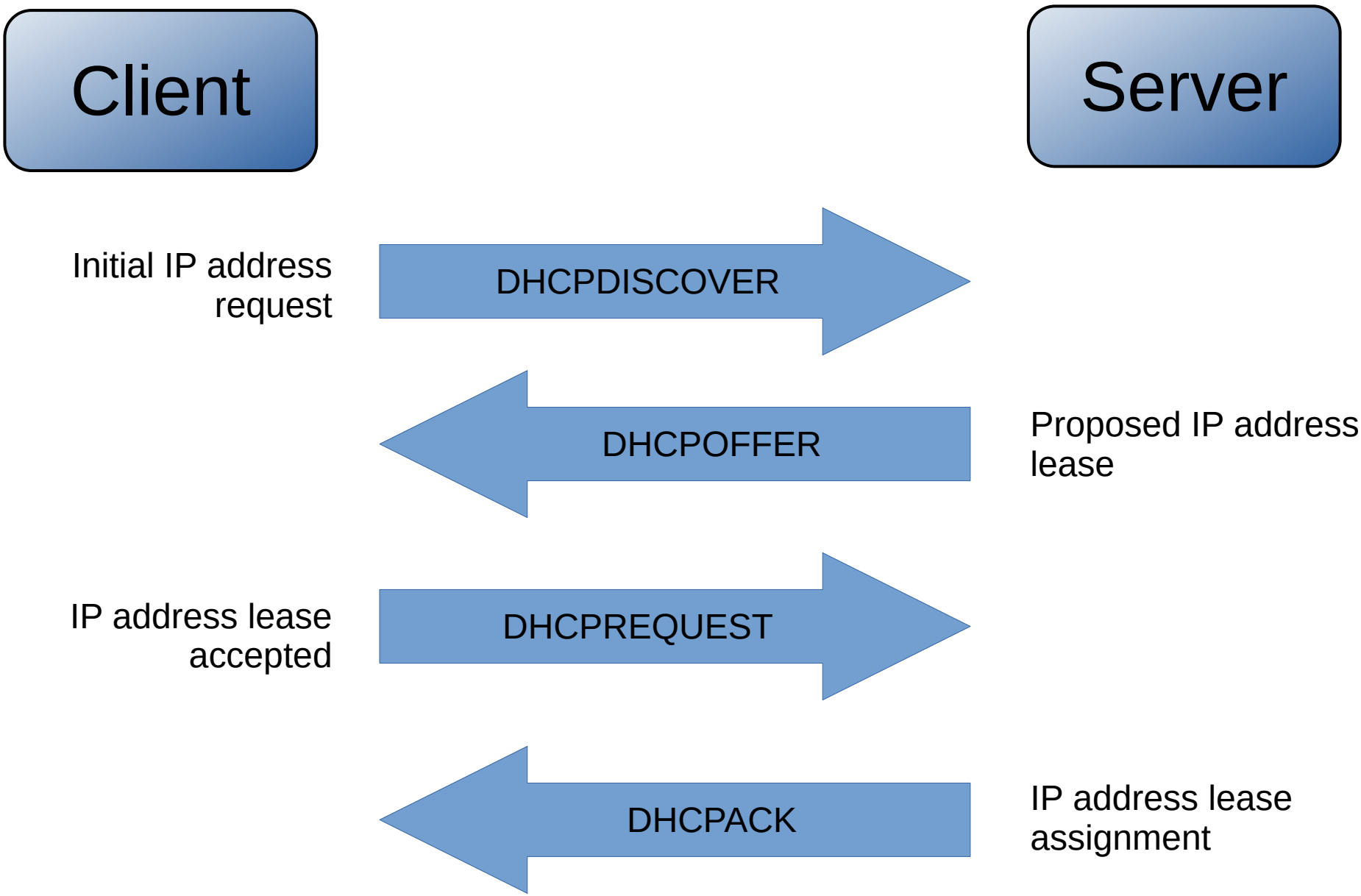
Linux Administration

Network services

Xavier Belanger

DHCP

- Dynamic Host Configuration Protocol
- Used to provide IP configuration to computers connecting to a network.
- Also used for extra configuration for specific devices (IP phones, …).
- Using port UDP/67 and UDP/68.


