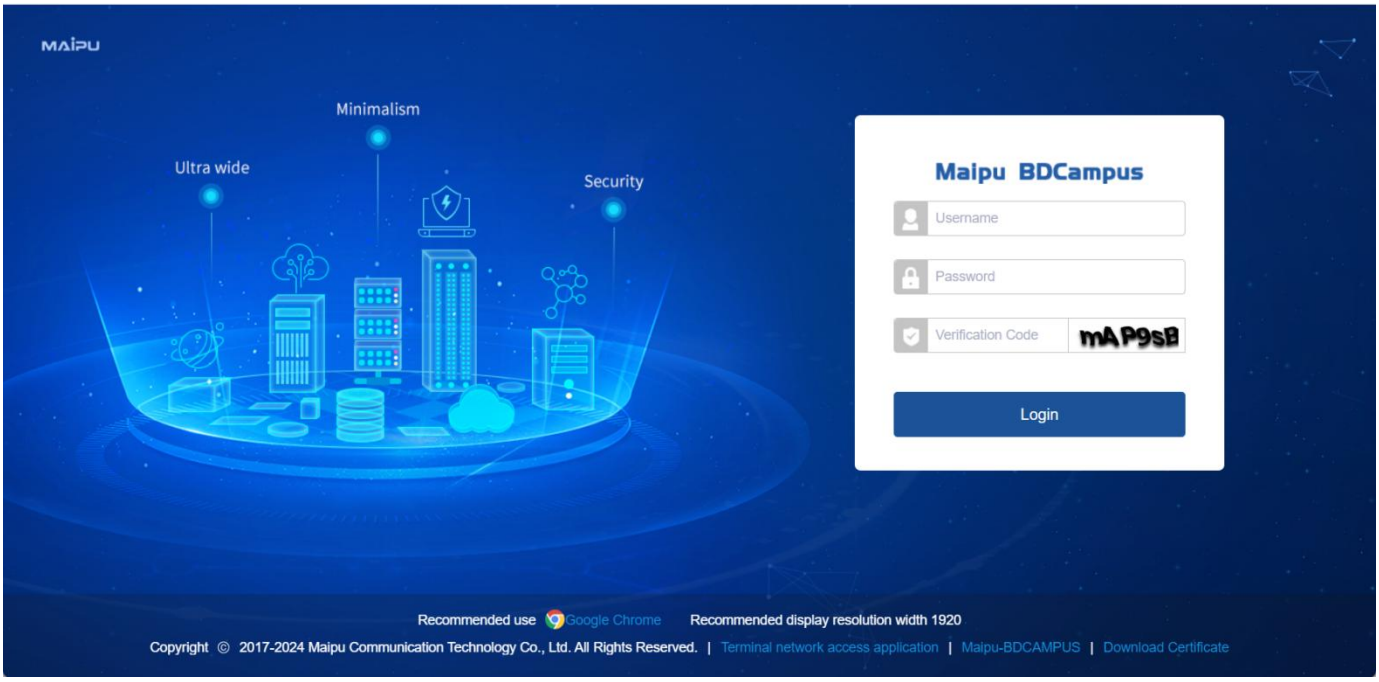
# Maipu BD-Campus SDN Controller Datasheet

## Overview

Maipu SDN BD-Campus solution is an integrated solution which includes Maipu SDN controller and Maipu SDN security switches and wireless. This solution greatly enhances internal campus network security by continuous monitoring and auto-blocking the abnormal terminal's network access. This would stop the potential virus spread or network attack from inside at the early stage. It earns more time for IT engineers to fix the vulnerability before it affects more terminals in the network.

Not just security concerned, Maipu SDN BD-Campus solution provides automation and insights for the whole network also. The automation helps reduce most of the traditional human errors via CLI commands, with just some simple clicks on the WEB GUI. This system also gives a full-dimension network insights by providing traffic monitoring different types of network and terminal statistics, IP & assets management and so on.



