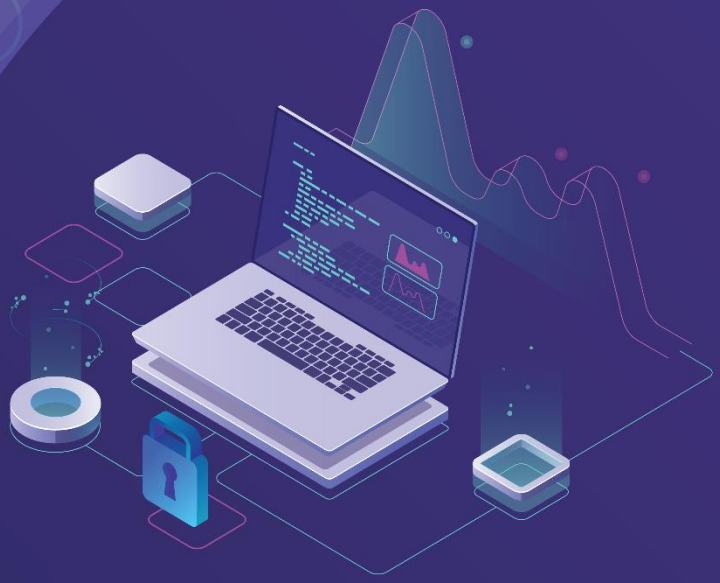
LiNKDOOD NETWORK ACCESS CONTROL



Control the access permission of trusted computer terminals which provides identity authentication

Network Access Control

Background

Linkdood NAC (Network Access Control) technology, is a system fundamentally guarantees the creditability of endpoints and controls the access permission of trusted computer terminals by means of identity authentication and security domain control to avoid a variety of security issues such as occupancy violations of enterprise network and information resources, Trojan and virus infection, enterprise information disclosure and unauthorized access due to access of untrusted terminals.

BEYOND SECURITY LINKDOOD

Table of Content

Contents

Introduction

NAC (Network Access Control) technology, is supported by various network equipment vendors with the aim preventing enterprise security hazards from emerging hacking techniques such as viruses and worms. This technology has been evolved from the initial stage of first-generation ARP access control technology to multiple forms of network access control technologies such as DHCP enforcer, 802.1x, EOU & Gateway Enforcer.

Linkdood NAC system fundamentally guarantees the creditability of endpoints and controls the access permission of trusted computer terminals by means of identity authentication and security domain control to avoid a variety of security issues such as occupancy violations of enterprise network and information resources, Trojan and virus infection, enterprise information disclosure and unauthorized access due to access of untrusted terminals.

System Structure

Linkdood network access control system is controlled by the access gateway (hereinafter referred to as the Linkdood gateway network access control), terminal agent client (hereinafter referred to as the access agent) and centralized management platform (hereinafter referred to as the management platform). These three sections constitute an integral part of Linkdood network access control system.

Figure 1

Some note-able key points in the report:

- **Network Access Control Gateway:** Responsible to evaluate the results of policies and match the corresponding access policy according to the evaluation results by uses its self-developed security Operating System, VRVOS as the core.
- **Integrated Management Platform:** Manage network access control gateway; including system management, configuration management, policy management, data and terminal management
- **Access Agent:** Provide an environment for submission of registration information on the terminal, control registration information required, and in special circumstances, prevents the registration of external personnel;
- **Third-party System:** Provide interfaces to Linkdood host audit system and Linkdood mobile security management system for function integration.

Core Technology

Linkdood network access control system uses a variety of core technology design which supports multiple access control modes for multi-dimensional terminal access security control.

1. Redirection

The purpose of access control is to prevent untrusted terminal from accessing the network. Untrusted terminals require time and resources to be identified. Linkdood network access control system optimized the redirection of access control process for registration, authentication, security and repair. The whole process of the redirection conforms to the terminal access behaviors in the overall process of terminal access and provides help tips in the redirect page:

- Redirects the unregistered terminals to the download page for registration;
- Redirects the unauthenticated users to authentication page which provides a variety of identity authentication methods;
- Provides personalized security rating and redirection page. Using Ajax technology, the security check results can be automatically updated. Also provides one-click repair policy in the redirection page;
- Provides help link for each redirection page, helps end users to automatically solve all the problems in the process of accessing network, reduces participation of network management personnel, improves the efficiency of network management and reduces labor costs.

