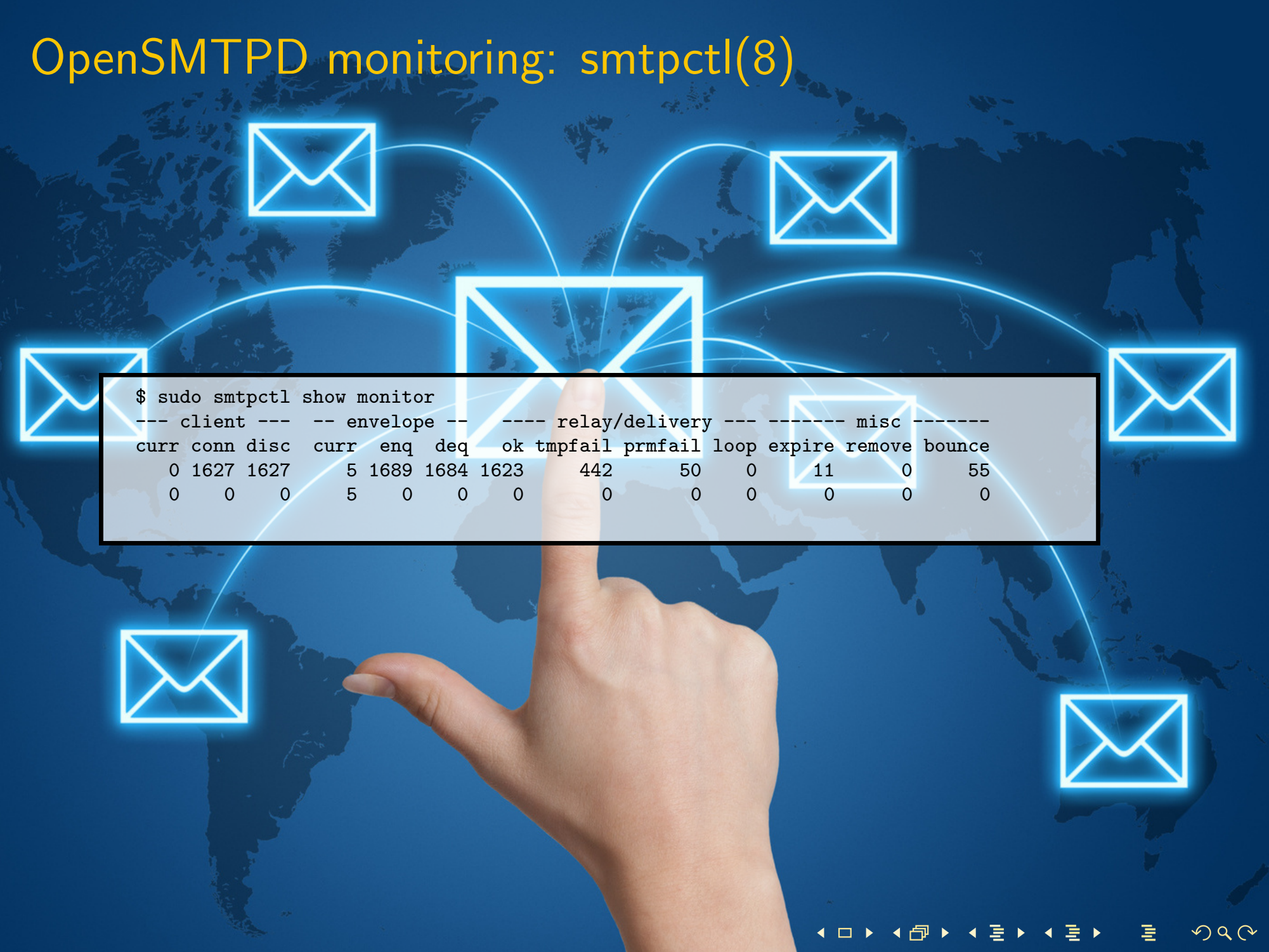
```
Nov 13 10:07:54 srv smtpd[21974]: smtp-in: New session a4bfab6025324cef from host \
localhost [127.0.0.1]
Nov 13 10:07:55 srv smtpd[21974]: smtp-in: Accepted message 99642806 \
on session a4bfab6025324cef: from=<giovanni@123.org>, to=<simone@456.it>, \
size=792, ndest=1, proto=ESMTP
Nov 13 10:07:55 srv smtpd[21974]: smtp-out: Connecting to \
smtps://1.2.3.4:456 (smtps.123.org) on session a4bfab63b131e516...
Nov 13 10:07:55 srv smtpd[21974]: smtp-in: Closing session a4bfab6025324cef
Nov 13 10:07:55 srv smtpd[21974]: smtp-out: Connected on session a4bfab63b131e516
Nov 13 10:07:55 srv smtpd[21974]: smtp-out: Started TLS on session a4bfab63b131e516: \
version=TLSv1.2, cipher=ECDHE-RSA-CHACHA20-POLY1305, bits=256
Nov 13 10:07:55 srv smtpd[21974]: smtp-out: Server certificate \
verification failed on session a4bfab63b131e516
Nov 13 10:07:56 srv smtpd[21974]: relay: Ok for 9964280638a33dd5: \
session=a4bfab63b131e516, from=<giovanni@123.org>, to=<simone@456.it>, \
rcpt=<->, source=192.168.1.2, relay=1.2.3.4 (smtps.123.org), delay=1s, \
stat=250 2.0.0: d984513a Message accepted for delivery
Nov 13 10:08:06 srv smtpd[21974]: smtp-out: Closing session a4bfab63b131e516: \
1 message sent.
```