# Key Features

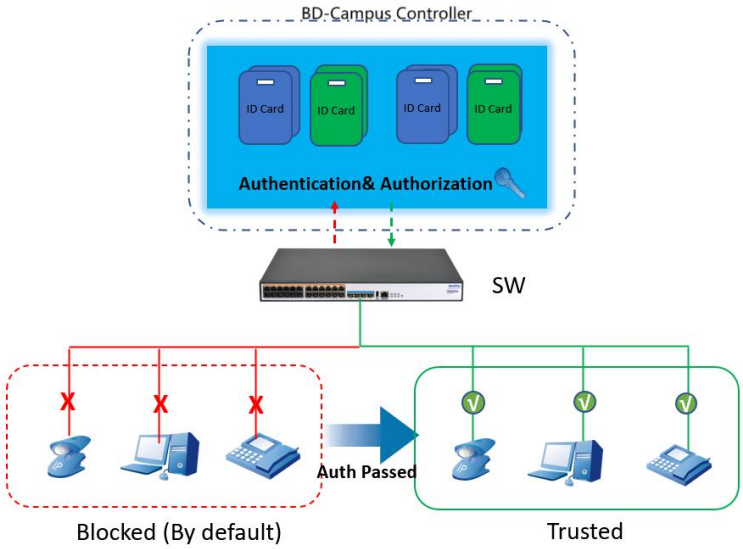
- **Unified Management for Wired and Wireless Networks**

  SDN BD-Campus solution for campus networks offers seamless integration of both wired and wireless network management. With a unified platform, you can centrally control, configure, and monitor all network elements—from wired connections to wireless access points—providing enhanced visibility and operational efficiency.

  This end-to-end management simplifies troubleshooting, optimizes performance, and enables rapid scalability. Whether expanding network capacity or implementing intelligent traffic steering, our solution meets the demands for flexibility, security, and high efficiency in modern campus networks.

- **Network Security**

  - **Zero Trust Network**




Zero Trust Access is one of the key features of Maipu BD-Campus Solution. It mainly does three things to guarantee your network is safely protected:

1) Different services are automatically segmented to avoid the influence of each other.

2) By default no terminal access is permitted until it is legally authenticated and authorized. This helps to prevent any unknown terminal access, ensuring that only the proven devices and users are in the network.

3) A Closed-loop network security monitoring and automation mechanism. BD-Campus Controller can interact with your UTM for any potential threat in the network. Once the UTM detects vulnerable behavior, it communicates with BD-Campus controller, then controller will locate and block the port on which the terminal is being connected. It protects the whole internal LAN network and ensures the block action can be taken at the very early stage. The key point is that the whole process is done automatically, without any human-being involved.

  - **Preventing Loops in the Network**

The switch can quickly detect and prevent the loop in the network. A loop warning will also be vividly shown on the Web GUI's virtual switch panel.

  - **Segment Services for a Safer Network**

By segmenting services into different networks, each network is independently running and the potential influence between services will be mostly avoided.

- **Multi-factor Access Policy Control**

Terminal credentials will be combined with the available access resources, the valid access time range and the permitted locations. This helps control the access privilege more accurately and flexibly.

## Network Automation


- **Zero Touch Provisioning(ZTP):**

It is used for automatic startup configurations after device hardware installation on sites. The whole process doesn't need any network engineer there and anyone can do this easily with just powering on the device.

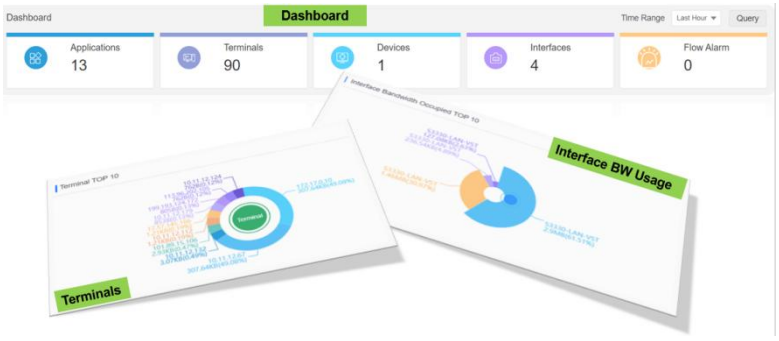
- **Service Auto Implementation:**

You can easily start your business services by simply defining the 4W1H modules on the controller's Web UI. The 4W1H are mapped to What service, Where to deploy, Who & When to access, and How users are authenticated. All the configuration scripts for corresponding devices will be done automatically.

