DNS(ネーム)サーバ設定

(1)DNS サーバ（bind）のインストール確認

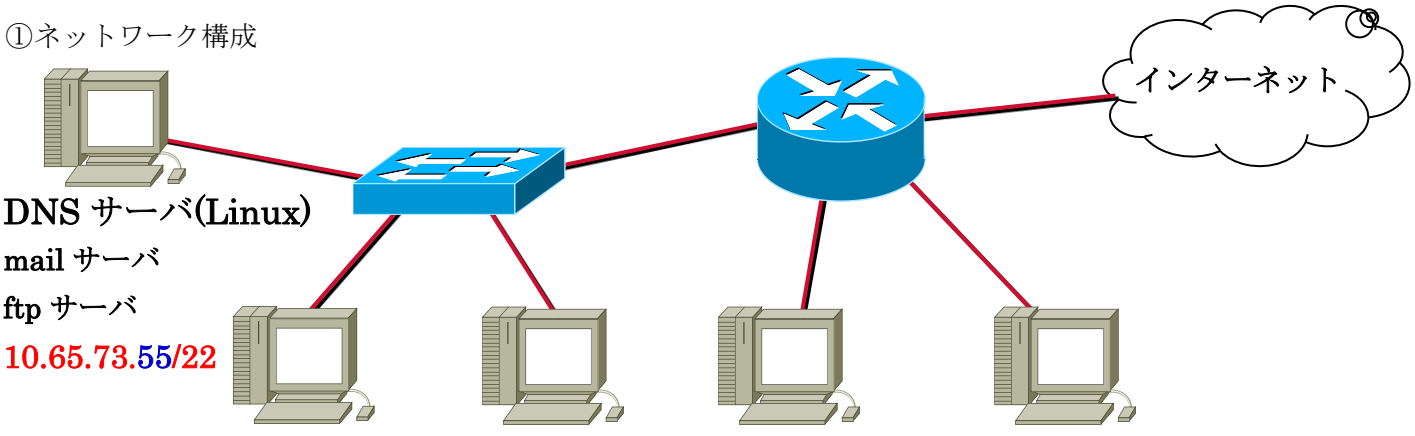
[hal@motobe ~]$ **rpm -q bind**
bind-9.16.23-11.el9.x86_64
[hal@motobe ~]$ **rpm -q bind-utils**
bind-utils-9.16.23-11.el9.x86_64
※共にインストールされているハズです

※インストールされていない時は
[hal@motobe ~]$**sudo yum install -ybind**
[hal@motobe ~]$**sudo yum install -ybind-utils**

●DNS とは関係ないのですが後(mail サーバ)で使用するプログラムを先にインストールしておきます
[hal@motobe ~]$ **sudo yum install -y s-nail**
[hal@motobe ~]$ **rpm -q s-nail**
s-nail-14.9.22-8.el9.x86_64 ←インストール出来ました

(2)構築の前に・・・DNS のイメージ

①ネットワーク構成



	DNS サーバ	クライント	
ホスト名	DNS サーバ	File サーバ	プリントサーバ
FQDN	motobe.com	file.motobe.com	print.motobe.com
ローカル IP アドレス	10.65.73.55/22	10.65.73.200/22	10.65.73.201/22

※DNS サーバ(Linux)の IP アドレスは「出席番号＋100」に手動設定　←手動(固定)IP
※DNS サーバ(10.65.73.55)の PC に FTP サーバと mail サーバも同居
※FQDN :「Fully Qualified Domain Name」の略。日本語では「完全修飾ドメイン名」あるいは「絶対ドメイン名」と訳されています。
※クライント(File サーバ、プリントサーバはダミー)
※HAL の学内 DNS サーバ：10.72.1.11、10.72.1.13　が 2 台あり

②対応表の管理

bind は**ホスト名と IP アドレスの対照表をゾーンという単位で管理**しています。

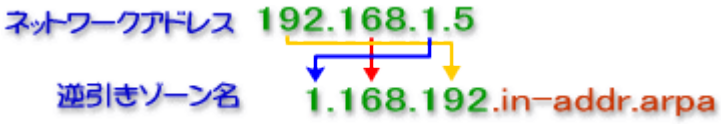
マスタサーバ(メインの DNS サーバ)として設定を行なうには、まずゾーン名を決める必要があります。