OpenSMTPD monitoring: smtpctl(8)



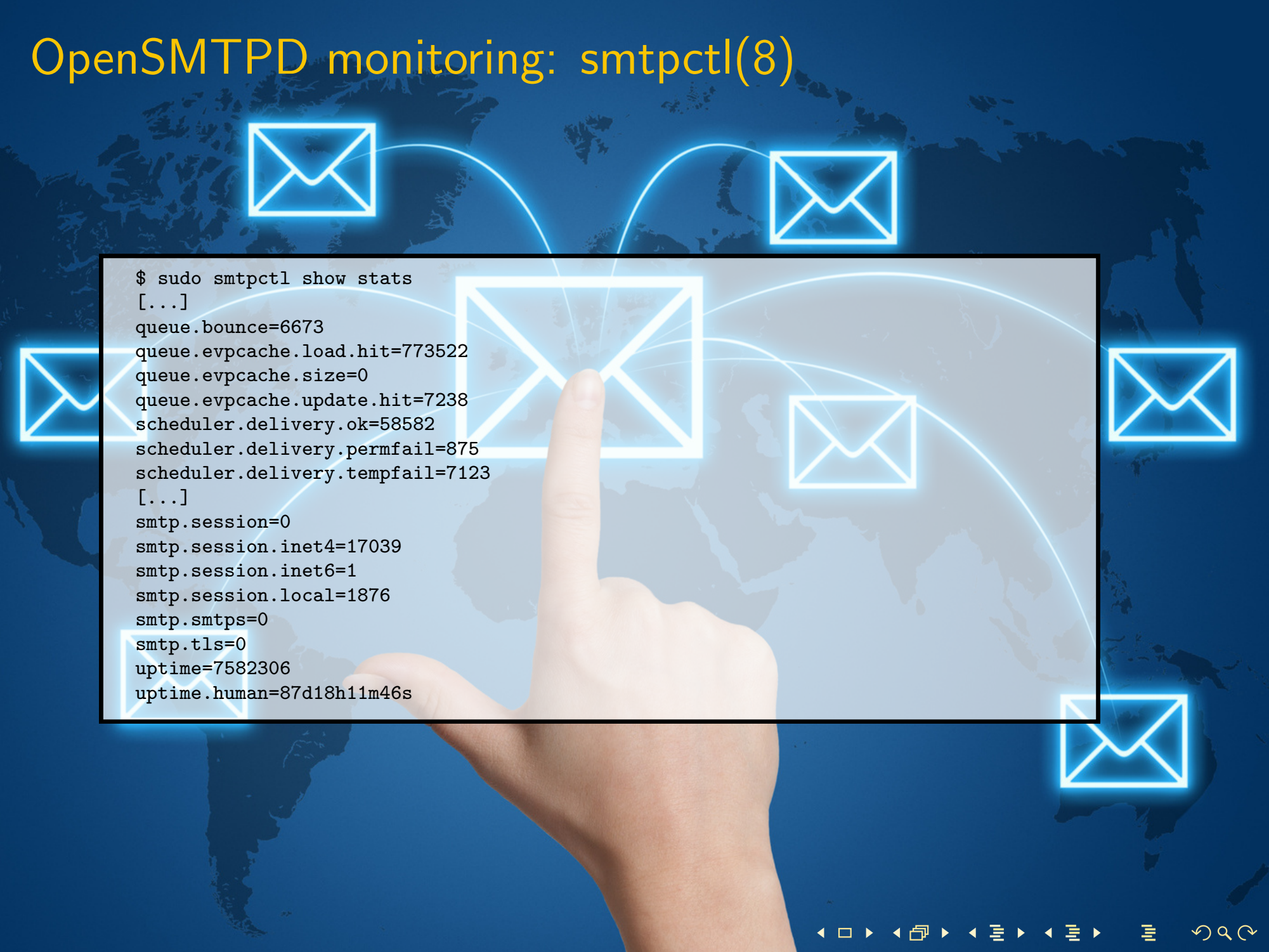
- smtpctl(8) is used to control and monitor smtpd(8)
- view mail queue
- increase logging
- monitor smtpd(8) process
- trace option to debug mail flow