- **One-Click Replacement and Auto Upgrade**

It's convenient and fast for network engineers to get rid of the traditional long-lasting procedure with the one-click device replacement and auto upgrade feature. Any human's error-prone mistake can be now avoided.

## Network Insights




With full-dimension reports on BD-Campus Controller, you can check the overall network status on Dashboard, such as Top 10 Terminal bandwidth, Top 10 interface Bandwidth Usage.

You can also use BD-Campus Controller to achieve the IP management, Asset Management etc.

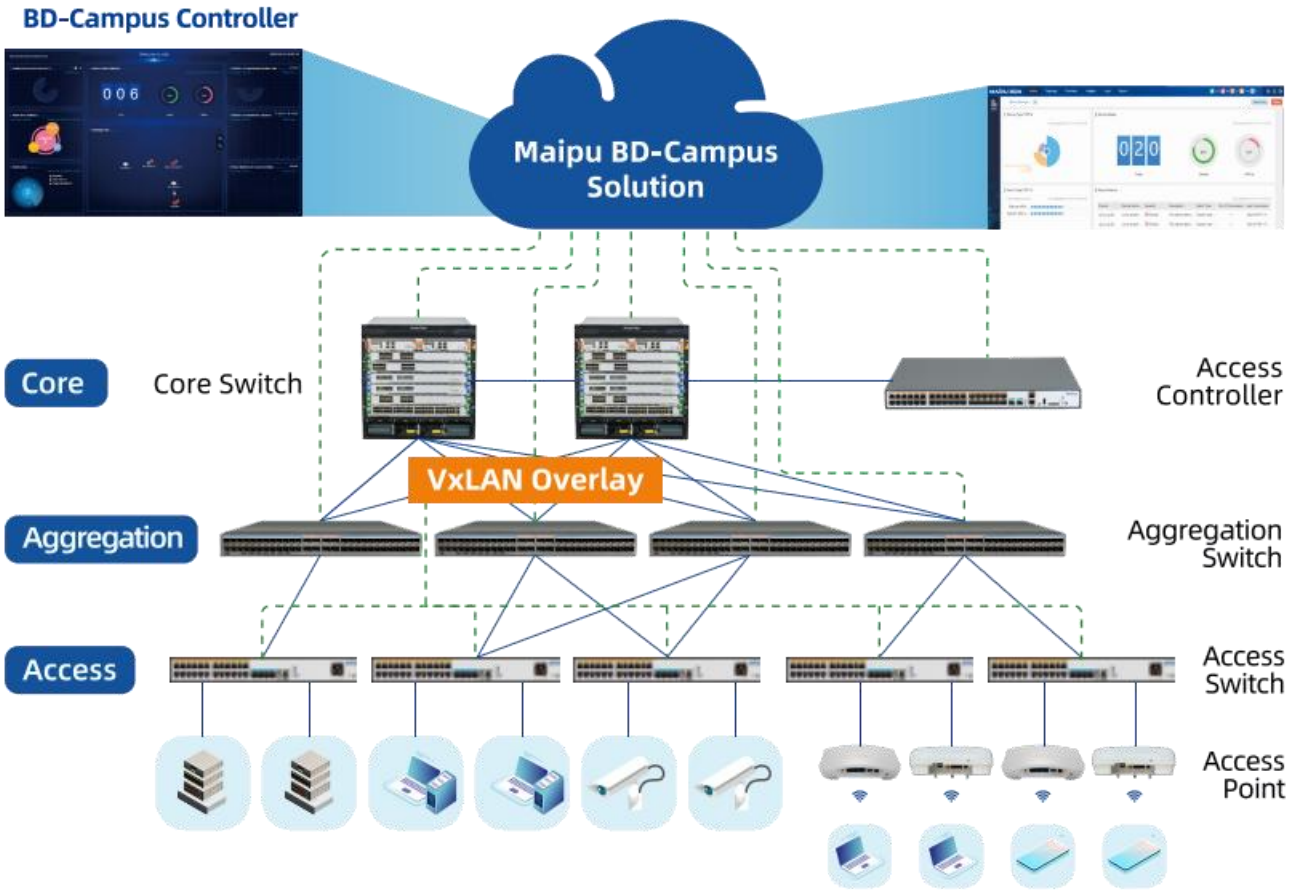
For network debugging, the rich logs and statistics can help network engineer quickly locate the issue and recover the network.

