DATACOM

DMCLOUD

CLOUD NETWORK MANAGEMENT SYSTEM

DATASHEET

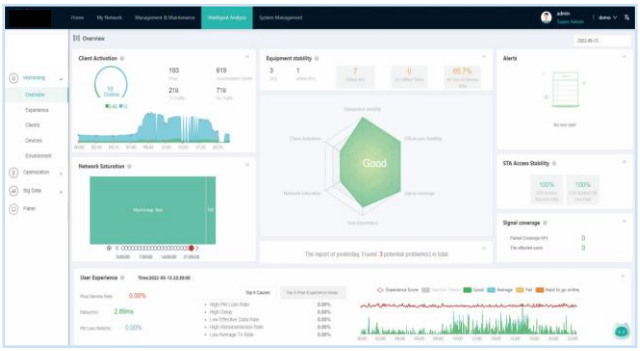
March/2026 rev00

WHAT IS DMCLOUD

The DmCloud solution provides full-lifecycle intelligent network services, covering network planning, deployment, operation, and maintenance. Based on big data, cloud computing, and AI technologies, it improves the efficiency of network construction and operation, maintenance and management of enterprises and partners, and facilitates the digital transformation of enterprises.

DEVICE STABILITY

More than 100 rule-based expert systems automatically check for abnormal devices that go online/offline, as well as configuration and version errors.



SIGNAL COVERAGE

Regardless of changes in the environment, the risk of network signal insufficiency is analyzed based on the connection records of the network terminal.

CONNECTION STABILITY

Wireless access success rate, abnormal disconnection, and roaming errors are detected.

USER EXPERIENCE

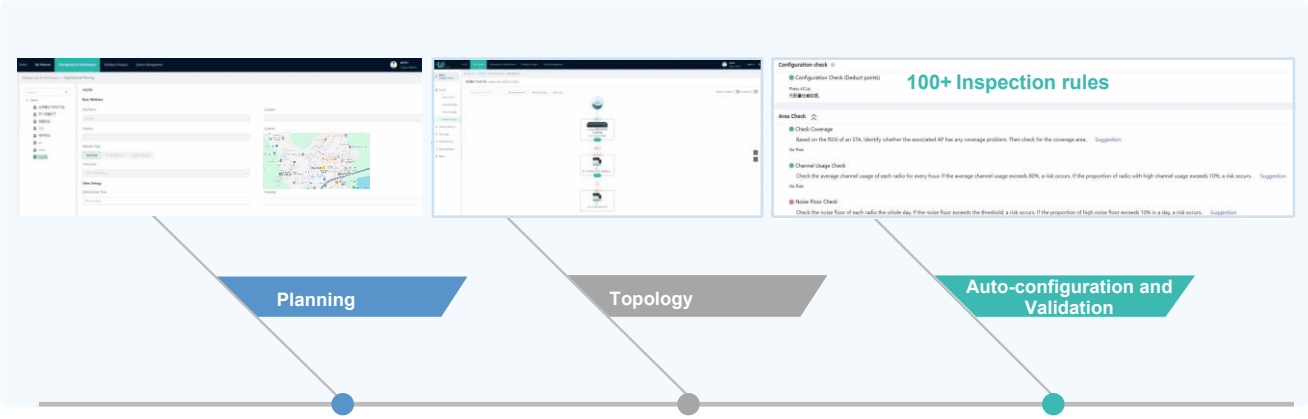
Based on delay, packet loss, signal strength, channel utilization, and other indicators, through millions of supervised AI training groups, the endpoint experience is rated as smooth, good, or poor.

TERMINAL ACTIVITY/NETWORK SATURATION

Risks that require network expansion are analyzed based on current user activity and saturation of network resources.

