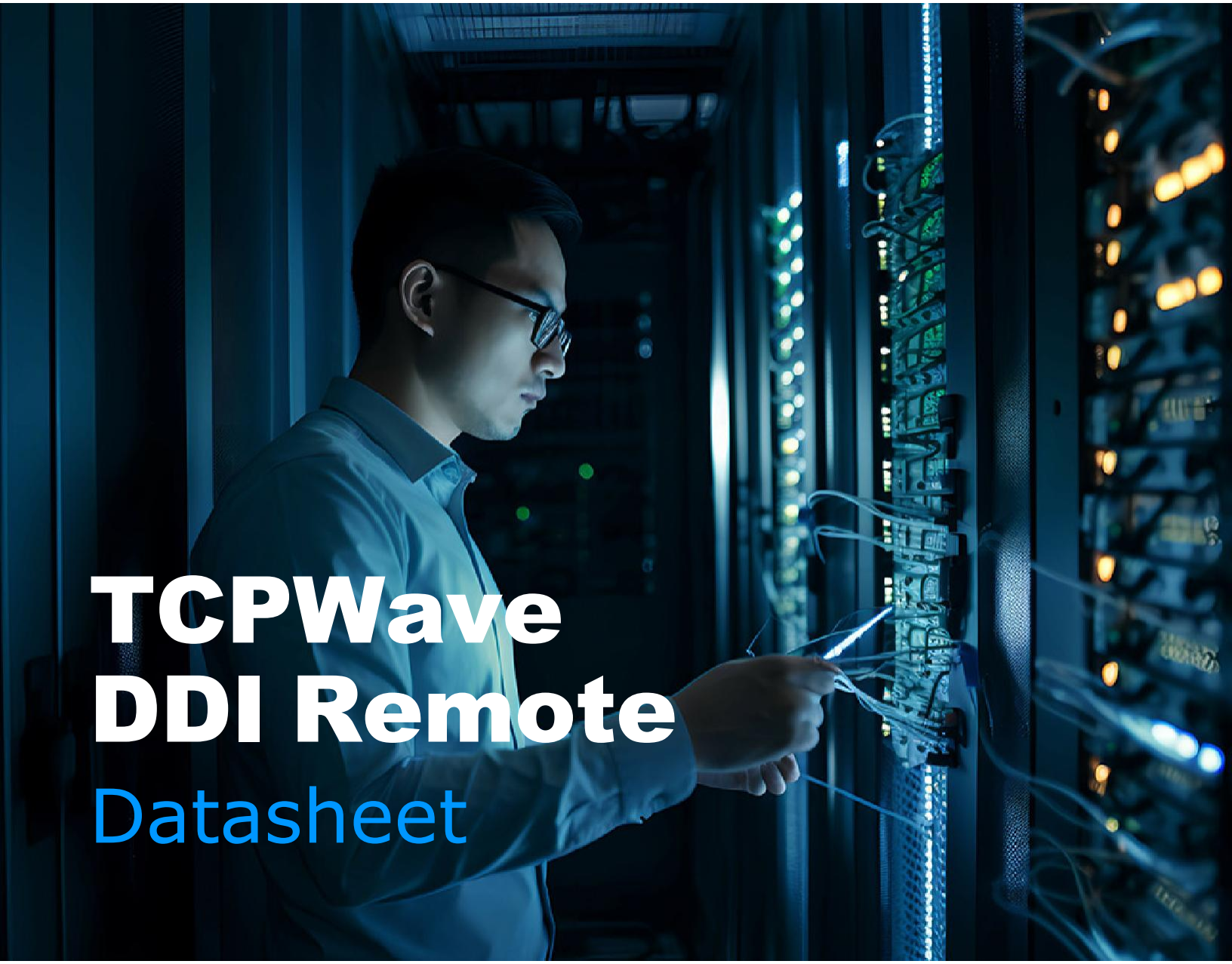
TCPWave
Secure, Smart, and Scalable Networks



TCPWave DDI Remote Datasheet

Overview

TCPWave DDI Remote leverages the power of ISC DHCP and KEA engines to deliver robust and efficient DHCP (Dynamic Host Configuration Protocol) services. These engines are renowned in the industry for their reliability, performance, and rich feature set, making them ideal choices for managing IP address allocation in diverse network environments.