# Product Specifications

| Specifications | Technical parameters |
|---|---|
| **Security** | Zero Trust Network Security |
| | Preventing Loops in the Network |
| | Segment Different Services for a Safer Network |
| | Multi-factor Access Policy Control |
| | Anomaly Detection & Automated Defense |
| | Third-party UTM (Unified Threat Management) Interoperability |
| | Terminal Migration Control |
| | QoS (Quality of Service) for Improved Network Service Experience |
| | Support for 802.1x, MAC authentication, and portal among various authentication methods to achieve more secure and detailed login control. |
| | Policy Following: Regardless of changes in the office location, the access control policies remain consistent. |
| | Dynamic Policy Support: User access control policies can adapt flexibly despite changes in the office location. |
| | Software-Defined Access Control based on a unified identity engine and a unified policy engine to determine a user's policies from multiple dimensions. |
| | Data Security Protection to ensure data encryption within the campus LAN. |
| | Terminal Vulnerability Scanning: One-click scanning of high-risk terminal ports with automatic isolation and blocking. |
| | Terminal Vulnerability Checks to assist in controlling terminal security. |
| | Integration with Traditional Security to fully accommodate traditional security networks. |
| | Dual-Network Carriage: Logical isolation between overlay and underlay networks, with the ability to designate networks for specific business service carriage based on needs. |
| | Network Escape: In case of controller anomalies, the forwarding path can be dynamically adjusted according to real-time network conditions to ensure orderly traffic forwarding. |
| | Underlay Link Failure Detection: By sending test messages to detect link connectivity and notifying network administrators promptly upon failures. |
| | Overlay Link Failure Detection: Providing tools for overlay network troubleshooting, accurately locating node and link failures, and ensuring precise recovery from network outages. |
| **Automation** | Zero-Touch Provisioning: Support for plug-and-play deployment, where devices are immediately operational upon connection. |
| | Service Orchestration via a Jigsaw Approach: Based on users, resources, and policies, orchestrate network services. The controller automatically recognizes the orchestration language, translates it into device language, and automatically distributes it to the corresponding devices for rapid service activation. |
| | One-Click Replacement: Support for quick and efficient substitution of malfunctioning equipment. |
| | Scheduled Firmware Upgrade/Configuration Backup: Capability to schedule firmware updates and back up configurations systematically. |
| | Automatic Network Topology Discovery: Automatically detect network topology and map device interconnections within the network topology. |

| | |
|---|---|
| **Visualization** | Port Traffic Statistics and Output: Support for monitoring and displaying real-time traffic on ports. |
| | Application Traffic Statistics and Output: Support for monitoring and displaying real-time traffic of applications. |
| | IP Resource Management: Capabilities for managing and recycling IP addresses. |
| | Endpoint Resource Management: Manage endpoint IPs, MAC addresses, and manufacturers. |
| | Large Screen Display: Support for displaying geographic locations of devices, network TOPO, OVERLAY topo, device status, traffic, and other system monitoring components. |
| | Network Topology Display: Show the relationships between devices/links within the network, and provide information on link congestion status. |
| | Device Interface Traffic Statistics and Output: Support for monitoring and displaying traffic on device interfaces. |
| | Real-Time Device Configuration Viewing: Ability to read device configurations in real-time from the controller. |
| | Real-Time Link Bandwidth Measurement: Display the actual bandwidth of network links. |
| | Real-Time Monitoring of Link Bandwidth, Latency, Jitter, and Packet Loss: Provide real-time monitoring and display of network link quality. |