LIFE CYCLE

PLANNING AND DEPLOYMENT



Planning and design of IT management architecture and network configuration on the cloud platform

Automatic device discovery and network topology generation on the cloud platform

Automatic configuration delivery and deployment deployment on the cloud platform

OPERATION AND MAINTENANCE

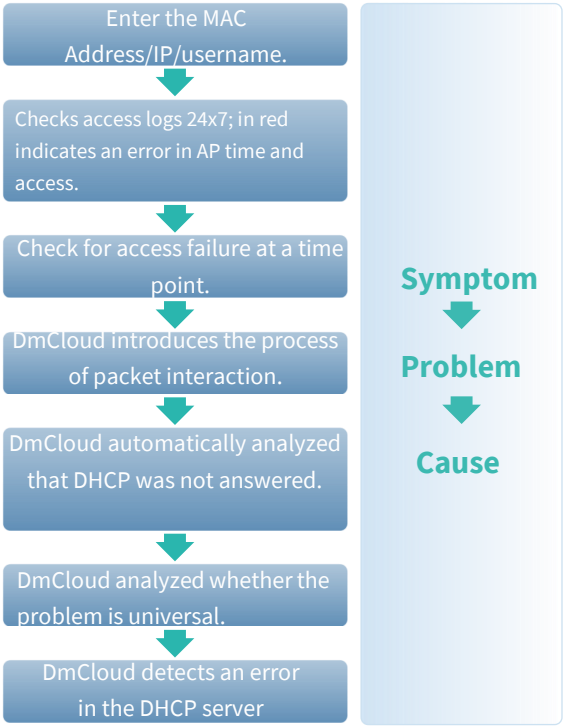
Detailing

Global perspective > regional perspective > individual perspective of the PC > individual perspective of the terminal

From the five dimensions of coverage, interference, roaming, access and authentication, existing problems are analyzed and suggestions are provided.

Root cause analysis

In a wireless environment, a problem may occur due to a weak signal, low rate, and interference. The factor analysis algorithm deduces the root cause of a problem symptom.



CLOUD INTELLIGENCE

OPTIMIZATION AND ROAMING

Network Optimization

Selection of Scenarios

DmCloud offers different network optimization solutions for varied scenarios, such as high-density offices, warehouses, event venues, and outdoor environments.

Optimization global

The user groups the APs in different scenarios. DmCloud then automatically analyzes and generates optimization plans, provides the configuration, and presents the network effects before and after optimization.

Protection in Real-time

Cloud and edge devices connect for real-time monitoring, on-premises optimization, and the ideal solution.

- Real-time monitoring of AP errors and active interference prevention
- Real-time monitoring of endpoint roaming and active prevention

Smart Roaming

Prediction low signal

The alignment of data, including terminal signal, delay, and packet loss, predicts the potential risk of poor quality terminals.

