InkBridge Networks

July 20, 2026

DNS for Internet Service Providers

White Paper

By Alan DeKok

Learn how InkBridgeDNS solves a specific ISP operational challenge: providing controlled access to DHCP lease data via standard DNS queries. This technical paper explains how DNS queries eliminate the need to build custom REST APIs for exporting customer and device information to carrier partners, monitoring systems, and compliance platforms.

DISCLAIMER
The information in this document is confidential, and is Copyright © 2024 InkBridge Networks. All Rights Reserved.

The information in this document are based on the current knowledge of InkBridge Networks. We reserve the right to withdraw or change the contents of this document at any time. We accept no responsibility should any damages be caused to a person, persons, device, devices, or organization as a result of the use that is made of information provided in, or taken from, this documentation or as a result of reliance on the information in this documentation.

Contents

1. Executive Summary 3
2. The DNS use case for ISPs 4
3. Why ISPs don't always need full-featured DNS 7
4. The advantages of convergence 9
5. Compliance and monitoring applications 10
6. Policy capabilities beyond standard DNS 11
7. Deploying and integrating 12
8. When to consider InkBridgeDNS 13
9. Technical specifications for InkBridgeDNS 14
10. Conclusion 15

Copyright © 2024 InkBridge Networks. All Rights Reserved

1. Executive Summary

You've deployed high-performance DHCP that handles millions of addresses. Now you need to answer the question: "Which customer has this IP address right now?"

InkBridgeDNS is a straightforward DNS server. Its main purpose is to export DHCP lease data via standard DNS queries, without requiring custom API development or integration complexity. External systems can query your DNS server using protocols they already understand ,and get back the customer or device information which you've configured it to export.

This export can solve specific ISP requirements about abuse complaint handling, carrier partner integration, lawful intercept compliance, and network monitoring.

The only limitationis that the InkBridgeDNS solution is targeted to ISPs. While it implements the most important portions of the DNS protocol, it is not intended to be part of a full-featured IP address management system.

Copyright © 2024 InkBridge Networks. All Rights Reserved

InkBridge Networks

2. The DNS use case for ISPs

ISPs with hundreds of thousands or millions of customers face a recurring operational challenge.

- Someone at IP address 203.0.113.42 triggers an abuse complaint.
- A carrier partner needs to identify which subscriber has a particular address for billing correlation.
- Law enforcement issues a lawful intercept request.
- Your monitoring system needs to associate traffic patterns with customer identifiers.

You have this information. It's in your DHCP database. The question is how to provide controlled access to it.

Traditional approaches and their problems

Custom REST API: Requires documentation, authentication infrastructure, client library development, and ongoing maintenance. Integration takes weeks or months. Every new partner or system requires custom development work.

File exports: Not real-time. Batch processes introduce delays. Integration partners must parse custom formats. Data can become stale between export cycles.

Direct database access: Creates security risks. Locks partners into your schema. Requires managing database credentials. Provides too much access to underlying systems.

InkBridgeDNS approach: We export DHCP lease information via standard DNS queries. Anyone who needs access queries DNS using protocols they already understand. No custom development is required.

Exporting data via DNS means that this information is independent of any underlying database! Are leases stored in MySQL, PostGreSQL, Redis, or LDAP? InkBridgeDNS can read them all. It doesn't even matter what database schema you are using, InkBridgeDNS requires only minor changes to read almost any database, or any schema.

Real-world example: Medical devices with cellular network connectivity

A medical device company deploys health monitors (blood sugar, blood pressure) with embedded cell connectivity. Each monitor gets an IP address via DHCP. The monitor transmits patient data to cloud services through a mobile carrier.

Copyright © 2024 InkBridge Networks. All Rights Reserved

InkBridge Networks

When carriers need to identify which customer account is associated with a particular monitor for billing or support purposes, they query InkBridgeDNS. The system returns the customer identifier tied to that IP address at that moment.

In this scenario, there is no custom API required. The systems are already on the Internet, so there are no privacy issues. The inter-company integration is simplified because the carrier's existing systems already know how to query DNS.

How it works

Here's the technical flow for querying DNS.