# Network Application



# Hardware Recommend Specification

### BD-Campus:

### A Linux system (required to have the Suse12 SP5 64-bit operating system installed).

| Number of Management Devices | Number of Managed Endpoints | CPU (Recommended Configuration) | Memory (Recommended Configuration) | Disk Performance Parameters (Minimum Configuration) |
|---|---|---|---|---|
| ≤440 | ≤5000 | Intel XEON Silver 4110 * 8 cores 16 threads 2.1GHz * 2 | 96G DDR4 | 960G 2.5 inches SSD*2 (RAID0)<br>600G 15K 2.5 inches SAS*2(RAID1)<br>1.2TB 10K 2.5 inches SAS *3(RAID5) |

### BDsec Component:

### A Linux system (required to have the Suse12 SP5 64-bit operating system installed).

| Number of Management Devices | Number of Managed Endpoints | CPU (Recommended Configuration) | Memory (Recommended Configuration) | Disk Performance Parameters (Minimum Configuration) |
|---|---|---|---|---|
| ≤440 | ≤5000 | Intel XEON Silver 4110 * 8 cores 16 threads 2.1GHz | 64G DDR4 | 1.2TB*2 10K 2.5 inches SAS (RAID1) |

# Order Information

| Product Model | | Description |
|---|---|---|
| **SDN Platform** | **Maipu BD-Campus** | Maipu BD-Campus SDN controller software platform, It provide the basic management for SDN switches and wireless AC and AP. |
| **Network Advanced Management Components** | **BD-BNP** | License for advanced network management function module, providing network planning, topology management, BYOD function, service automation deployment, etc. |
| | **BD-Campus-L-50** | License for 50 network node management, providing advanced management functions of LAN network, including device discovery, network topology presentation, network planning, service plan and service auto implementation |
| | **BD-Campus-L-100** | License for 100 network node management, providing advanced management functions of LAN network, including device discovery, network topology presentation, network planning, service plan and service auto implementation |
| | **BD-Campus-L-500** | License for 500 network node management, providing advanced management functions of LAN network, including device discovery, network topology presentation, network planning, service plan and service auto implementation |
| | **BD-Campus-L-1000** | License for 1000 network node management, providing advanced management functions of LAN network, including device discovery, network topology presentation, network planning, service plan and service auto implementation |

| | | |
|---|---|---|
| **Unified Authentication Components** | **BD-UIM** | License for Maipu unified authentication management function module, providing user identity authentication, access authorization, access auditing functions, 802.1x/Portal/MAC authentication |
| | **BD-UIM-L-100** | License for 100 terminal's for authentication per day |
| | **BD-UIM-L-500** | License for 500 terminal's for authentication per day |
| | **BD-UIM-L-2000** | License for 2000 terminal's for authentication per day |
| | **BD-UIM-L-5000** | License for 5000 terminal's for authentication per day |
| **Network Performance Components** | **BD-NPM** | License for network performance analysis function module, providing flow analysis such as network applications, terminals, interfaces |
| | **BD-NPM-L-1** | License for one network node's performance analysis |
| **Controller Cluster Components** | **BD-CLS** | License for cluster mode installation, providing the cluster-based installation with multiple hardware servers |

*Maipu Communication Technology Co., Ltd*
Maipu Mansion，No.16, Jiuxing Avenue
High-tech Park
Chengdu, Sichuan Province
P. R. China
610041
Tel: (86) 28-65544850,
**Fax:** (86) 28-65544948,
**URL:** http:// www.maipu.com
**Email:** overseas@maipu.com