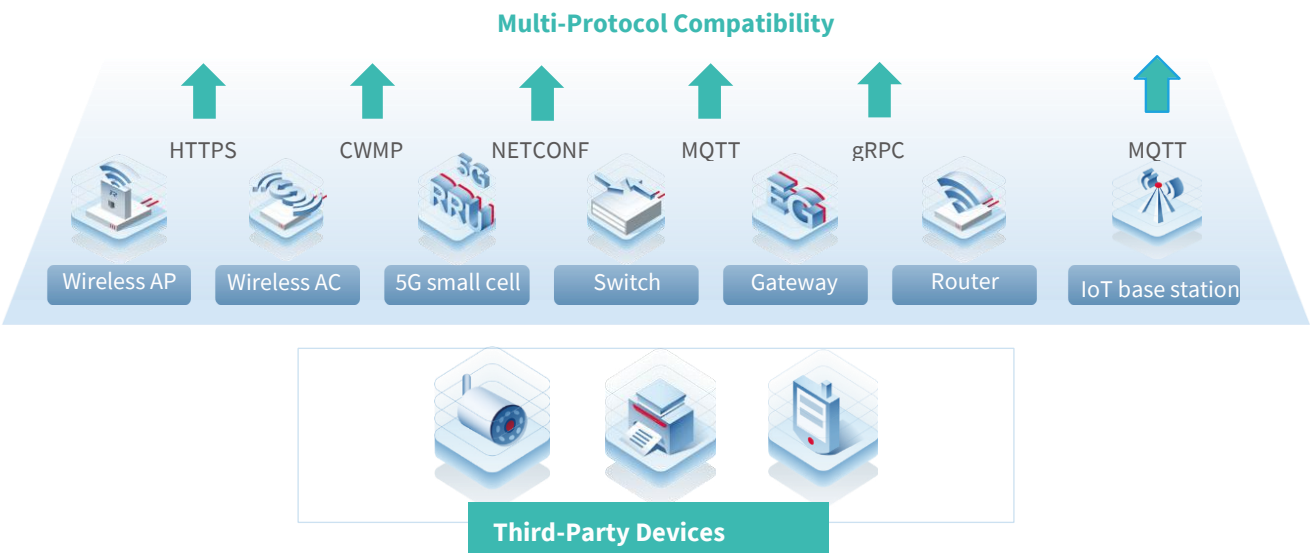
Induction Lossless

When a terminal is at risk of receiving low-quality signals, the Neighbor AI Radio will monitor in real-time for better choices and attempt to induce roaming in a way that the terminal does not notice, so that the terminal can connect to a better AP in advance.

Ongoing Closed loop

The roaming induction log of all terminals will always be uploaded to DmCloud for comparison and analysis before and after induction, and the process can be viewed and continuous improvement can be achieved.

INTER-WAN ACCESS PLATFORM



KEY FEATURES

PLANNING AND CONFIGURATION

Organizational Planning:

- Management of the network's organizational structure, including creating, editing, and deleting branches and sites.
- Unlimited amount of managed devices
- Support for more than 5,000 users.
- Batch import of site information from a CSV file.
- Tree view of the network hierarchy.
- Search and filter websites by name.
- Set a project as the default to open automatically when you log in.
- Transfer a project to another user.
- Manage project users, including assigning permissions and deleting accounts.

Simulation and Coverage Planning:

- Import of floor plans for accurate simulation of the environment.
- Drawing obstacles on floor plans, such as walls and furniture, to simulate the impact on signal coverage.
- Definition of materials, thicknesses and colors of obstacles.
- Virtual positioning of access points (APs) on floor plans.
- Simulation of Wi-Fi signal propagation considering obstacles and construction materials.
- Floor plan scale adjustment for greater simulation accuracy.
- Visualization of the signal simulation at different intensity levels.
- Generation of detailed coverage planning reports with heat maps and AP placement recommendations.

Wireless Configuration:

- Creating, editing, and deleting configuration profiles for wireless networks (SSIDs).
- Setting radio parameters such as channel, bandwidth (20MHz, 40MHz, 80MHz, 160Mhz) and transmit power.
- Wireless security configuration, including encryption modes (WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK, WPA2-ENTERPRISE, WPA3, WAP/WAP2-PPSK) and authentication (PSK, 802.1X).
- PPSK support.
- Data rate limit setting for individual users or for all users in an SSID.
- Advanced options such as preferred 5G and SSID hiding.
- Linking configuration templates to specific sites.
- Delivery of configurations to AP devices in real-time or scheduled.
- Support for creating CAPWAP tunnels to the APs.

Configuration Tools:

- Management via WEB interface
- Access to equipment via SSH.
- Creation and management of CLI command sets for advanced configuration of network devices.
- Applying CLI command sets to individual devices, groups of devices, or entire sites.
- CLI configuration delivery modes: incremental (additional commands) or full overwrite (config.txt file override).
- Scheduling CLI configuration tasks.
- Backup and restore device settings.
- Debugging CLI commands for troubleshooting.
- SNMPv1/v2/v3 support

MONITORING AND OPTIMIZATION

AP Monitoring:

- Real-time monitoring of AP status, including connectivity, CPU and memory utilization, traffic, and channel utilization.
- Viewing detailed information about each AP, such as model, firmware version, MAC address, and number of connected clients.
- Alerts and notifications in case of failures or performance issues in APs.
- Generation of AP performance reports with graphs and statistics.
- Reboot and update APs remotely.

