infoblox | NETWORKComputing

Why DDI? Top 3 reasons to integrate DNS, DHCP, and IP Address Management in Your Network

Why the rapid shift to DDI?

For years, IT managers have used separate tools for the 3 core elements of network infrastructure.

DNS (Domain Name System) matches easy-to-remember names to computer addresses.

Without it, devices can't connect with any network or internet location.

DHCP (Dynamic Host Configuration Protocol) delivers IP addresses to every device on the network.

Without IP addresses, devices can't communicate.

IPAM (IP Address Management) assigns and resolves IP addresses to machines.

Without it, you can't plan, track, or manage IP address space used in a network.

But the network landscape has evolved rapidly, becoming more distributed, dynamic, and complex.

- Hybrid and multi-cloud are on the rise
- Workforces have become more distributed
- Businesses have embraced IoT

This new landscape has created new challenges for networking professionals.

Incomplete Visibility

- No authoritative, real-time view of asset library

Limited Automation

- Silos and manual configurations increase errors and outages

Inadequate Control

- Inability to enforce security
- Management overhead

The solution is DDI:
A single solution and common platform integrating the management of DNS, DHCP, and IPAM.

Top 3 Benefits of DDI

1. Full Visibility

- Rich contextual data eliminates security gaps
- Centralized reporting for auditing, compliance, performance, analytics

2. Stronger Workflow Automation

- Increase the speed of innovation
- Eliminate misconfiguration outages
- Enable consistency and scalability

3. Seamless Control

- Significantly reduce inefficient handoffs between silos
- Eliminate errors and save time and money
- Improved user experience

Ultimately, adopting DDI will create more network reliability, enterprise-wide visibility, and stronger security monitoring and response capabilities.

reduction of time for collecting device inventory

reduction in configuration errors

reduced time spent on troubleshooting outages caused by DNS and DHCP[1]

6 Steps to Adopting DDI

1. **Choose the Right DDI Solution**
   Select a DDI solution that aligns with the specific requirements and scale of your network.
2. **Assess and Plan**
   Conduct a thorough network infrastructure assessment, including existing DDI configurations. Develop a detailed migration plan to transition to the integrated DDI solution.
3. **Pilot Deployment**
   Before a full-scale deployment, pilot the solution in a controlled environment to identify and address potential issues and enable a smooth transition.
4. **Data Migration**
   Migrate existing data from separate DDI systems to the integrated DDI platform to maintain continuity and preserve historical network information.
5. **Configuration and Testing**
   Configure the integrated DDI solution according to network requirements. Thoroughly test the system to ensure that DNS resolution, DHCP lease assignments, and IP address management are functioning as expected.
6. **Training and Documentation**
   Train administrators and staff on the integrated DDI solution using comprehensive documentation to facilitate ongoing management and troubleshooting.

Get the Full Report ›

Why DDI? Why is it Important to Integrate DNS, DHCP, and IP Address Management in Your Network

1. Tolly Report, Infoblox Authoritative IPAM for DNS and DHCP, 2022