Service layering

Integrating Samba with existing DNS infrastructure

SambaXP 2018
June 6th/7th 2018
Pieter Hollants

Pieter who?

Frankfurt, Germany-based developer (Python, C, ...) but also...

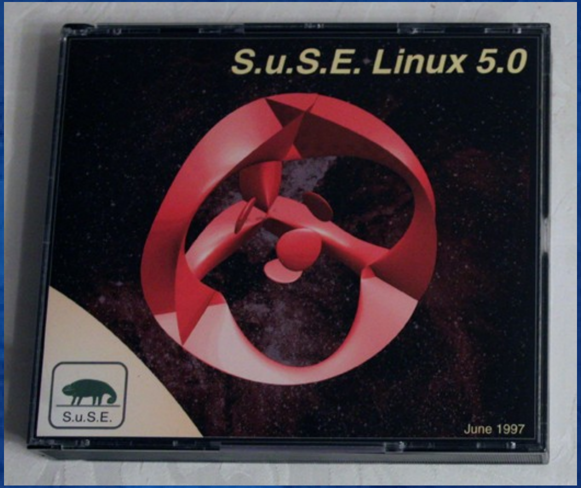
- 3y IT support in Netware/Win 95 times
- 9y (Senior) Intern at SUSE Consulting
- 4y Linux Systems Engineer at German Air Traffic Control (automated installations of high availability-systems, hardware standardization)

...and freelancing since over 15y (dev & admin)

I love Samba and I hate Samba

...for it is lovely if it works but a nightmare to debug.

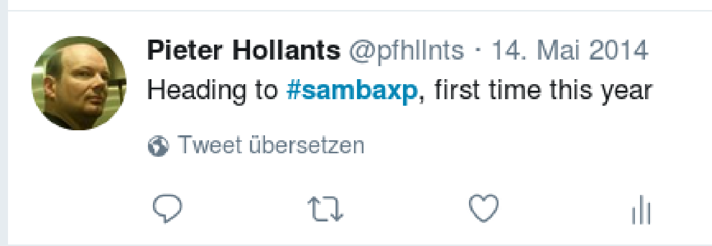
- Using SUSE Linux since 5.0, thus Samba since 2.0.5 (?)
- Not a Samba developer
- Supported small companies with Windows clients, NT4 domain with single PDC, shares, netlogon scripts, printer drivers, OpenLDAP & RFC2307bis fun
- Unfortunately no Samba AD, customers went Windows/Outlook route



cstan.io

Samba community & me

- Always liked cross-plattform approach even if not exactly sexy among puristic Linuxbeards
- No steady member of any community due to continously changing interests & profane requirements such as earning money
- Long been eyeing with sambaXP
- Taking part since 2014 to get closer to community
- Lack of user talks, strong focus on dev topics
- This year got motivated to put my money where my mouth is and submitted talk



Pieter Hollants @pfhllnts · 14. Mai 2014

Heading to #sambaxp, first time this year

SOHO?

London SOHO?

Wikimedia Commons / panoramio.com / joinai; CC

SOHO!

- Well-aged term for *Small Office / Home Office* with 1 to 10 employees
- Typical evolution: Single PC → PCs → Server → NAS → cloud services?
- No IT department
- No (full-time) administrator
- Restrictions on time and budget
- Backups often neglected
- Redundancy unrealistic
- “Cost of failure < cost of mitigation”

Wikimedia Commons / Stubacca; CC-BY-SA

I agree to disagree...

- Got LANs with central device (server/NAS) as central data store facilitating backup
- Improved reliability thanks to
  - distribution of functionality over multiple devices
  - advent of flash-based low voltage devices such as routers, reducing risk of mechanical failures (no hard disks, no fans)
- Price drop for manageable switches, UPSes...

Affordable reliability now a topic in SOHO as well.

Service layering model (1/2)

I like to *model* the no longer so trivial SOHO world and distinguish between

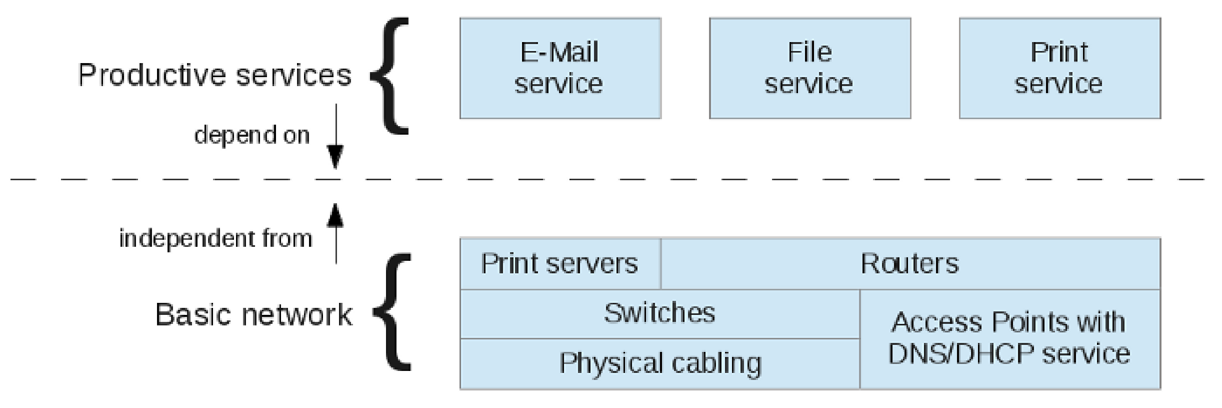
- ➔ *basic network* services (necessary utilities for)
- ➔ *productive* services (provide actual customer value).