Customer Monitoring:

- Real-time view of clients connected to the Wi-Fi network, including information about the device, MAC address, signal, data rate, connection time, and connected SSID.
- Tracking of clients' connection and roaming history, with information about the APs they have connected to and the signal quality on each connection.
- Identifying clients with connectivity or performance issues, such as low data rate, high packet loss, or authentication issues.
- Generation of customer analytics reports, including information on data usage, connection time, and user experience.
- Tagging VIP clients for priority monitoring.

- Detecting clients with abnormal behavior, such as excessive roaming or repeated association attempts.
- View client exception statistics such as access, disconnect, packet loss, latency, roaming, and repeat association exceptions.

Radio Optimization:

- Automatic optimization of AP channels and transmit power to minimize interference and maximize Wi-Fi network performance.
- Manual optimization option for fine-tuning radio parameters, such as selecting specific channels and adjusting transmit power individually.
- Scheduling radio optimization tasks to run automatically at specific times.
- View radio optimization reports with details about the changes made, such as the new channels and power levels assigned to each AP.
- Channel customization for radio optimization, allowing the definition of specific channels to be used.

Roaming Optimization:

- DmCloud manages access point roaming according to 802.11k/v/r standards.
- Analysis of the roaming behavior of clients on the Wi-Fi network, including roaming time, the number of roaming events, and the quality of the signal during roaming.
- Identification of roaming problems, such as stickiness to an AP even with a weak signal and remote association to a distant AP.
- Automatic or manual adjustment of roaming parameters, such as the RSSI threshold for AP switching, to improve the user experience.
- View roaming optimization reports with details about the changes made and the impact on the user experience.

Switch Monitoring:

- Real-time monitoring of switch status, including connectivity, port utilization, active VLANs, and interface errors.
- View detailed information about each switch, such as model, firmware version, MAC address, and number of ports.
- Alerts and notifications in case of failures or performance problems in switches.
- Generation of switch performance reports.

SECURITY AND ACCESS

Role-Based Access Control (RBAC):

- Creation of roles with different levels of permission to manage user access to the platform, such as administrator, operator or viewer.
- Assigning roles to individual users or groups of users.
- Restricting access to platform features and functionality based on assigned roles, such as accessing network settings, monitoring devices, or generating reports.
- Centralized management of permissions and roles, allowing administrators to control access granularly.

Visitor Authentication:

- Customizable captive portal for guest user authentication, with options to customize the login page, logo, terms of use, and welcome messages.

- Support for different authentication methods, including:
    - **SMS:** sending a verification code by SMS to the user's cell phone.
    - **Voucher:** authentication through a prepaid or system-generated code.
    - **Social Networks:** authentication using social network accounts such as Facebook and Instagram.
    - **One-click login:** Simplified authentication with a single click.
- Voucher management, including code generation, setting expiration, duration, traffic limit, and usage tracking.
- Integration with social networks for simplified authentication, allowing users to connect to the network using their social network accounts.
- Configuration of authentication pages, including login page, authentication page, authentication success page, announcements, and notifications.
- Configuration of authentication policies, such as MAB authentication, authentication required after a number of days or after each connection.
- Timeout setting to force the user to go offline after a period of time.
- Adding authenticated devices and applying the authentication policy to other sites.

White / Black List:

- Creation of whitelisted or blacklisted devices based on MAC addresses or OUI (unique organizational identifier).
- Black/white list enforcement, preventing them from connecting to the Wi-Fi network.
- Allow access only to whitelisted devices, ensuring that only authorized devices can connect.
- Adding devices to the black/white list based on individual MAC addresses or MAC address ranges (OUI).
- Centralized black/whitelist management, allowing administrators to control access granularly across the network.
- Option to synchronize black/whitelist settings with network devices such as access controllers (CAs).