OpenSMTPD monitoring: smtpctl(8)



```
$ sudo smtpctl show monitor
--- client ---  -- envelope --   ---- relay/delivery --- ------- misc -------
curr conn disc  curr  enq  deq   ok tmpfail prmfail loop expire remove bounce
   0 1627 1627     5 1689 1684 1623     442      50    0     11      0     55
   0    0    0     5    0    0    0       0       0    0      0      0      0
```

OpenSMTPD monitoring: smtpctl(8)



```
$ sudo smtpctl show stats
[...]
queue.bounce=6673
queue.evpcache.load.hit=773522
queue.evpcache.size=0
queue.evpcache.update.hit=7238
scheduler.delivery.ok=58582
scheduler.delivery.permfail=875
scheduler.delivery.tempfail=7123
[...]
smtp.session=0
smtp.session.inet4=17039
smtp.session.inet6=1
smtp.session.local=1876
smtp.smtps=0
smtp.tls=0
uptime=7582306
uptime.human=87d18h11m46s
```

OpenSMTPD monitoring: smtpctl(8) trace

```
[...]
expand: 0x133db4879018: inserted node 0x133cf460d800
expand: lka_expand: username: giovanni [depth=1]
lookup: lookup "giovanni" as ALIAS in table db:aliases -> 0
lookup: lookup "giovanni" as USERINFO in table getpwnam:<getpwnam> -> "giovanni:
1000:103:/home/giovanni"
mproc: lka -> parent : 1080 IMSG_LKA_OPEN_FORWARD
imsg: parent <- lka: IMSG_LKA_OPEN_FORWARD (len=1080)
mproc: parent -> lka : 1080 IMSG_LKA_OPEN_FORWARD
imsg: lka <- parent: IMSG_LKA_OPEN_FORWARD (len=1080)
expand: no .forward for user giovanni, just deliver
lookup: lookup "giovanni" as USERINFO in table getpwnam:<getpwnam> -> "giovanni:
1000:103:/home/giovanni"
mproc: lka -> queue: allocating 128
mproc: lka -> queue: realloc 128 -> 512
mproc: lka -> queue : 361 IMSG_LKA_ENVELOPE_SUBMIT
mproc: lka -> queue : 9 IMSG_LKA_ENVELOPE_COMMIT
expand: 0x133db4879018: clearing expand tree
imsg: queue <- lka: IMSG_LKA_ENVELOPE_SUBMIT (len=361)
queue-backend: queue_envelope_create(09a2ee6000000000, 342) -> 1 (09a2ee60261b00
61)
[...]
```

Questions ?


SNB
Information Technology
& Web Solutions
OpenSMTPD
WE DELIVER.
OpenSMTPD