2. Policy Routing

Policy routing mode of Linkdood access control system requires the core of the network infrastructure equipment (such as core switches) to support policy routing. Upstream request is directed to Linkdood network access control system through the control of policy routing and then it is authenticated, and credibility determined through the Linkdood access control system. By discarding or basic forwarding to the original route, reliable terminals can be filtered to achieve the effects of access control. The specific process can be illustrated in the following flow diagram:

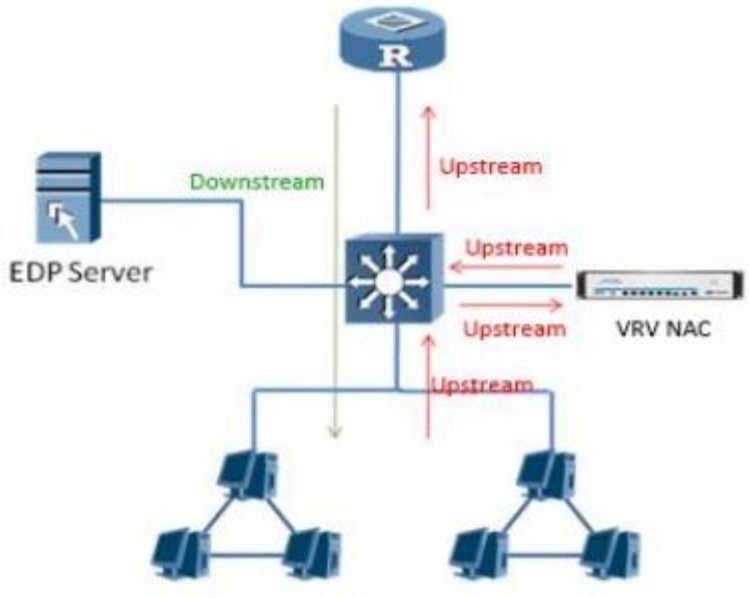


Figure 2

Since the policy routing mode only processes the request for upstream operations, the forwarding for downstream operation will not be affected. This guarantees security and is more suitable to be used in most types of network environments.

3. Bypass Interference

This is a new type of access control technology based on the concept of access control. Compared with the policy routing access control mode, the bypass interference access control mode has more prominent security features. In principle, although policy routing access control mode is deployed in a bypass mode, it hijacks the upstream traffic to filter the operation traffic. Bypass interference access control mode replicates traffic to filter upstream operation traffic, and then interrupts the current traffic through bypass interference. This is a true bypass deployment mode and does not need any changes to the direction of the current traffic flow. Because bypass interference deployment has no effect to the current operation traffic, it has unique and incomparable security. Refer to the operation processes as below:

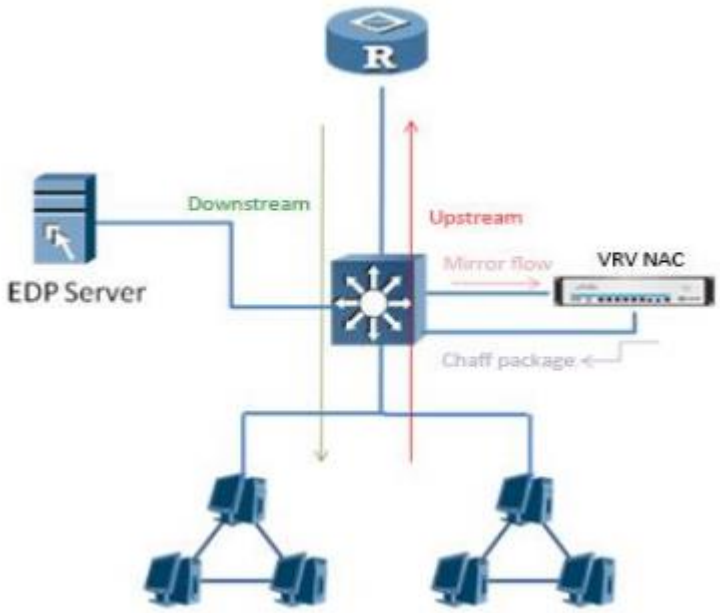

R
Downstream
Upstream
Mirror flow
VRV NAC
EDP Server
Chaff package

Figure 3

4. Transparent Bridges

Transparent bridge technology has been accepted by most network security devices and is currently the strictest deployment technology in the level of network gateway control. Linkdood network access control system concatenates the bridge into the network without changing the existing topology and filters traffic IP using the method of ACL to isolate and repair untrusted terminal.

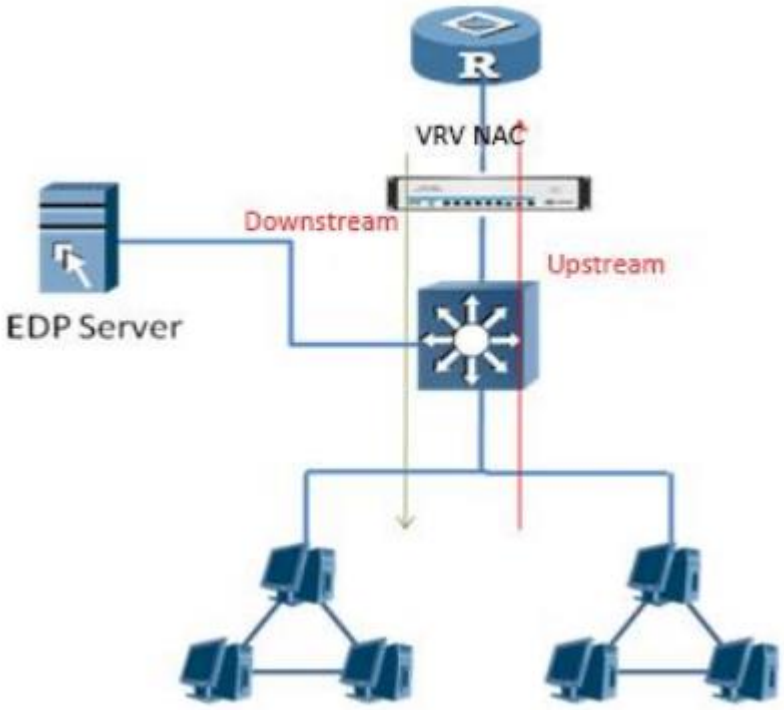


Figure 4

5. Multiple Access Control Technology

Linkdood network access control system integrates with multiple access methods, such as DHCP, 802.1 X, Agent access, SNMP access and clientless access to meet various kinds of access control requirements of access network, access internal business on terminals and exchange visits to ensure that only terminals that pass authentication and security check can access Intranet. Additionally, the access is under control and illegal or unsecure terminals will be isolated for repair.

Figure 3

Security Check

Security check is the network access proof for endpoint. Unsafe endpoint access network will cause immeasurable losses for network. For example, spread of virus and Trojan causes the problem of data leakage and unsafe policies causes the endpoints to be vulnerable to attacks. Based on the above problems, Linkdood NAC reinforces endpoint security. It evaluates potential risks of endpoint, repairing and reinforcing the risks according to evaluation result.

- **Anti-virus Software Check**: Check and evaluate endpoint anti-virus software installation condition. Two options are available: “required” and “not required”.
- **Sharing Resource Check:** Check endpoint sharing resource condition. Two options are available: “allowed” and “not allowed”.
- **System Loophole Check**: Check endpoint system loophole condition. Two options are available: “allowed” and “not allowed”.
- **IE Homepage Check:** Check IE homepage settings configuration. Two options are available: “allowed changing homepage” and “not allowed changing homepage”.
- **Guest Account Check:** Check endpoint guest account status. Two options are available: “allowed” and “not allowed”.
- **Remote Desktop Check**: Check remote desktop status. Two options are available: “allowed” and “not allowed”.
- **Start Item Check**: Check progress start condition; support “not allowed to start”. Progress list of start item can be customized.
- **Weak Password Check**: Scan users with weak password. Two options are available: “allowed” and “not allowed”.
- **Start Service Check**: Check system start service condition. Support settings of “required start item”. Service list can be customized.