ISC DHCP Engine

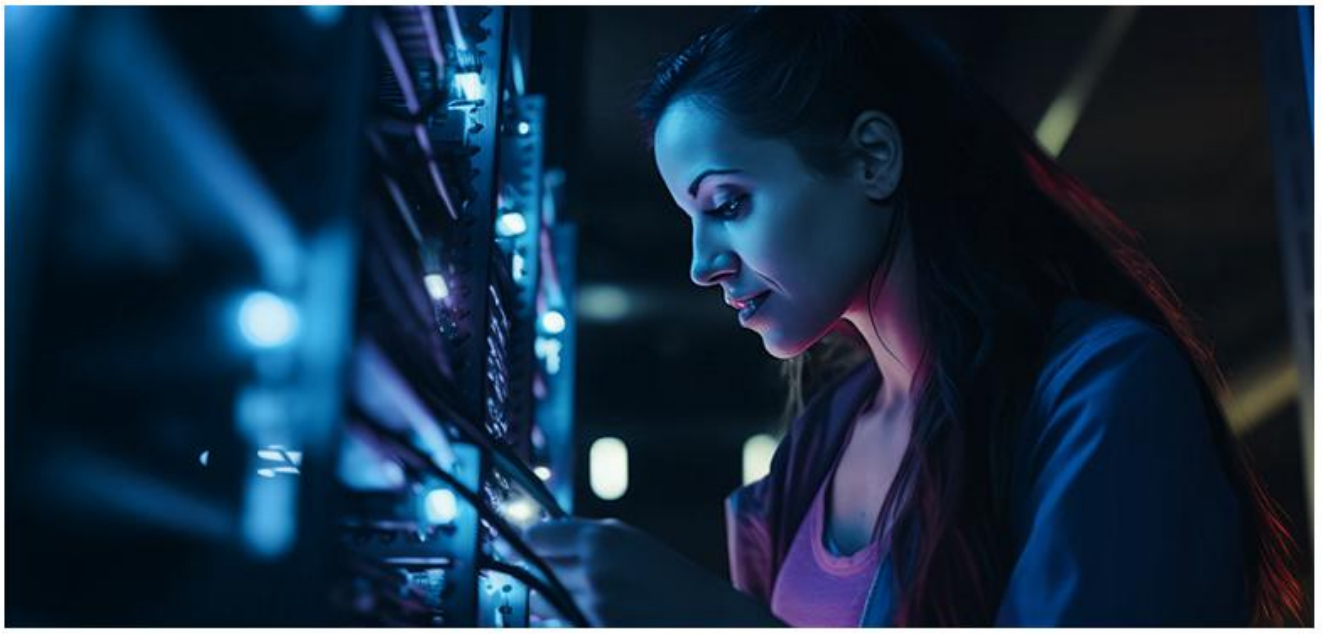
The ISC DHCP (Internet Systems Consortium DHCP) engine is a widely used solution known for its stability and flexibility. It supports dynamic address assignment, lease management, and configuration options customization, catering to various network requirements. ISC DHCP is highly scalable, capable of handling large-scale deployments with ease while maintaining efficient resource utilization.

KEA DHCP Engine

The KEA DHCP engine is a modern, high-performance DHCP server developed by the Internet Systems Consortium (ISC). Designed with performance and scalability in mind, KEA offers advanced features such as dynamic lease allocation, prefix delegation, and flexible configuration management. KEA is optimized for modern network architectures and supports IPv4 and IPv6 address assignment, ensuring seamless integration into heterogeneous network environments.

DHCP Failover

In addition to offering DHCP services powered by ISC and KEA engines, TCPWave DDI Remote provides robust DHCP failover capabilities to ensure high availability and fault tolerance in DHCP service delivery. DHCP failover mechanisms enable automatic failover between primary and secondary DHCP servers, ensuring uninterrupted service availability in the event of server failures or network disruptions.