Basic network services are independent = Productive services don’t interfere with them.

“If everything above crashes, I still want to be able to surf the Web for troubleshooting purposes.”

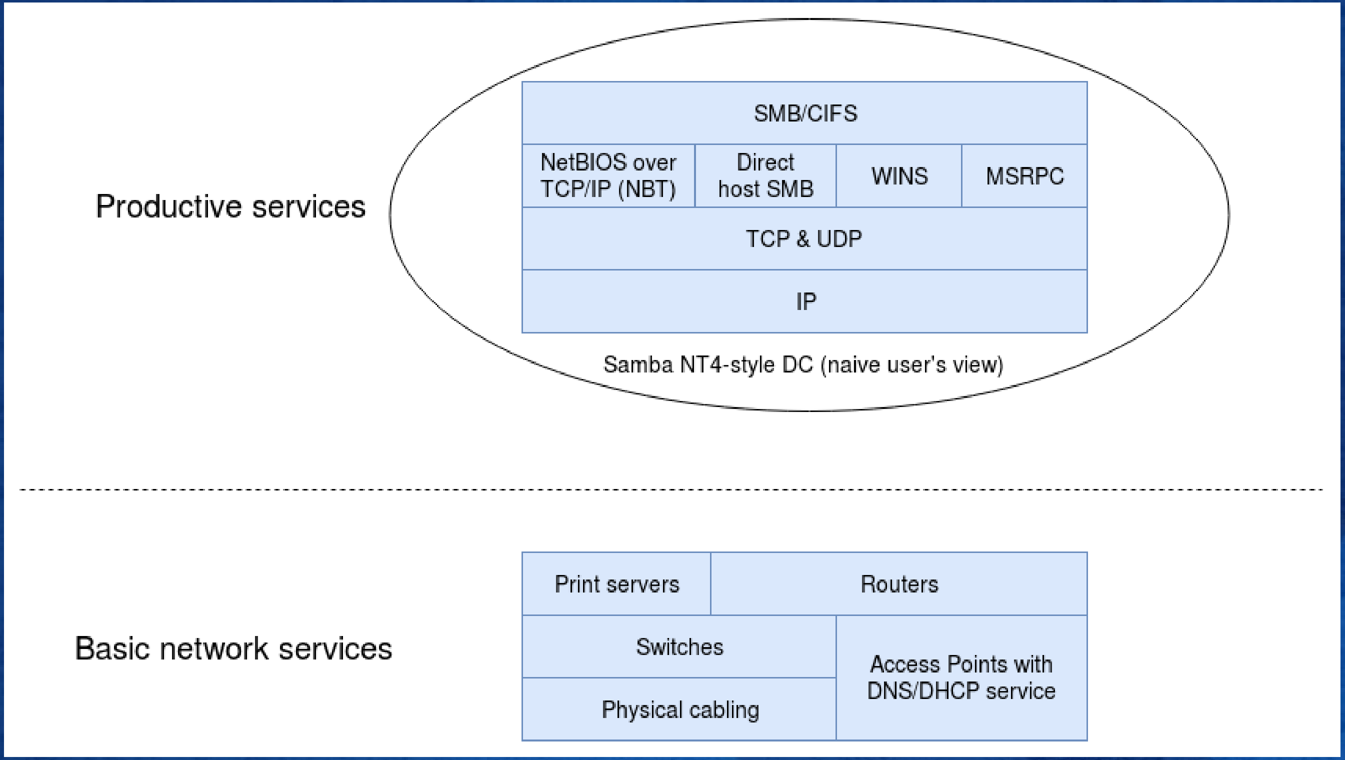
Service layering model (2/2)

- In SOHO DNS & DHCP requirements are easy
- Can be served by dnsmasq running on an embedded OS such as OpenWrt on a flash-based router.



Where would we place Samba?