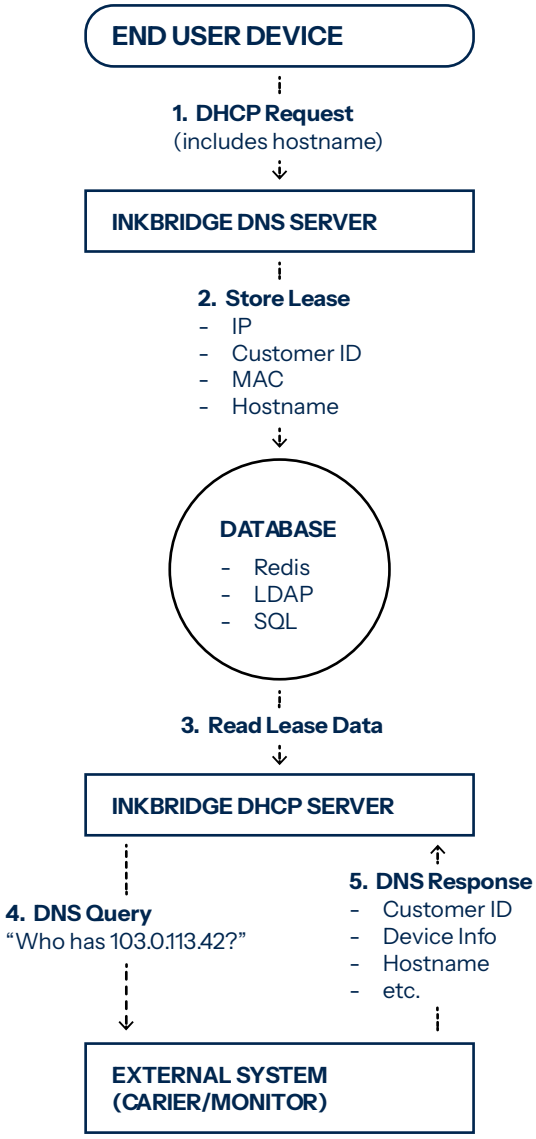
1. DHCP assigns an IP address to a device and captures the hostname from the DHCP packet (e.g., "device-12345.customer.isp.com").
2. Lease information is stored in your database (Redis, LDAP, MySQL, PostgreSQL, or others).
3. DNS server reads from the same database.
4. External system queries: "What's at 203.0.113.42?".
5. DNS returns: customer identifier, device MAC address, hostname, or whatever other information that you've configured it to export.

Note that due to the complex policy language, it is easy to filter DNS queries based on source address. So if a supported partner asks about a MAC address, InkBridgeDNS can return an answer. If an unknown source asks the same question, InkBridgeDNS instead replies with no information. These policies give you flexibility, security, and simplicity.

The DNS server and DHCP server share the same data store and there is no synchronisation required. The information is always up to date in real-time.

Copyright © 2024 InkBridge Networks. All Rights Reserved

InkBridge DNS Technical Flow



KEY BENEFITS

- Real-time data
- No synchronisation delays
- Standard DNS protocol
- No custom API needed
- Shared database

DHCP and DNS servers query the same database - no data synchronisation required

What gets exported

You control exactly what information DNS returns:

- Customer identifiers (maintaining appropriate privacy levels)
- Device MAC addresses
- Hostname information from DHCP packets
- Custom information based on your requirements
    - When the system also uses RADIUS for authentication, the InkBridgeDNS product can even return RADIUS accounting information in DNS!

Responses can be policy-driven. Internal monitoring systems might receive full device details, while carrier partners receive only customer IDs. Different queries can return different information based on your business rules.

Database Integration

InkBridgeDNS is database agnostic. It works with:

- MySQL
- PostgreSQL
- Redis
- LDAP (Active Directory, OpenLDAP)
- Oracle
- Microsoft SQL Server
- Any database with standard query interfaces

If you're already using InkBridgeDHCP, the DNS component uses the same databases. You do not need to maintain separate data stores or migrate schemas.

Copyright © 2024 InkBridge Networks. All Rights Reserved

3. Why ISPs don't always need full-featured DNS

ISPs and enterprises manage IP addresses fundamentally differently, which affects their DNS requirements.

ISP address management:

- Pool-based allocation: "There are a million users, we have a million IPs. Give one of the users an IP, I don't care which one."
- Minimal static address requirements
- Customer identity tracked via RADIUS Accounting.
- No DNS-based device naming schemes required.

Enterprise address management:

- Individual assignments: "This person wants her laptop to have the same address."
- Static IPs for printers, servers, conference rooms.
- DNS names tied to specific devices: chris-laptop.company.com.
- Integration with Active Directory for device management
- RADIUS is rarely used, and RADIUS accounting is even more rarely used.

For ISPs, RADIUS Accounting already records when customers connect and disconnect, and all customer session information lives in the RADIUS Accounting database. ISPs therefore don't need don't need complex address management platforms designed for enterprises. There is no need to use a complicated GUI to track and assign IP addresses across different departments. If an IP address is free, it is allocated to the next available user.