Access Authentication Log

Linkdood NAC supports recording of users’ authentication condition, which includes authentication time, username, authentication type, IP and authentication behavior. It also provides check port to view specific user’s network access condition within a specific period.

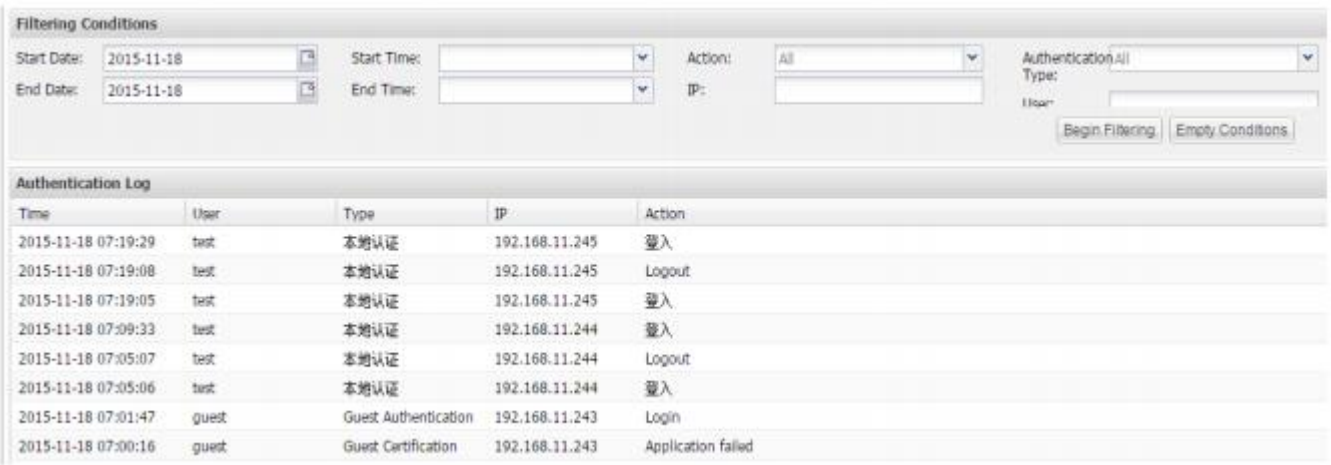

Filtering Conditions
Start Date: 2015-11-18
End Date: 2015-11-18
Start Time:
End Time:
Action: All
IP:
Authentication Type: All
Begin Filtering
Empty Conditions
Authentication Log
Time User Type IP Action
2015-11-18 07:19:29 test 本地认证 192.168.11.245 登入
2015-11-18 07:19:08 test 本地认证 192.168.11.245 Logout
2015-11-18 07:19:05 test 本地认证 192.168.11.245 登入
2015-11-18 07:09:33 test 本地认证 192.168.11.244 登入
2015-11-18 07:05:07 test 本地认证 192.168.11.244 Logout
2015-11-18 07:05:06 test 本地认证 192.168.11.244 登入
2015-11-18 07:01:47 guest Guest Authentication 192.168.11.243 Login
2015-11-18 07:00:16 guest Guest Certification 192.168.11.243 Application failed

Figure 5

Whole Network Monitoring

Provide real-time statistics of whole network device's information, such as registration, authentication, security check and unaudited guest. Provide real-time statistics of device port occupation, CPU and memory usage rate. Also provide overall network online user's trend chart on that day.

Figure 6

Flexible Deployment

Linkdood NAC adopts independent hardware design and supports various deployment modes, which can be adapted to different network topology environment. The system preferentially uses bypass access control deployment mode, which can select policy routing control mode and bypass mirror control mode according to supporting conditions of the switch. If support for policy routing control mode and bypass mirror control mode is unavailable, it can adopt Transparency Bridge to control the network. In topology environment such as wireless, router, hub and switch that are out of administrator's control, it supports mutual access between NAT Traversal and local area network. These deployments can be adapted to various network environments of different users, preventing untrusted endpoint from connecting with network. The following images shows some typical deployment modes.