Client
Server
Initial IP address request
DHCPDISCOVER
DHCPOFFER
Proposed IP address lease
IP address lease accepted
DHCPREQUEST
DHCPACK
IP address lease assignment

ISC DHCPD and Kea

- Historically ISC DHCPD has been the main DHCP server used on Linux and UNIX systems. It at reached end of life support.
- The configuration file is usually /etc/dhcpd.conf.
- ISC Kea is a more modern DHCP server (also more complex).

```
# 24 hours lease (24*3600 seconds)
default-lease-time 86400;
# 48 hours maximum lease
max-lease-time 172800;


# Local network
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.60 192.168.1.90;
  option routers 192.168.1.1;
  option domain-name-servers 192.168.1.10;
  option domain-name "example.net";
}
```

SSH

- Secure Shell
- Used to remotely connect to a system, execute commands and transfer files.
- Using port TCP/22.

OpenSSH

- Initially developed for the OpenBSD system, OpenSSH has been ported to various other systems.
- It’s highly configurable, and can be fine-tuned for specific usages.
- The default configuration file for the service is /etc/ssh/sshd_config.

DNS

- Domain Name System
- Used to convert names to IP addresses and IP addresses to names.
- DNS actually provide much more than addresses and names resolution.
  This service is essential for almost all other services. Email relies heavily on DNS.
- Using port UDP/53 and TCP/53.

DNS server roles

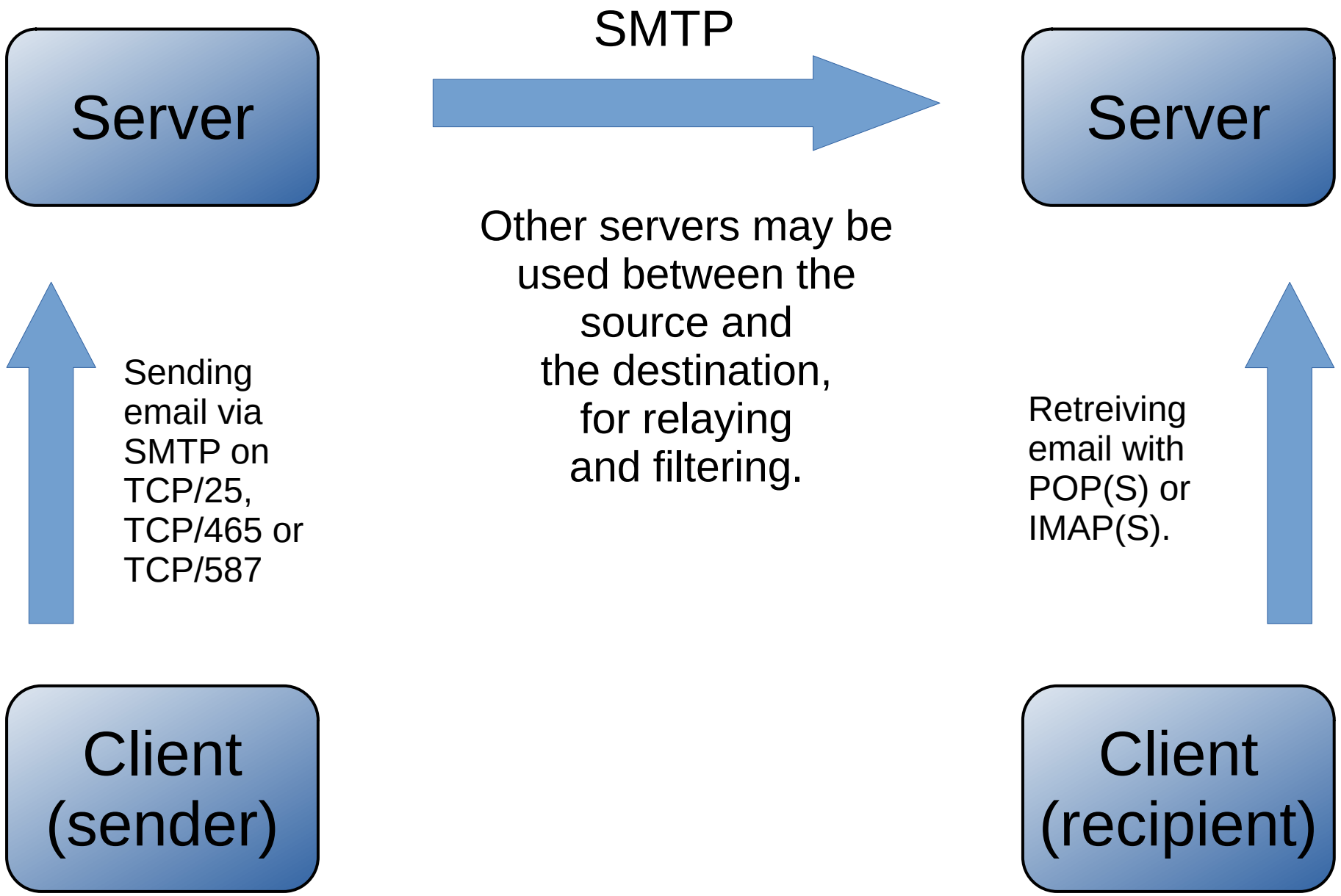
- A DNS server can be configured in two different modes:
  - authoritative mode, where the server is the authority for one or more networks.
  - recursive mode, where the server will relay the queries from the clients to another server.
- It’s possible to use both modes on the same system, but this is against good practices.