Why DNSSEC, DNS over HTTP, and DNS over TLS aren't required for this use case

Those protocols provide cryptographic validation that DNS responses haven't been tampered with. They can be useful for public-facing DNS services where you're serving records to untrusted parties across the internet. They can also be useful for individual subscribers, so that their DNS queries are kept private.

For ISPs exporting DHCP lease data:

- You're not serving public DNS records.
- Querying systems are your own infrastructure or trusted partners.
- Data comes directly from your authoritative DHCP system.
- Queries typically happen over private networks or VPNs.
- The threat model doesn't require cryptographic validation.

Copyright © 2024 InkBridge Networks. All Rights Reserved

If an attacker has compromised your internal network to the point where they can intercept DNS queries between your systems, DNSSEC won't solve your problem. Your security focus should be on network segmentation and access controls.

What about DDI/IPAM platforms?

DDI (DNS, DHCP, IPAM - IP Address Management) platforms are designed for enterprises that need to manage static address assignments. These platforms excel at scenarios where:

- Individual users request specific IP addresses.
- Devices need consistent DNS names (the printer is always printer-3rd-floor.company.com).
- IT staff manually assign and track address allocations.
- Active Directory integration drives device naming.

ISPs don't have these requirements. Dynamic IP address pools handle millions of customers without manual management. So a DDI platform solves an enterprise problem that ISPs just don't have.

Performance considerations

Many commercial DNS vendors put a strong emphasis on performance: "hundreds of thousands of queries per second!" That capability is necessary for public-facing recursive resolvers handling queries from millions of internet users. It's less useful in pretty much every other situation.

For exporting DHCP lease data to your own systems and carrier partners, you need a far lower query volume. InkBridgeDNS handles the query rates that ISPs actually encounter for this use case without the complexity and cost of high-end DNS infrastructure optimised for public internet services. While we don't do hundreds of thousands of queries a second, we can easily do tens of thousands of queries a second, all the while enforcing complex policies.

4. The advantages of convergence

Infrastructure convergence refers to reducing the number of separate products and vendors in your network by using integrated solutions that work together natively.

Instead of purchasing DHCP from one vendor, DNS from another, and RADIUS from a third, convergence means using a single vendor whose products share databases, configurations, and support infrastructure. The goal is to reduce integration complexity and operational overhead.

Convergence reduces the complexity of assembling infrastructure from multiple vendors. If you bought boxes from five different companies, you would spend enormous amounts of time gluing them all together.

Each integration requires custom development. Configuration changes in one system must be manually replicated to others. When something breaks, troubleshooting spans multiple vendor support teams.

With integrated DHCP and DNS from the same vendor:

- Configuration changes to DHCP pools are automatically reflected in DNS exports
- Manual synchronisation of data between systems is not needed
- You have a single support relationship for the entire stack
- Troubleshooting is simplified when one team maintains related components

Convergence also gives you database flexibility. Commercial DNS solutions typically require you to use their database schema. Migrating your existing data to their systems means adapting your processes to their requirements. Proprietary schemas create vendor lock-in.

InkBridgeDNS works with your existing database infrastructure and schema:

- No forced migration to vendor-specific databases
- Queries can be trivially customized, and are not hard-coded
- You can mix and match data sources (LDAP for static data, Redis for dynamic leases)
- No software updates are required to handle new DHCP options

When you need to export a new piece of information, you can make a simple change. There are no code changes required, and you don't have to wait for a vendor release cycle.

Copyright © 2024 InkBridge Networks. All Rights Reserved

5. Compliance and monitoring applications

When someone at IP address 203.0.113.42 sends spam, posts copyrighted material, or triggers a security incident, you need to identify them quickly.

Common compliance scenarios:

- DMCA copyright infringement notices
- Spam complaints from other ISPs
- Security incidents requiring customer notification
- Lawful intercept requests from law enforcement

With DNS export, the process is straightforward: query the IP address, receive the customer identifier you've configured to export. You don't have to build authentication into a custom API or grant database access to external systems.

For lawful intercept specifically, you can provide law enforcement with a DNS query interface that returns only the information they're authorised to access, without exposing your full customer database.

Standard network monitoring tools can query DNS to correlate network behaviour with customer information:

- Traffic analysis tools identify unusual patterns from specific addresses.
- Security systems associate attack traffic with customer accounts.
- Capacity planning correlates usage patterns with customer segments.
- Carrier partners track data usage for shared infrastructure.

Because these tools already understand DNS queries, integration is trivial and there's no need for custom plugins or API client development.