Attack Detection:

- Monitoring network traffic for known attack patterns, such as packet flooding, brute force attacks, and unauthorized access attempts.
- Detection of intrusion attempts, such as port scans, SQL injection attacks, and cross-site scripting (XSS).
- Real-time alerts and notifications in case of attack detection, allowing administrators to take immediate action to protect the network.
- Generation of security reports with details about detected attacks, including type of attack, origin, target, and date/time.
- Automatic blocking of IP or MAC addresses from known attackers.

Device Isolation:

- Automatic isolation of infected or suspicious devices to prevent the spread of threats on the network.
- Option to manually isolate devices through the management interface.
- Notification to administrators about isolated devices, including information about the reason for isolation and the isolation time.
- Creation of isolation rules based on different criteria, such as device type, MAC address, SSID, or traffic behavior.
- Integration with intrusion detection systems (WIDS) for automatic isolation of devices based on security alerts.

ANALYSIS AND REPORTING

Traffic Analysis:

- Collection and analysis of real-time and historical network traffic data, including information on traffic volume, traffic types, protocols used, and key applications.
- Visualization of graphs and tables with traffic statistics such as throughput, bandwidth utilization, traffic distribution by SSID, AP, and client.
- Identifying bottlenecks and performance issues in the network, such as congested links, overloaded APs, or bandwidth-hungry clients.
- Generation of custom traffic reports, with filters by period, traffic type, device or customer.
- Analyzing traffic trends to identify usage patterns and predict future capacity needs.

Spectrum Analysis:

- Radio frequency spectrum monitoring to identify sources of interference, such as other Wi-Fi devices, microwave ovens, or cordless phones.
- Visualization of spectrum heat maps to identify areas with high interference and the channels affected.
- Recommendations for optimizing channel selection and AP transmit power, based on spectrum analysis.
- Detection of unauthorized devices that may be causing network interference.
- Generation of spectrum analysis reports with detailed graphs and statistics.

Report Generation:

- Create custom reports on network performance, security, and utilization, including information on device status, network traffic, security events, resource utilization, and user experience.
- Options to schedule report generation at regular intervals, such as daily, weekly, or monthly.
- Export reports in different formats, such as PDF and CSV, for easy data sharing and analysis.
- Customization of reports with the inclusion of logos, contact information, and other branding elements.

Device Management:

- Complete inventory of all network devices managed by the platform, including APs, switches, gateways, routers, and other compatible devices.
- Centralized device configuration, including network parameters (IP addresses, VLANs, DHCP), security (firewall, access control lists), and device-specific functionalities.
- Remote firmware update of devices to ensure they are running the latest and most secure version of the software.
- Remote reboot of devices in case of problems or need to apply new settings.
- Monitoring device status and performance, including connectivity, resource utilization, and alarm information.
- Grouping devices by type, location, or other criteria for easy management and enforcement of configurations in bulk.
- Creation of HTTP tunnels for secure remote access to network devices.

Integration with External Systems:

- Integration with network monitoring systems (NMS) for event and alert correlation, enabling a unified view of network performance and security.
- Integration with identity and access management (IAM) systems for centralized user authentication, using protocols such as RADIUS or LDAP.
- Integration with other network management tools, such as help desk systems for ticket tracking and data analytics tools for deeper insights into network usage.