Samba NT4-style DC



Productive services

SMB/CIFS

NetBIOS over TCP/IP (NBT) | Direct host SMB | WINS | MSRPC

TCP & UDP

IP

Samba NT4-style DC (naive user's view)

Basic network services

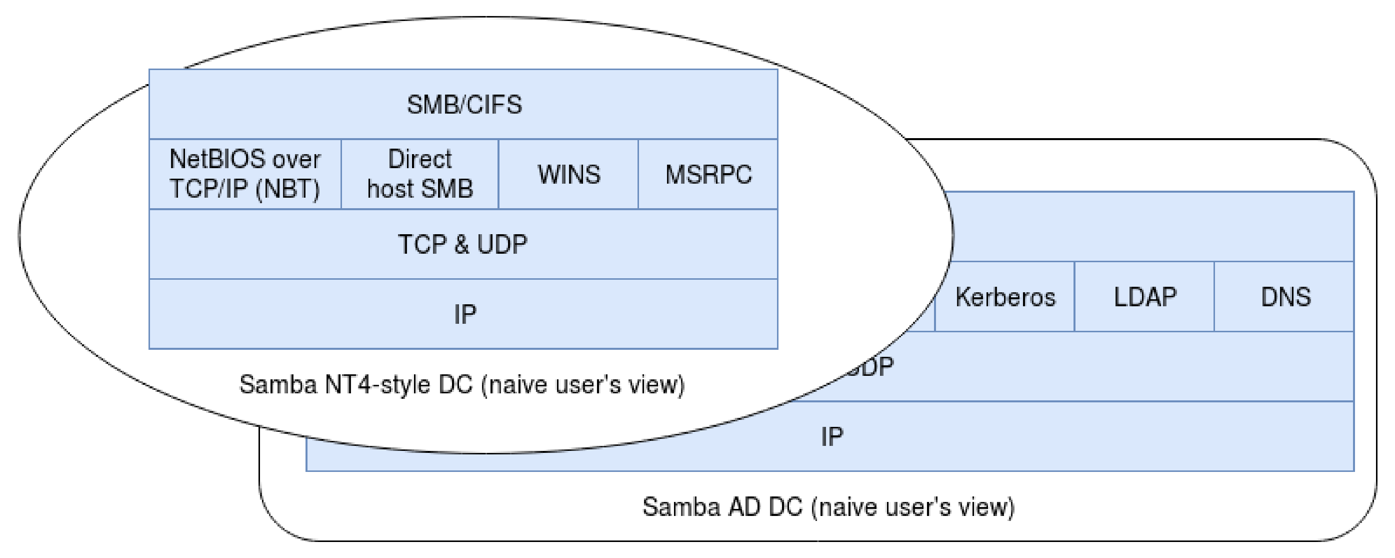
Print servers | Routers

Switches | Access Points with DNS/DHCP service

Physical cabling

- Easy: run nmbd, smbd, winbind, done.
- NetBIOS/WINS runs pretty independent from DNS.
- No interference with basic network services

Samba AD


SMB/CIFS
NetBIOS over TCP/IP (NBT)
Direct host SMB
WINS
MSRPC
TCP & UDP
IP
Samba NT4-style DC (naive user's view)
Kerberos
LDAP
DNS
UDP
IP
Samba AD DC (naive user's view)

Three additional services with tight interdependencies and peculiarities of their own:

- Kerberos
- LDAP
- DNS

AD DNS peculiarities (1/2)

Special requirements for DNS servers:

- ➔ dynamic DNS updates
- ➔ special SRV/A/CNAME records for locating services

DNS servers running on embedded Linux not really well-suited: Kai Blin looked at dnsmasq[1], but dead end.

Could create required records manually[2], but too hackish and unsupported. And still no dynamic DNS updates.

[1] http://lists.thekelleys.org.uk/pipermail/dnsmasq-discuss/2010q1/003554.html
[2] http://edoceo.com/howto/samba4