また、この**ゾーンには正引きゾーンと逆引きゾーン**があります。

※内部からの問い合わせは、ローカル IP の返却を行い、外部からの問い合わせは自サーバのグローバル IP を返却するように構築を行います。
(外部からの問い合わせにローカル IP を返却しても意味がありませんし、ローカル情報を公開する事は好ましくありませんので制限をかける事とします。)

③正引きゾーン名とは・・・
正引きはドメイン名を IP アドレスに変換します。
正引きゾーンファイル名はドメインの motobe.com が正引きゾーン名となります

④逆引きゾーン名とは・・・
逆引きゾーンは IP アドレスをドメイン名に変換を行ないます。
使用する IP アドレスのネットワークアドレス部分から作成し、ネットワークアドレスを逆から作成しその値+.in-adde.arpa とします。
言葉だと分かりにくいので逆引きゾーン名を例とすると、



逆引きゾーン名は(例)1.168.192.in-addr.arpa になります

⑤固定 IP アドレスの設定
以前設定した　Linux 右上のボタン中の　→　有線設定
→　IPv4　→　手動　→　10.65.73.(出席番号＋100)
→　DNS(10.65.73.(出席番号＋100)
→　適用
[hal@motobe ~]$**ifconfig**　←変更確認
※上手く変更できない時は
Linux 右上のボタン中の　→　有線　→　オフ　→　接続

(2)DNS（BIND）設定

①設定ファイルのバックアップと変更

[hal@motobe ~]$**sudo cp /etc/named.conf /etc/named.conf.old**←DNS サーバ設定コピー
※絶対にバックアップを取っておいてください

[hal@motobe ~]$**ls /etc/named.conf**
named.conf　　**named.conf.old**

[hal@motobe ~]$ **sudo vi /etc/named.conf**　　←DNS サーバ設定ファイル編集
※先頭の数字は(:setnum で行番号を表示しているだけ)

・9 行目の空欄に追記

```
10    acl internal-network {
11          10.0.0.0/8;
12 };
```

・15 行目　全てに対してポート番号 53 をリッスンする

```
15          listen-on port 53 { 127.0.0.1; };
    ↓
15listen-on port 53 { any; };
```

・16 行目　IPv6 もリッスン(使わない時は nome)

```
16          listen-on-v6 port 53 { ::1; };
    ↓
16listen-on-v6 port 53 { any; };
```

・23 行目　bind を使用する範囲を指定(内部からのみ問合せを許可)

```
23          allow-query     { localhost;};
    ↓
23          allow-query     { localhost; internal-network; };
```

・25 行目～に追記　外部のネームサーバに問い合わせを転送する場合。複数ある場合は、以下の様に複数行で記述
　　10.72.1.11 と 10.72.1.3 は HAL の DNS サーバ

```
25forwarders{
2610.72.1.11;
2710.72.1.13;
28 };
```

・最終行に追記

```
71    zone "motobe.com" IN {
72            type master;
73            file "motobe.com.lan";
74            allow-update { none; };
75    };
76
77    zone "73.65.10.in-addr.arpa" IN {
78            type master;
79            file "73.65.10.in-addr.arpa.db";
80            allow-update { none; };
81    };
```

※保存して終了

②内向き正引き(ドメイン名⇒IP アドレス)ゾーンの作成

内向き正引きゾーンファイル(motobe.com.lan)の作成

```
[hal@motobe ~]$ sudo   vi   /var/named/motobe.com.lan
$TTL 86400
@ IN SOA motobe.com. root.motobe.com. (
  2023092501 ; serial
  3600          ; refresh (1 hour)
  900           ; retry (15 minutes)
  604800        ; expire (1 week)
  86400         ; negative (1 day)
)
   IN       NS                  motobe.com.
   IN       MX        10        mail.motobe.com.
   IN       A                   10.65.73.55
mail     IN        A          10.65.73.55
ftp      IN        A          10.65.73.55
file     IN        A          10.65.73.200
print    IN        A          10.65.73.201
www      IN    CNAME      motobe.com.
```