ISC BIND

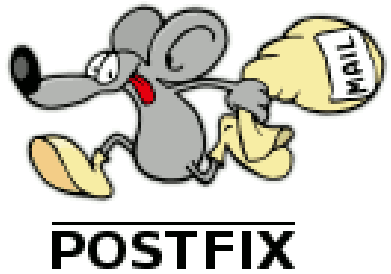
- Historically ISC BIND has been the main DNS server used on Linux and UNIX systems.
- The configuration file is usually /etc/named.conf, plus some additional files for zones if required.

SMTP, POP, IMAP

- On the server side:
  - Simple Mail Transfer Protocol (TCP/25, TCP/465 SMTPS, TCP/587 - Submission)
- On the client side:
  - Post Office Protocol (TCP/110, TCP/995 - POPS)
  - Internet Message Access Protocol (TCP/143, TCP/993 - IMAPS).


SMTP
Server
Server
Other servers may be used between the source and the destination, for relaying and filtering.
Sending email via SMTP on TCP/25, TCP/465 or TCP/587
Retreiving email with POP(S) or IMAP(S).
Client (sender)
Client (recipient)

Postfix



- Postfix is one of the most well-known email server application on Linux (Exim is another known solution).
- The configuration can vary greatly depending on the purpose of the server itself (relay, mailbox hosting, filtering, etc.).
- In itself Postfix only sends and receives email; it doesn’t provide access to the recipient mailboxes.

Courier, Dovecot

- Specific services can be deployed to manage mailboxes and provide POP and IMAP access; Courier and Dovecot at some of the most well-known applications for this.
- A webmail is only an interface to a regular IMAP server.

HTTP

- HyperText Transfer Protocol
- Initially developed and used for the World Wide Web, nowadays used for plenty of other applications.
- Using port TCP/80 and TCP/443 (HTTPS) by default.

Apache HTTPD

- Apache HTTPD is one of most-used web servers (Nginx is the closest competitor).
- That application has been around for a long time and has a large community, with plenty of documentation available.

```
# This is the main Apache HTTP server configuration file.
# It contains the configuration directives that give
# the server its instructions.
#
# Do NOT simply read the instructions in here without
# understanding what they do.  They're here only as hints
# or reminders.  If you are unsure consult the online docs.
# You have been warned.
```

Debian/Ubuntu specifics

- On any Debian-based Linux distribution, the Apache HTTPD configuration is split across various files and sub-directories.
  - /etc/apache2/conf-available and /etc/apache2/conf-enabled
  - /etc/apache2/mods-available and /etc/apache2/mods-enabled
  - /etc/apache2/sites-available and /etc/apache2/sites-enabled
- Additional commands are also available to perform common operations.
  - a2enconf and a2disconf (enable or disable a specific configuration)
  - a2enmod and a2dismod (enable or disable a specific module)
  - a2ensite and a2dissite (enable or disable a specific site)

LDAP

- Lightweight Directory Access Protocol
- Used as a directory to authenticate users, can store various type of information for each entity.
- Using port TCP/389 and TCP/636 (LDAPS).

OpenLDAP

- OpenLDAP is the most popular free and open-source directory application.
- Fact: many organizations are using Microsoft Active Directory.
  Active Directory is based on LDAP and can be used as such.

Samba

- Samba is a client / server application allowing integration with MS Windows AD domains (user authentication, file and printer sharing).
- In some instances it could be used as a replacement of an Active Directory environment.

About SSL/TLS

- SSL: Secure Socket Layer
- SSL is obsolete and insecure, but the acronym is still very much in use.
- TLS: Transport Layer Security
- TLS is used to encrypt and authenticate network traffic for various applications.

OpenSSL

- On Linux systems, OpenSSL is the mostly commonly used cryptography library and tool set.
- OpenSSL can be used to generate security certificates, data encryption and help for troubleshooting.