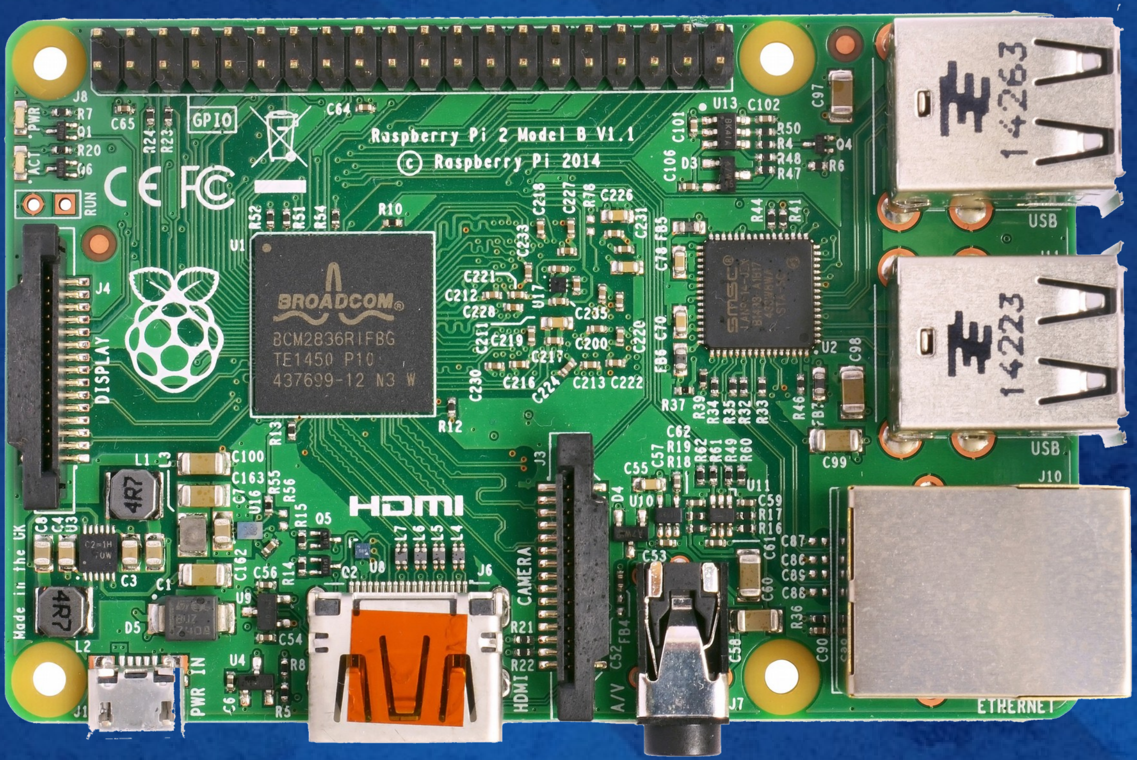
AD DNS peculiarities (2/2)

With dnsmasq out of the game two options:

- Samba-internal DNS server written by Kai Blin (for smaller setups, limited functionality: no caching, no recursive queries, no xfers...)
- Bind9 with DLZ DNS Backend (complex configuration, for larger setups)

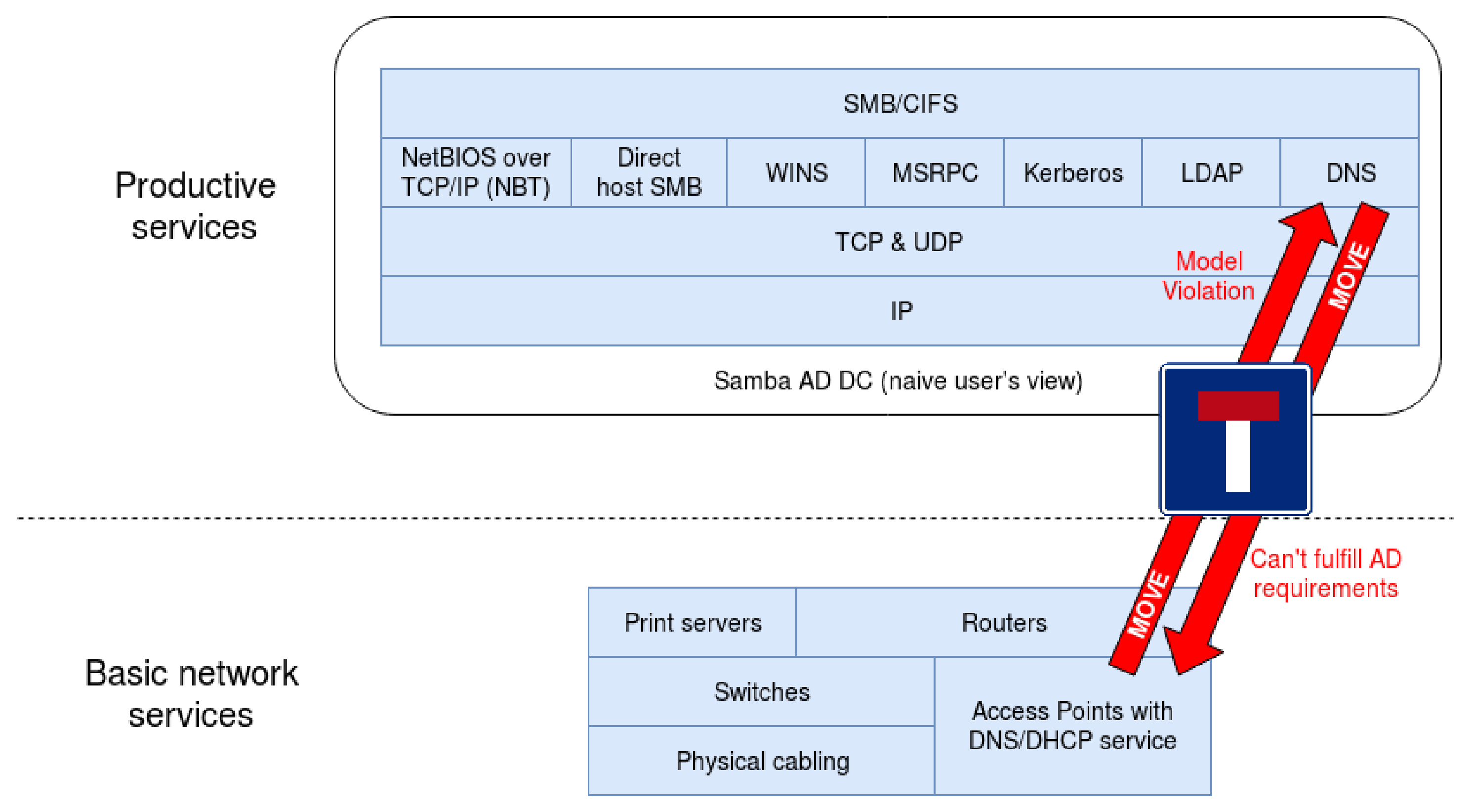
Problem: they (still) don't really run on embedded Linux well, neither Samba nor Bind.