※motobe.com の後の　．(ドット)を忘れないように！

※IN がある行の先頭 3 行には**スペースが絶対に必要**(特に張り付けた方はスペースが消えているので注意)**←★重要！**

※file と print はダミー

※NS レコードはゾーンを管理する DNS サーバを指定します。
※MX レコードはメールの配信先を指定します。(メールサーバの構築で必要となります。)
※A レコードはホストに対する IP アドレスを記載する。
※CNAME レコードは別名でアクセスする場合に指定します。
※空白に注意！コピペだけは上手く行かない時が有りますから、空白だけは TAB キーで空白を入れなおした方が良いかも。　←人によっては TAB キーよりも半角スペースの方が良いかも・・・
※大丈夫と思いますが青字は各自の Linux 設定に直して下さい。

③内向き逆引き(IP アドレス⇒ドメイン名)ゾーンの作成

内向き逆引きゾーンファイル(73.65.10.in-addr.arpa.db)の作成

[hal@motobe ~]$ **sudo　vi　/var/named/73.65.10.in-addr.arpa.db**

```
$TTL 86400
@ IN SOA   motobe.com. root.motobe.com. (
  2023092501 ; serial
  3600       ; refresh (1 hour)
  900        ; retry (15 minutes)
  604800     ; expire (1 week)
  86400      ; negative (1 day)
)
   IN     NS   motobe.com.
55       IN       PTR       motobe.com.
55       IN       PTR       mail.motobe.com.
55       IN       PTR       ftp.motobe.com.
200      IN       PTR       file.motobe.com
201      IN       PTR       print.motobe.com
```

※motobe.com の後の　．(ドット)を忘れないように！　ただし、別の IP の file と print サーバは必要なし。
※IN がある行の先頭行にはスペースが絶対に必要(特に張り付けた方はスペースが消えているので注意)←★重要！
※PTR レコードが IP アドレスからホスト名に変換する為のレコードです。
※空白に注意！コピペだけは上手く行かない時が有りますから、空白だけは TAB キーで空白を入れなおした方が良いかも。　←人によっては TAB キーよりも半角スペースの方が良いかも・・・
※大丈夫と思いますが青字は各自の Linux 設定に直して下さい。

■ゾーンファイルの用語

- TTL(Time To Live)はレコードの生存時間を設定します。
- SOA(Start Of Authority)レコードにはゾーン空間についての権限などの情報を記載します。
- Serial：ゾーン情報のバージョンを管理する。(慣習的に日付+更新分の 2 桁を付ける)
- Refresh：セカンダリサーバがプライマリサーバに更新があったか確認する間隔。

・Retry：上記の問い合わせで応答が得られなかった場合サイド問い合わせる間隔。
・Expire：この時間を越えるとセカンダリサーバはデータを破棄する。
・Minimum：キャッシュサーバが情報を保存する時間。
・NS レコード：ネームサーバを記載する。
・MX レコード：メールサーバを記載する。
・A レコード：ホストに対する IP アドレスを記載する。
・PTR レコード：IP アドレスからホスト名(FQDN)に変換するレコード。

(3)DNS 動作前のネットワークファイル関連の確認

① 名前解決ファイル『hosts』の変更

ホストファイルより、ループバックアドレス(IPv4 は 127.0.0.1、IPv6 は::1)以外を削除(コメント)します。

[hal@motobe ~]$ sudo vi /etc/hosts

```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4   ←IPv4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6   ←IPv6
```

※今回は確認のみ変更なし

※127.0.0.1 はループバックアドレスと言う特別なアドレス

②DNS 参照設定ファイル『resolv.conf』の変更

DNS サーバ指定ファイルの確認

[hal@motobe ~]$ sudo vi /etc/resolv.conf

```
# Generated by NetworkManager
#search OSAKA-NET.nkz.ac.jp com
#nameserver 10.72.1.13
#nameserver 10.72.1.11
search  motobe.com
nameserver  10.65.73.55
```

※学校の設定をコメント化(HAL の設定 2 行目～4 行目が無ければコメント化しなくて構いません)

※『search』は、ショート名(ftp や print)でアクセスされた時、その属性値『motobe.com』を補います。

『nameserver』は、名前解決するサーバを指定します。(即ち、自サーバになります。)

※大丈夫と思いますが青字は各自の Linux 設定に直して下さい。

③順序設定ファイルの変更

名前解決をする順番を hosts ファイル→dns の順に名前解決します。

[hal@motobe ~]$ sudo vi /etc/nsswitch.conf

#84 行目

```
84 hosts:      files dns myhostname          ←変更なし、確認のみ
```

(4)BIND 起動

[hal@motobe ~]$ **sudo systemctl start named** ← DNS サーバー起動
[hal@motobe ~]$ **sudo systemctl enable named** ← DNS サーバー自動起動設定