COMPATIBLE EQUIPMENT

MODEL	DESCRIPTION	PHOTO
DM-AP 610 *825.8037.xx*	DM-AP 610 – AX1800 dual-band Wi-Fi 6 (802.11ax) wireless AP with up to four spatial streams. Up to 1.775 Gbps data rate, 1x 10/100/1000Base-T uplink port, PoE and DC power compatible. The PoE injector is sold separately and can be purchased from Datacom. The DC power adapter must be purchased separately from a third-party vendor if necessary).	
DM-AP 620 *825.8033.xx*	DM-AP 620 – AX3000 AX3000 dual-band indoor wireless AP with up to four spatial streams. Up to 2.976Gbps data rate, 1x 10/100/1000Base-T port with PoE support, 1x 2.5GbE SFP port, and DC power. The PoE injector is sold separately and can be purchased from Datacom. The DC power adapter must be purchased separately from a third-party vendor if necessary).	
DM-AP 920 *825.8041.xx*	DM-AP 920 – AX3000 dual-band Wi-Fi 6 (802.11ax) outdoor wireless AP with up to four spatial streams. Up to 2.976Gbps data rate, 1x 10/100/1000Base-T port with PoE support, 1x 2.5GbE SFP port, and DC power. The PoE injector is sold separately and can be purchased from Datacom. The DC power adapter must be purchased separately from a third-party vendor if necessary).	
DM-AP GT110 *825.8042.xx*	DM-AP GT110 – Next-Generation Unified Security Gateway. Equipped with a total of 8 GE ports (up to 2 WAN and 7 LAN), it supports up to 7x POE/POE+. Offers features such as high-performance NAT, WAN load balancing, intelligent flow control, visualized IPsec VPN, web authentication, and more Includes rack-mount kit, recommended for scenarios with up to 300 concurrent users. Compatible with DmCloud for centralized management.	
DM1205C 24GP+4XS 825.4542.xx	DM1205C 24GP+4XS Switch L3 with 24 electrical Gigabit Ethernet ports with PoE+ support (370W) and 4 optical 1/10G Ethernet uplink ports on SFP+ connectors. Internal AC Power Supply.	
DM-S100 8GT2GX 825.4543.xx	DM-S100 8GT2GX L2 Fanless Switch with 8 Electrical Gigabit Ethernet Ports and Two Optical Gigabit Ethernet Uplink Ports on SFP Connectors. SFPs must be purchased separately. Managed by DmCloud.	

DM-S100 8GP2GX 825.4544.xx	DM-S100 8GP2GX L2 Fanless Switch with 8 electrical Gigabit Ethernet ports with PoE/PoE+ support and two optical Gigabit Ethernet uplink ports on SFP connectors. SFPs must be purchased separately. Managed by DmCloud.	
DM-S300 24GT4XS 825.4545.xx	DM-S300 24GT4XS L3 Switch with 24 Gigabit Ethernet Electrical Ports and 4 Optical 1/10G Ethernet Uplink Ports on SFP+ Connectors. Internal AC Power Supply. Managed by DmCloud.	
DM-S300 24GP4XS 825.4546.xx	DM-S300 24GP4XS L3 Switch with 24 electrical Gigabit Ethernet ports with PoE+ support (370W) and 4 optical 1/10G Ethernet uplink ports on SFP+ connectors. Internal AC Power Supply. Managed by DmCloud.	
DM-S300 48GT4XS 825.4547.xx	DM-S300 48GT4XS L3 Switch with 48 electrical Gigabit Ethernet ports and 4 optical 1/10G Ethernet uplink ports on SFP+ connectors. Internal AC Power Supply. Managed by DmCloud.	
DM-S300 48GP4XS 825.4548.xx	DM-S300 48GP4XS L3 Switch with 48 electrical Gigabit Ethernet ports with PoE+ support (370W) and 4 optical 1/10G Ethernet uplink ports on SFP+ connectors. Internal AC Power Supply. Managed by DmCloud.	
DM-S400 20XS4VS2QX 825.4549.xx	DM-S400 20XS4VS2QX L3 Switch with 20 1G/2.5G/10G SFP+ ports, 4 10G/25G SFP28 ports, and 2 40G QSFP+ ports. Supports redundant AC supplies that must be purchased separately. Transceivers must be purchased separately. Managed by DmCloud.	

DATACOM

Rua América, 1000 | 92990-000 | Eldorado do Sul | RS | Brazil
+55 51 3933 3000
sales@datacom.com.br