In terms of privacy, you control exactly what information gets exported. For privacy compliance:

- Export customer IDs without exposing names, addresses, or payment information.
- Provide device identifiers without personally identifiable details.
- Return only the minimum information required for each use case.
- Implement geographic or regulatory-based query restrictions via policies.

The principle is that you provide enough information to solve operational problems without exposing sensitive customer data unnecessarily.

Copyright © 2024 InkBridge Networks. All Rights Reserved

InkBridge Networks

6. Policy capabilities beyond standard DNS

Traditional DNS servers typically return the same answer to every query for a given name. InkBridge DNS supports policy-driven responses based on:

- Who's querying (source IP address or network)
- What they're querying (address range, customer type)
- Time of day or other contextual factors
- Almost any custom business logic

Example policies: Internal monitoring systems querying from 10.0.0.0/8 receive full device details:

- Customer ID
- Device MAC address
- Hostname
- Gateway information
- Lease start time

Carrier partners querying from their networks receive limited information:

- Customer ID only
- Lease status (active/expired)

Abuse complaint systems querying specific address ranges receive:

- Customer contact identifier
- Service tier
- Account status

Policies are defined in a simple policy language. The same policy engine that handles RADIUS and DHCP applies to DNS queries, so there is only one policy language across all protocols!

Adding a new policy or modifying existing ones doesn't require code changes or software upgrades. Update the configuration, and the DNS server applies the new rules.

7. Deploying and integrating

You have two main options for InkBridgeDNS architecture:

- **Integrated deployment (most common):** DNS server runs on the same systems as DHCP. Both components query the same database. This is the simplest deployment for most ISPs.
- **Separated deployment:** DNS servers run independently, querying the same database as DHCP. Useful when you need to isolate DNS queries from DHCP processing for security or performance reasons.

Both architectures scale horizontally. Add more DHCP servers to handle more lease assignments. Add more DNS servers to handle more queries. They all read from the same distributed database (Redis Cluster, replicated SQL, etc.).

DNS queries eliminate the need to document REST APIs, build authentication infrastructure, or develop custom integration code. The protocol is standard, well-understood, and supported by every system. Integration happens in minutes because there's nothing custom to explain or implement.

Here's what it means when you use DNS queries for lease data export:

For carrier partners: They already have DNS client libraries in their systems. Point them at your DNS server. Provide documentation on what hostnames to query. Integration complete.

For monitoring tools: Most monitoring systems have built-in DNS query capabilities. Configure them to query your DNS server for IP address information. You don't need a custom plugin.

For compliance systems: Standard DNS resolver libraries exist for every programming language. A few lines of code queries your DNS server and parses the response.

Compare this to building a custom REST API:

- Write API specification.
- Implement authentication (OAuth, API keys, etc.).
- Develop client libraries or provide detailed integration documentation.
- Handle API versioning.
- Maintain backwards compatibility as requirements change.
- Debug custom integration issues with each partner.

With DNS, you're using a protocol that's been stable for decades. Every system knows how to query DNS. There are no custom integration issues because there's no custom code.

Copyright © 2024 InkBridge Networks. All Rights Reserved

8. When to consider InkBridgeDNS

You likely need InkBridgeDNS if one or more of the following apply:

- You're exporting DHCP lease data to external systems (carriers, monitoring tools, compliance platforms).
- You face compliance requirements for customer identification (abuse complaints, lawful intercept).
- You want to avoid building and maintaining custom APIs.
- You need policy-driven control over what information different systems can access.
- You're looking to reduce the number of vendors in your infrastructure.

Key decision questions

Do external systems need to query "who has this IP address?"
If yes, DNS provides the most straightforward integration path.