Key features of DHCP failover in TCPWave DDI Remote Include:

1 Redundant DHCP Server Configuration

Administrators can configure multiple DHCP servers in redundant pairs, with both servers acting as the active-active. DHCP failover configuration ensures that both servers are synchronized and capable of serving DHCP requests, minimizing service disruptions and downtime.

2 Automatic Failover Detection

TCPWave DDI Remote continuously monitors the availability and health of DHCP servers, automatically detecting failures or network partitions. In the event of a primary server failure, the secondary server seamlessly takes over DHCP service delivery, ensuring uninterrupted IP address allocation and lease management.

3 Load Balancing and Load Sharing

DHCP failover mechanisms support load balancing and load sharing between primary and secondary servers, distributing DHCP requests evenly across available server resources. Load balancing optimizes resource utilization and enhances DHCP service performance, ensuring efficient handling of client requests even under high load conditions.

DNS

TCPWave DDI Remote harnesses the capabilities of BIND, NSD, and Unbound engines to provide robust DNS (Domain Name System) services. These engines are industry-leading solutions known for their reliability, performance, and extensive feature sets, ensuring efficient domain name resolution and authoritative name serving.

- **Authoritative DNS Appliance**

  TCPWave offer authoritative DNS appliance for hosting authoritative zone data, available in two flavors: ISC BIND and NSD authoritative. With our solutions, you can easily manage your authoritative DNS data, ensuring it is always up to date and accessible.

- **Cache DNS Appliance**

  TCPWave's cache DNS appliance enables you to perform recursive lookups with ease, available in two flavors: ISC BIND cache and Unbound cache. With our solutions, you can ensure high performance and reliability for your DNS queries.

- **Dual DNS**

  TCPWave offer ISC's BIND, Unbound, and NSD DNS flavors preloaded with our remote appliance package. After configuration, they work in sync, ensuring continuous DNS operations, even during DNS attacks or physical failures.

- **Stealth DNS Master**

  Our stealth DNS master keeps your master DNS appliance hidden from the DNS infrastructure, protecting your DNS data. The authoritative DNS appliances visible on the network function as DNS slaves, ensuring your DNS zones are not writable.

- **Master-Slave**

  We ensure high availability and continuity of DNS services by configuring multiple authoritative DNS appliances as master or slave. This is done by allowing a single DNS zone to serve multiple appliances, resulting in a comprehensive DNS resiliency solution for organizations.

TCPWave DNS Anycast

TCPWave DNS Anycast, when integrated with routing protocols such as BGP (Border Gateway Protocol), VRRP (Virtual Router Redundancy Protocol), IS-IS (Intermediate System to Intermediate System), and OSPF (Open Shortest Path First), enhances the efficiency, resilience, and scalability of DNS service delivery. By leveraging these routing protocols, TCPWave optimizes DNS resolution, improves network performance, and ensures high availability of DNS services across distributed network environments.

TCPWave DNS Security

- TCPWave DNS employs a robust security model to safeguard against various DNS-related threats. It encompasses features such as DNSSEC (Domain Name System Security Extensions) for data integrity and authentication, DNS firewalling to filter malicious traffic, and anomaly detection to identify suspicious activities.
- TCPWave also supports Zeek & Suricata which provides IDS & IPS support.
- It also supports encryption protocols like DNS over TLS (DoT) and DNS over HTTPS (DoH) to protect DNS queries and responses from eavesdropping and tampering. With comprehensive threat intelligence integration and real-time monitoring capabilities, TCPWave DNS ensures the integrity, confidentiality, and availability of DNS services, safeguarding against DNS-based attacks and ensuring secure and reliable domain name resolution for users and applications.

TCPWave NTP

TCPWave NTP (Network Time Protocol) services offer accurate and reliable time synchronization across distributed network environments. NTP is essential for ensuring consistent timekeeping across devices, applications, and systems, which is critical for various network operations, including authentication, logging, and event correlation.