Could use this...



- SD cards not really reliable
- Prefer embedded devices with flash
- Or real hardware...

The problem



- Server with Samba/Bind9 becomes productive service but we said DNS is basic service – model violation!
- (Single) Point of Failure: Samba down, all DNS down

Running both at the same time

a.) Clients talk to Samba, forwarding to dnsmasq

- ➔ Doesn’t solve isolation problem: Samba down → all down!

b.) Primary DNS: Samba (forwarding to dnsmasq)
Secondary DNS: dnsmasq

- ➔ Samba down → timeouts for all!
- ➔ Inconsistent client behavior depending on used DNS server (records available vs. not available)

So what now, Sherlock?

On second thought what we really want is:

- ➔ only AD clients depend on Samba (forwarding to dnsmasq)
- ➔ all other clients depend on dnsmasq only

Because if Samba's DNS is down, so is the rest of Samba and AD clients are affected anyway

However e.g. Linux clients keep working

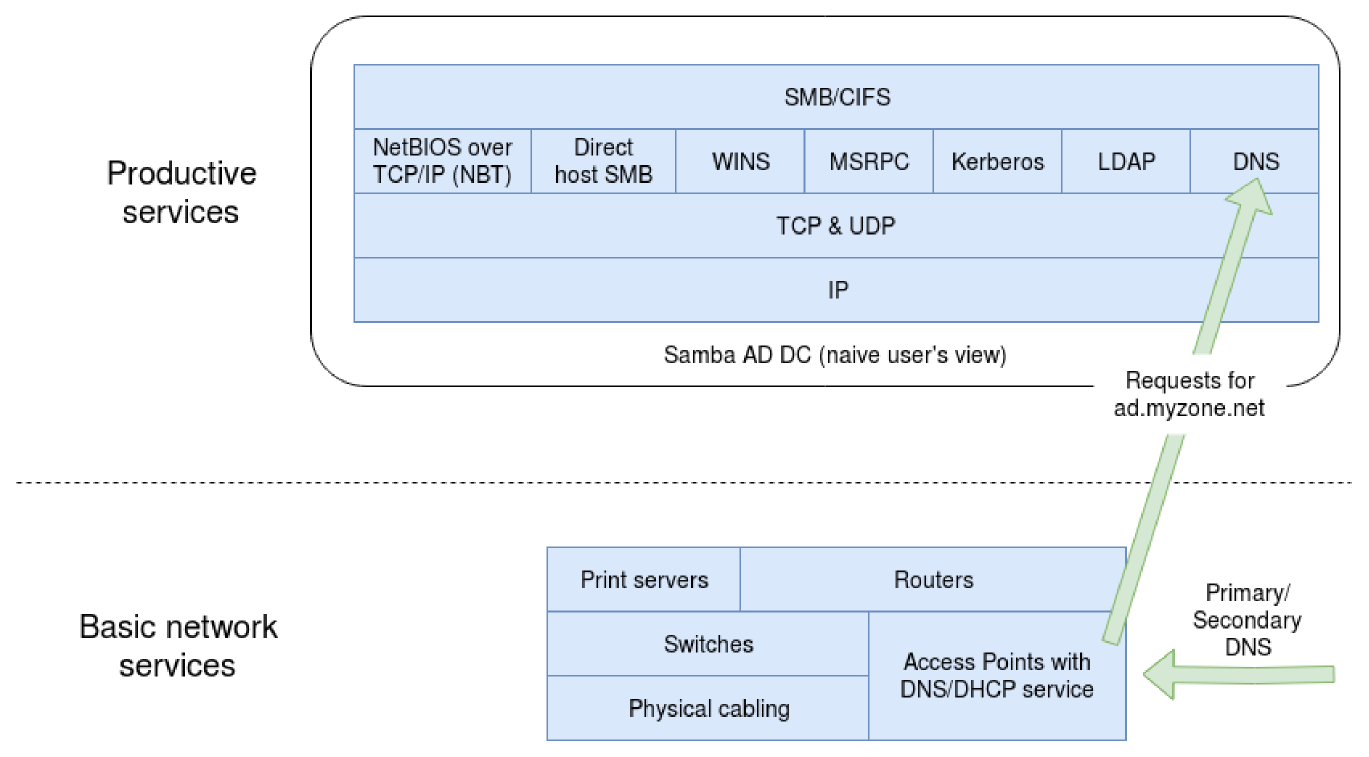
So what now, Sherlock??