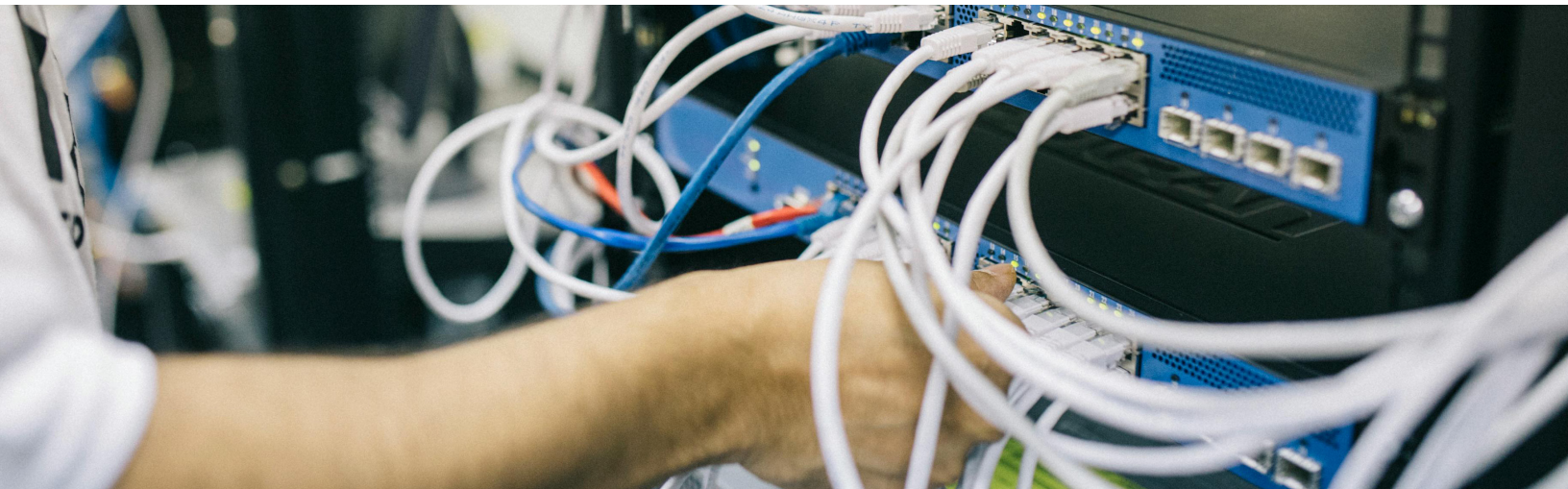
Are you building a custom API to expose this data?
Consider whether DNS queries would accomplish the same goal with less development effort.

Do different requesters need different information?
Policy-driven DNS can return appropriate data to each requester without multiple APIs.

Are you already using or evaluating InkBridgeDHCP?
DNS integration uses the same database infrastructure with minimal additional complexity.

You don't need InkBridgeDNS if:

- You're managing enterprise address assignments with static IPs tied to specific devices.
- You need DNSSEC for public-facing DNS services.
- You require DNS over TLS/HTTPS for encrypted queries.
- You're looking for a general-purpose authoritative name server.
- Your use case is recursive resolution for end users.



9. Technical specifications for InkBridgeDNS

Common supported DNS record types

- **A records:** IPv4 address lookups
- **AAAA records:** IPv6 address lookups
- **PTR records:** Reverse DNS (IP to name)
- **TXT records:** Custom text information export

Additional record types can be added via configuration without software upgrades.

Database support

- MySQL
- PostgreSQL
- Redis (including Redis Cluster)
- LDAP (OpenLDAP, Active Directory)
- Oracle
- Microsoft SQL Server
- MongoDB
- IBM DB2

Custom database integration is possible for databases with standard query interfaces.

Performance characteristics

Query performance depends on your database backend. Typical performance:

- Redis: Sub-millisecond query response
- MySQL/PostgreSQL with proper indexing: Single-digit milliseconds
- LDAP: 10-50ms depending on directory server load

For ISP lease data export use cases, these response times are more than adequate.

You're not handling millions of queries per second from public internet users. You're handling periodic queries from monitoring systems and carrier partners.

Deployment requirements

- Runs on commodity x86_64 hardware
- Linux operating system (Ubuntu, CentOS, RedHat)
- Network access to database backend
- Minimal CPU and memory requirements (scales with query volume)

InkBridgeDNS can be deployed on the same servers as DHCP or on dedicated systems depending on your architecture preferences.

Copyright © 2024 InkBridge Networks. All Rights Reserved

InkBridge Networks

10. Conclusion

InkBridgeDNS solves a specific ISP operational problem: providing controlled access to DHCP lease data via standard protocols.

Instead of building custom APIs with authentication infrastructure and client libraries, you export data via DNS queries. Integration with carrier partners, monitoring systems, and compliance platforms becomes trivial because every system already knows how to query DNS.

The practical outcome: integration measured in minutes instead of months. Standard protocols instead of custom development. One vendor for your high-performance DHCP and DNS export requirements.

For ISPs that need to answer “who has this IP address?” queries efficiently and securely, DNS provides the most straightforward solution.

About InkBridge Networks

InkBridge Networks engineers, supports, and installs foundational network solutions for authentication and network security. The core team founded and continues to maintain the open-source FreeRADIUS Project, the world’s most popular RADIUS server, supporting hundreds of millions of users every day.

InkBridge Networks provides solutions engineering, support packages, consulting, and training optimised for mid-size to large enterprises, internet service providers, and universities.

For more information:
info@inkbridge.io
www.inkbridgenetworks.com

Copyright © 2024 InkBridge Networks. All Rights Reserved

InkBridge Networks