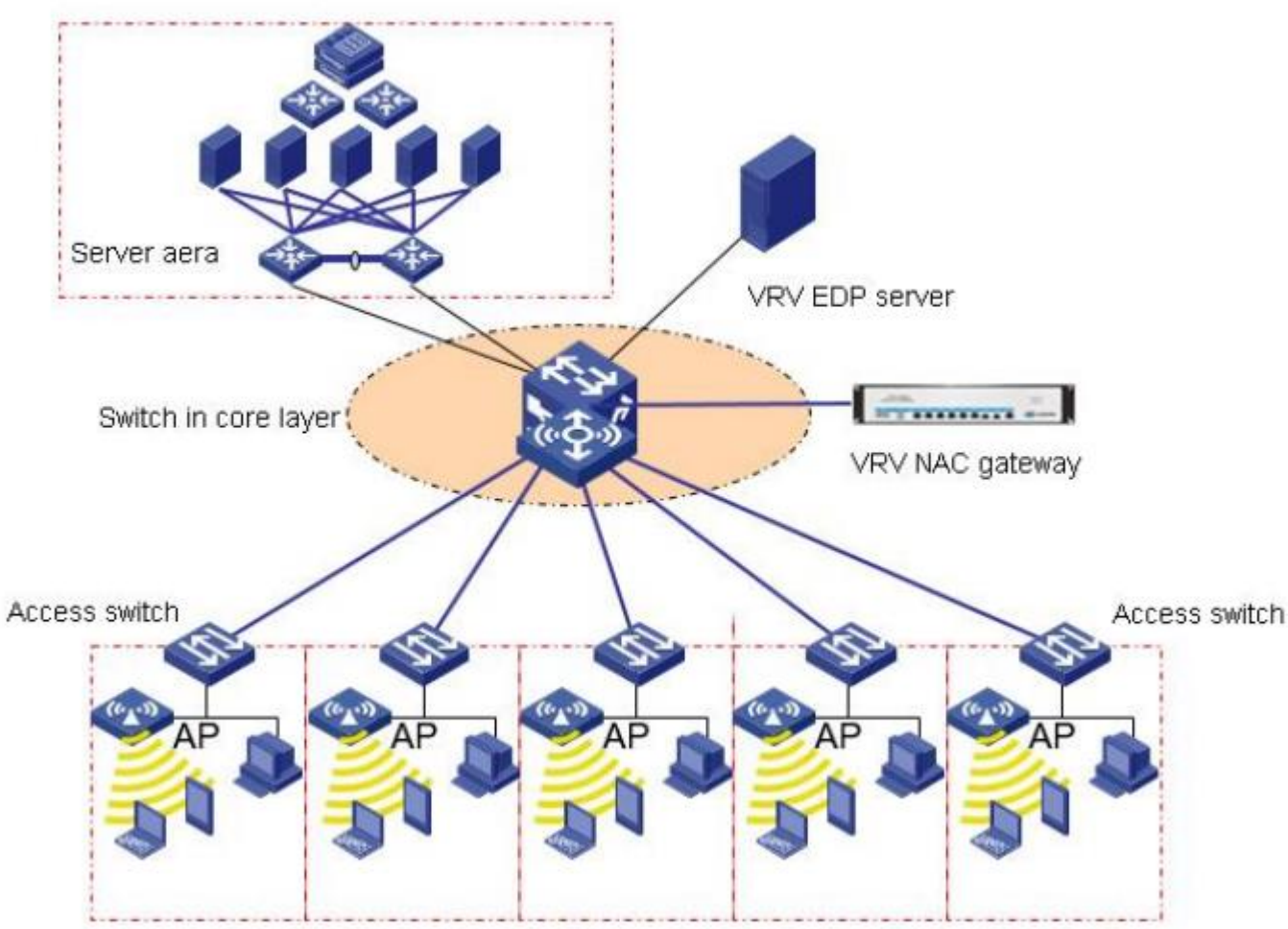


Figure 7

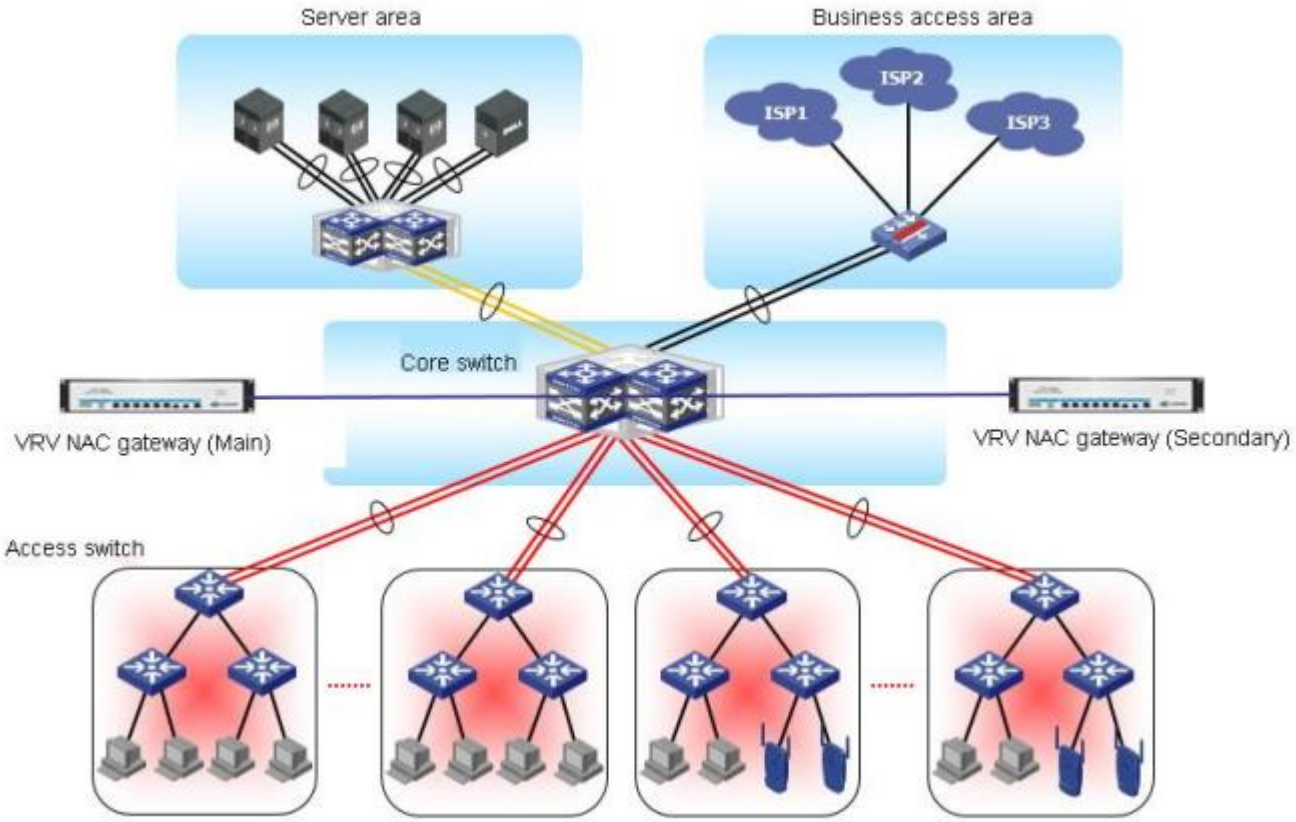


Figure 8

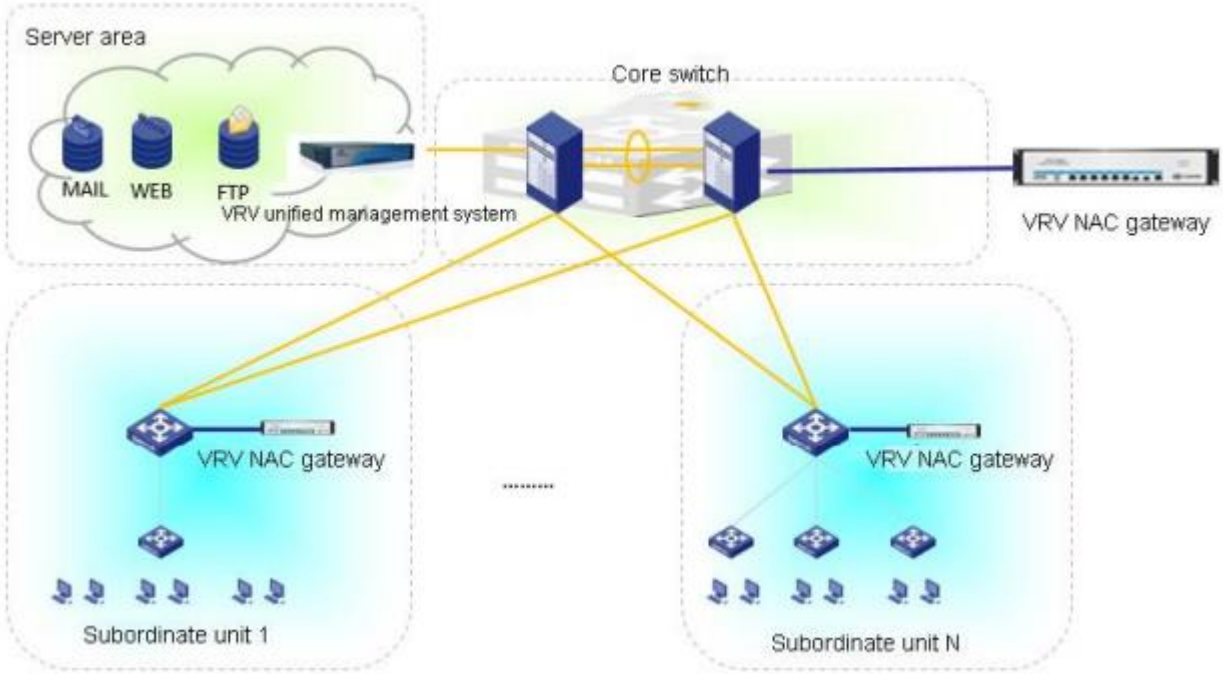


Figure 9

Product Specification

LD-BMG-200

1U Rack, 6 1000BASE-T interfaces, 2 USB interface, 1 RS232 serial port (RJ-45), 1TB hard disk, single AC power supply.				
Project	**Device type**	**Product number**	**Description**	**Performance**
Main System	Hardware Device	LD-BMG-200	Linkdood Network Access Control System LD-BMG-200	Use with no more than 200 authenticated users; support max 200Mbps traffic throughput;160,000 concurrent connections; max connection 6000/S

LD-BMG-500

1U Rack, 6 1000BASE-T interfaces, 2 USB interface, 1 RS232 serial port (RJ-45), 1TB hard disk, single AC power supply.				
Project	**Device type**	**Product number**	**Description**	**Performance**
Main System	Hardware Device	LD-BMG-500	Linkdood Network Access Control System LD-BMG-500	Use with 200-500 authenticated users; support max 500 Mbps traffic throughput; 400000 concurrent connections; max connection 8000/S

LD-BMG-1000

1U Rack, 6 1000BASE-T interfaces, 2 USB interface, 1 RS232 serial port (RJ-45), 1TB hard disk, single AC power supply.				
Project	**Device type**	**Product number**	**Description**	**Performance**
Main System	Hardware Device	LD-BMG-1000	Linkdood Network Access Control System LD-BMG-1000	Use with 500-1000 authenticated users; support max 800 Mbps traffic throughput;600000 concurrent connections; max connection 10000/S