※「失敗」のエラーが出たらメッセージをよく見て修正！ line～と有ったらその行を見てみる！
※メッセージが出なくて「失敗」のみの時は設定ファイルをもう一度順番に確認。
スペース、ドット、ファイル名等の名前が間違っていませんか？

[hal@motobe ~]$ **sudo systemctl status named**

でエラー内容の確認が出来ます。

◎エラー例

[hal@motobe ~]$ **sudo systemctl start named**
Job for named.service failed because the control process exited with error code. See "**systemctl status named.service**" and "journalctl -xe" for details.←起動エラー

[hal@motobe ~]$ **sudo systemctl status named.service**←エラー内容の確認
● named.service - Berkeley Internet Name Domain (DNS)
Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: disabled)
Active: failed (Result: exit-code) since 月 2021-09-07 05:27:08 JST; 20s ago
Process: 17044 ExecStartPre=/bin/bash -c if [! "$DISABLE_ZONE_CHECKING" == "yes"]; then /usr/sbin/named-checkconf -z "$NAMEDCONF"; else echo "Checking of zone files is disabled"; fi (code=exited, status=1/FAILURE)

9 月 07 05:27:08 motobe.com bash[17044]: **internal/73.65.10.in-addr.arpa/IN: unknown class/type**
9 月 07 05:27:08 motobe.com bash[17044]: zone localhost.localdomain/IN: loaded serial 0
9 月 07 05:27:08 motobe.com bash[17044]: zone localhost/IN: loaded serial 0
9 月 07 05:27:08 motobe.com bash[17044]: zone 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0....al 0
9 月 07 05:27:08 motobe.com bash[17044]: **zone 1.0.0.127.in-addr.arpa/IN: loaded serial** 0
9 月 07 05:27:08 motobe.com bash[17044]: **zone 0.in-addr.arpa/IN: loaded serial 0**
9 月 07 05:27:08 motobe.com systemd[1]: named.service: control process exited, code=exited status=1
9 月 07 05:27:08 motobe.com systemd[1]: Failed to start Berkeley Internet Name Domain (DNS).
9 月 07 05:27:08 motobe.com systemd[1]: Unit named.service entered failed state.
9 月 07 05:27:08 motobe.com systemd[1]: named.service failed.
Hint: Some lines were ellipsized, use -l to show in full.

※上記の例では「**73.65.10.in-addr.arpa**」ファイルにエラーが出ています。
対策としてはもう一度
[hal@motobe ~]$ **sudo vi /var/named/73.65.10.in-addr.arpa.db** を確認

(5)FW への登録

[hal@motobe ~]$ **sudo firewall-cmd --add-service=dns --permanent**
success
[hal@motobe ~]$ **sudo firewall-cmd --reload**
success
[hal@motobe ~]$ **sudo firewall-cmd --zone=public --list-services --permanent**
cockpit dhcpv6-client **dns** http https nfs samba ssh telnet

(6)DNS の動作確認その 1　　Linux 上

・正引き確認

[hal@motobe ~]$ **nslookup motobe.com**　←正引き確認(超重要コマンド)
Server:　　10.65.73.55
Address:　　10.65.73.55#53

・逆引き確認

[hal@motobe ~]$**nslookup 10.65.73.55**　←逆引き確認(超重要コマンド)
55.73.65.10.in-addr.arpa name = mail.motobe.com.
55.73.65.10.in-addr.arpa name = motobe.com.
55.73.65.10.in-addr.arpa name = ftp.motobe.com.
※今回 Linux(10.65.73.55)には DNS、mail、ftp サーバーが同居している為、設定が 3 つ見える

・リダイレクト確認　←自分の Linux(DNS)で名前解決出来ない時

[hal@motobe ~]$**nslookup www.yahoo.co.jp**
Server:　　10.65.73.55
Address:　　10.65.73.55#53

Non-authoritative answer:
www.yahoo.co.jp canonical name = edge12.g.yimg.jp.
Name:　edge12.g.yimg.jp
Address: 182.22.25.124
※HAL の DNS(10.72.1.11、10.72.1.13)にリダイレクトして解決された！

以上！

●「NT43 Linux 資料 27 DNS 設定その 2(10 月 23 日改訂版)」へ続く