Could feed clients different DNS servers via DHCP so they get different “views” on same DNS zone

- ➔ We’d have to replicate dnsmasq records to Samba so it knows “basic” zone records as well
- ➔ Samba’s internal server can’t do that actually
- ➔ Even if it could, dnsmasq certainly can’t

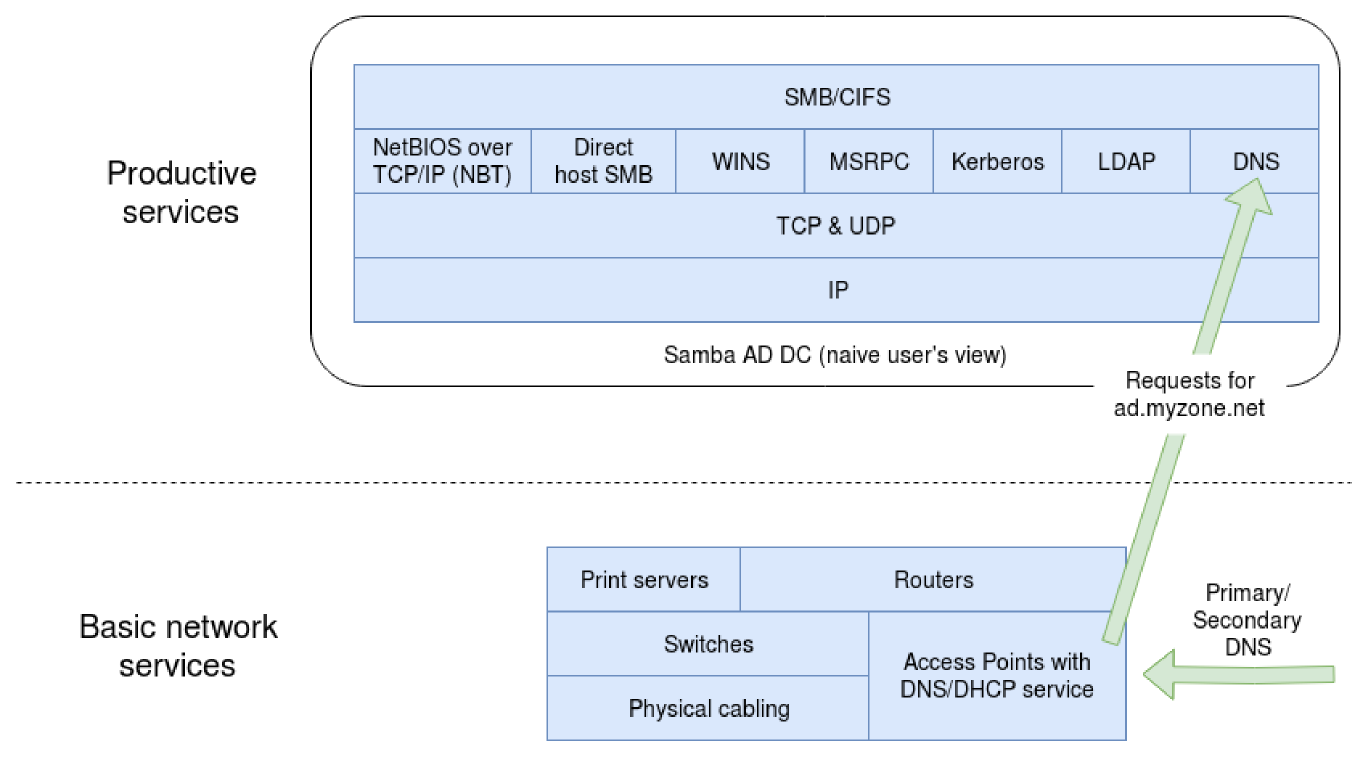
…hey, why don’t we give AD a separate DNS zone? How about subzone?

