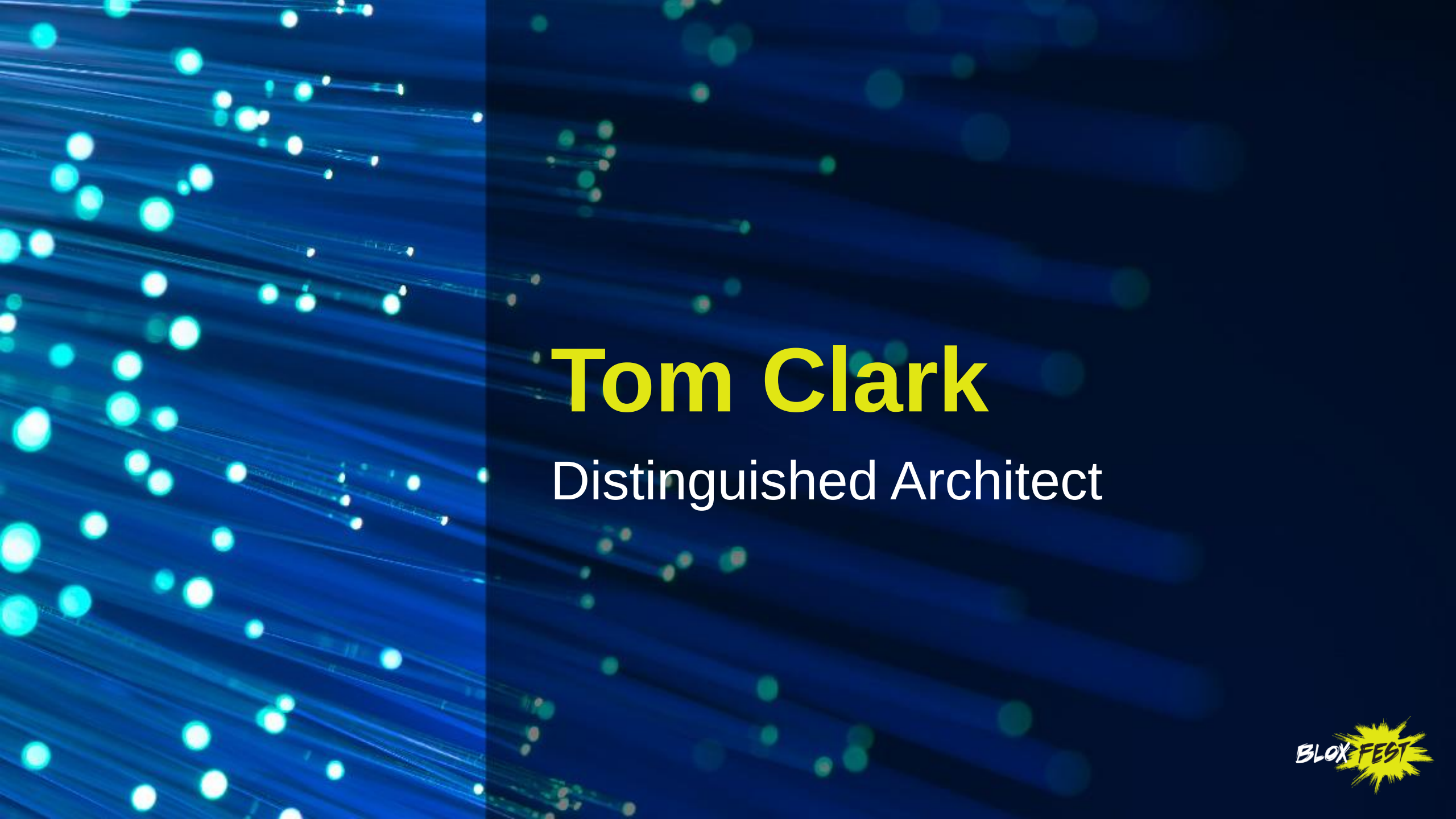
Top Ten Best Practices for a Successful Architecture


Tom Clark
Distinguished Architect
BLOX FEST

Tip #1: Enable Lease Scavenging

- By default, DHCP will allocate a new address for a new client rather than reuse an address from an existing client
- Implication is that over time all addresses in a range will be used, thus creating lots of lease objects. This is especially bad in the case of IPv6 where ranges can be very large
- Fix this by enabling lease scavenging so that old leases are discarded after being unused for some time (client is gone)
- Suggested scavenge time of one week (after expiry)

Tip #2: Enable DNS Scavenging (Manual)

- If DNS records are updated by DHCP, they are automatically removed when the lease expires
- Not always true for records updated directly by the client!
  - They stick around!
- Enabling DNS scavenging can help identify such records (and automatically remove them if so configured)
  - Also useful for static records no longer in use
- Suggest the feature be enabled to only identify the records and allow you to gain confidence before enabling automated removal

Tip #3: Empty the Recycle Bin

- Every time an object is deleted, it goes to the recycle bin
- Recycle bin only emptied on a full NIOS upgrade
- So, it can get quite a number of objects…
- Suggest a monthly cleanup at a time where all is well
  - Review recent items to ensure nothing valuable!

Tip #4: Allocate Enough DHCP Addresses to Survive Failure of an FO Peer

- When both peers are up, they trade addresses to ensure that both have a supply of free addresses for clients
- When a peer fails, its addresses are no longer available unless the peer is placed in “partner down”
- However, if the range is large enough, you don’t have to do that because there will be sufficient addresses at the remaining peer
- So, you can avoid emergency maintenance activity!

Tip #5: Use Anycast for Client-facing Recursion

- Using anycast for client resolver configuration means you can add, remove, and relocate the edge DNS servers without changing the client configuration (in DHCP or otherwise)
- If a server is down, instead of each client needing to time out and try the other one, routing does it for you. Better client experience

Tip #6: Don’t Use Anycast for Authoritative or Second-level Recursion

- However, it doesn’t make sense to use anycast for the case where other name servers are making the decision
- Name servers balance queries based on round-trip-time, which can be thrown off if routing changes

Tip #7: Move R/O API to the GMC

- Often, organizations will have a need to (for example) export all the network definitions to another system
- Doing this on the GM interferes with GUI usage and replication
- Instead, point those API queries over to the GMC
  - Hopefully it is lightly loaded before promotion

Tip #8: Move to REST API

- With the Perl API, you need to update the Perl module each release
  - Also need to manage other Perl modules/versions
    - Crypt:SSLeay, LWP::UserAgent, XML::Parser, Net::INET6Glue, and Perl itself!
- Makes it hard to use the same scripts against multiple grids with different versions
- Using REST avoids all that!
  - curl -k1 -u admin:testpw -X GET https://192.168.1.2/wapi/v2.2/network
    - Gets all the networks just like that!

Tip #9: Tune Up Your DHCP

- Re-evaluate your lease times
  - “Oh yeah, we set that extra low for our migration two years ago”
- Disable “update on renew”
  - Causes a lot of load and doesn’t really address a real issue
  - Also might be left over from a migration
- Consider having DHCP perform DNS updates, not the client
  - DHCP always cleans up when the lease expires, more “real time”
  - More secure compared to unsecured (no GSS-TSIG) client updates
  - Depend on a few DHCP servers to get it right, not thousands of clients

Tip #10: Use Query Capture, Not Query Logging

- Much lower performance impact
- Can save limited amount on appliance disk, or unlimited on off-box storage
- Can capture either queries or responses

- Tip #10A: If you have reporting, use it for lease history rather than the legacy lease history feature


BLOX FEST
Infoblox