Enlightenment (1/2)



- dnsmasq stays primary/secondary DNS for all clients
- Configure dnsmasq to forward requests for subzone to Samba (not DNS delegation: no NS records needed)

Enlightenment (2/2)



- DHCP hands out *.ad.myzone.net names to AD clients.
- (Almost) nothing to do with IP subnets: two DNS zones, but still only one IP subnet! (However…)

Forward ever...

So far only addressed *forward* lookups from names to IP addresses.

Perfectly fine to have both

- dnsmasq: myserver.myzone.net A 192.168.0.1
- Samba: myserver.ad.myzone.net A 192.168.0.1

Clients will accept this just happily.

...backward never

But for *reverse* lookup:

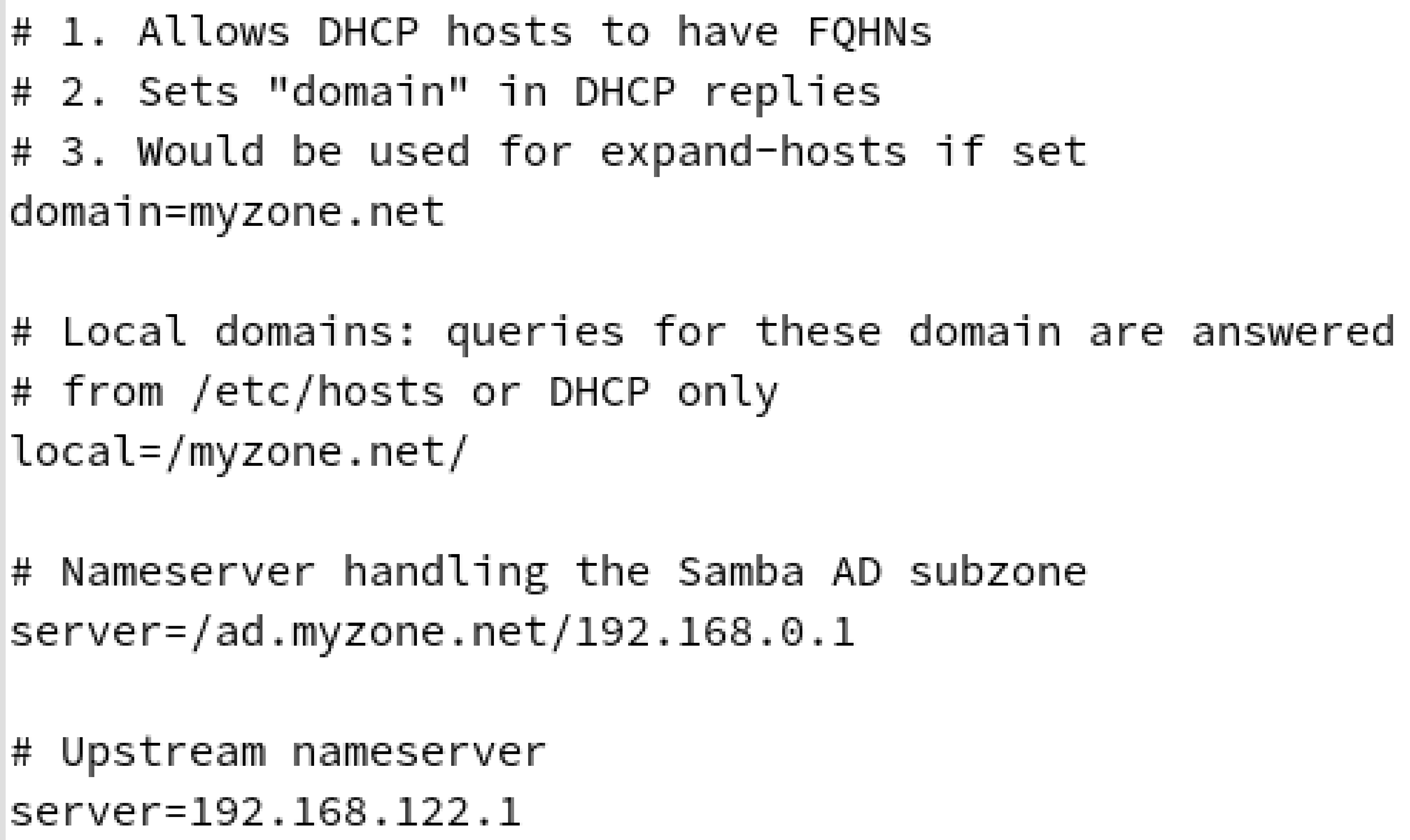
- dnsmasq: 1.0.168.192.in-addr.arpa A myzone.site.net

which means:

ReverseLookup(ForwardLookup(name)) != name

Kerberos may not like that unless one adds `rdns = false` to `/etc/krb5.conf`.

dnsmasq setup (1/2)



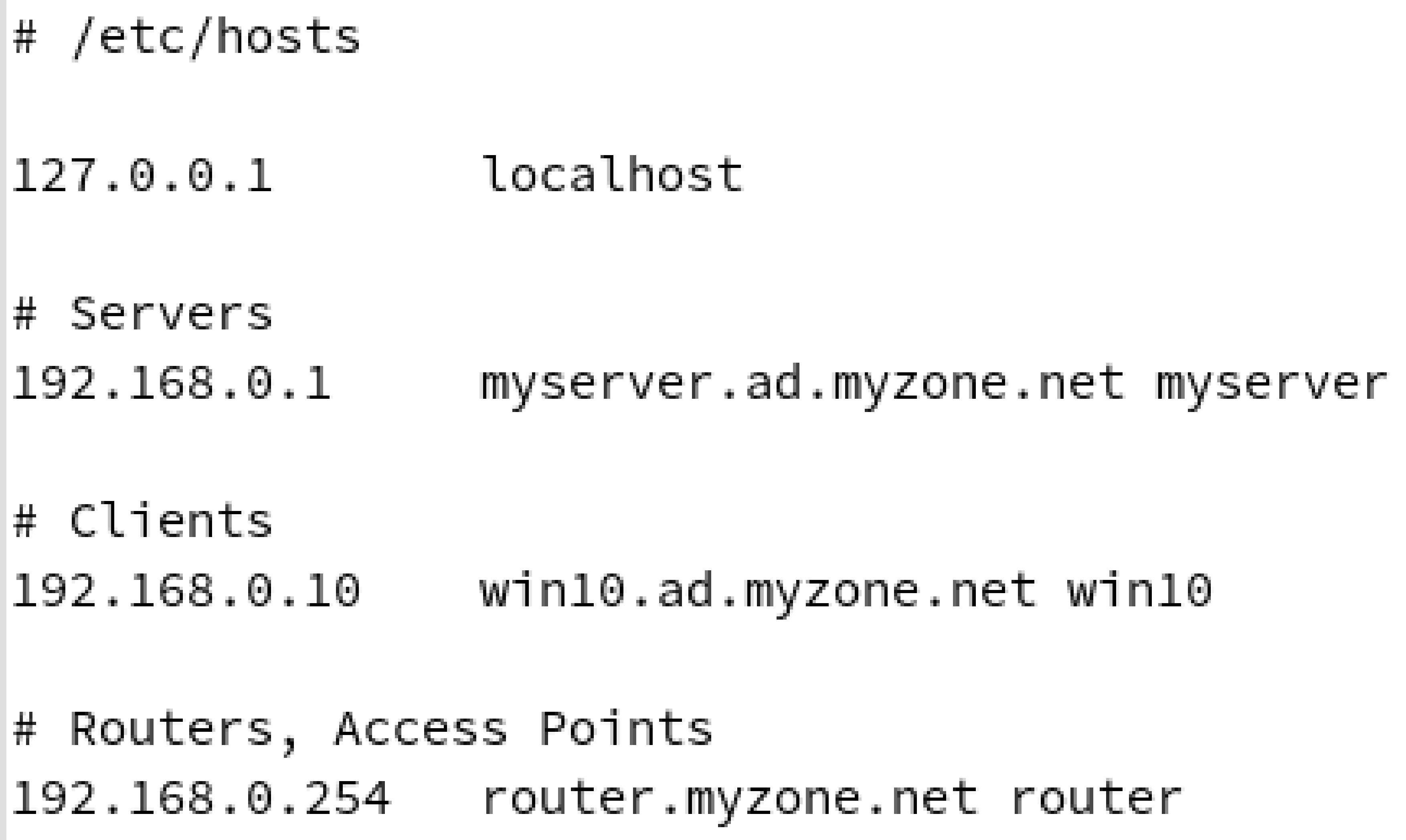
```
# 1. Allows DHCP hosts to have FQHNs
# 2. Sets "domain" in DHCP replies
# 3. Would be used for expand-hosts if set
domain=myzone.net

# Local domains: queries for these domain are answered
# from /etc/hosts or DHCP only
local=/myzone.net/

# Nameserver handling the Samba AD subzone
server=/ad.myzone.net/192.168.0.1

# Upstream nameserver
server=192.168.122.1
```

dnsmasq setup (2/2)



```
# /etc/hosts

127.0.0.1       localhost

# Servers
192.168.0.1     myserver.ad.myzone.net myserver

# Clients
192.168.0.10    win10.ad.myzone.net win10

# Routers, Access Points
192.168.0.254   router.myzone.net router
```

Questions?
Feedback?

Pieter Hollants

@ pieter@hollants.com

pfhllnts