LD-BMG-2000C

1U Rack, 6 1000BASE-T interfaces, 2 USB interface, 1 RS232 serial port (RJ-45),1TB hard disk, single and dual AC power supply configurations are available.				
Project	**Device type**	**Product number**	**Description**	**Performance**
Main System	Hardware Device	LD-BMG-2000	Linkdood Network Access Control System LD-BMG-2000C	Use with 1000-2000 authenticated users; support max 1.5Gbps traffic throughput; 1000000 concurrent connections; max connection 16000/S
Accessory (Optional)	Optical bypass	BMG-BYPASS-M M-D	Dual multimode optical bypass module	
Accessory (Optional)	Optical bypass	BMG-BYPASS-S M-D	Dual single mode optical bypass module	
Accessory (Optional)	Secondary AC power	BMG-POWER-R	Secondary AC power	

LD-BMG-2000F

2U Rack, 6 1000BASE-T interfaces, 4 optical interface 2 USB interface, 1 RS232 serial port (RJ-45), 1TB hard disk, single and dual AC power supply configurations are available.				
Project	**Device type**	**Product number**	**Description**	**Performance**
Main System	Hardware Device	LD-BMG-2000	Linkdood Network Access Control System LD-BMG-2000F	Use with 1000-2000 authenticated users; support max 1.5Gbps traffic throughput; 1000000 concurrent connections; max connection 16000/S
Accessory (Optional)	Optical bypass	BMG-BYPASS-M M-D	Dual multimode optical bypass module	
Accessory (Optional)	Optical bypass	BMG-BYPASS-S M-D	Dual single mode optical bypass module	
Accessory (Optional)	Secondary AC power	BMG-POWER-R	Secondary AC power	
Accessory (Optional)	Optical expansion card	BMG-OPTI-GE-4P	4-channel gigabit Ethernet optical interface board	
Accessory (Optional)	Optical expansion card	BMG-OPTI-10GE-4P	4-channel 10 gigabit Ethernet optical interface board	
Accessory (Optional)	Optical module	GSFP-MM-SX-500M	Gigabit multimode SFP optical module, 850nm, transmission distance 500m	
Accessory (Optional)	Optical module	GSFP-SM-LX-10 KM	Gigabit multimode SFP optical module, 1310nm, transmission distance 10kmm	
Accessory (Optional)	Optical module	10GSFP-MM-SX500M	10 Gigabit multimode SFP optical module, 850nm, transmission distance 500m	
Accessory (Optional)	Optical module	10GSFP-SM-LX10KM	10 Gigabit single mode SFP optical module, 1310nm, transmission distance 10kmm	
Accessory (Optional)	Optical fiber	DLC-DLC-MM 3M	Multimode LC-LC fiber jumper, 3M long	
Accessory (Optional)	Optical fiber	DLC-DLC-SM 3M	Single mode LC-LC fiber jumper, 3M long	

LD-BMG-3000C

2U Rack, 6 1000BASE-T interfaces, 2 USB interface, 1 RS232 serial port (RJ-45), 1TB hard disk, single and dual AC power supply configurations are available.				
Project	**Device type**	**Product number**	**Description**	**Performance**
Main System	Hardware Device	LD-BMG-3000	Linkdood Network Access Control System LD-BMG-3000C	Use with 2000-3000 authenticated users; support max 2 Gbps traffic throughput; 1200000 concurrent connections; max connection 22000/S
Accessory (Optional)	Optical bypass	BMG-BYPASS-M M-D	Dual multimode optical bypass module	
Accessory (Optional)	Optical bypass	BMG-BYPASS-S M-D	Dual single mode optical bypass module	
Accessory (Optional)	Secondary AC power	BMG-POWER-R	Secondary AC power	

LD-BMG-3000F

2U Rack, 6 1000BASE-T interfaces, 4 optical interface, 2 USB interface, 1 RS232 serial port (RJ-45), 1TB hard disk, single and dual AC power supply configurations are available.				
Project	**Device type**	**Product number**	**Description**	**Performance**
Main System	Hardware Device	LD-BMG-3000	Linkdood Network Access Control System LD-BMG-3000F	Use with 2000-3000 authenticated users; support max 2 Gbps traffic throughput; 1200000 concurrent connections; max connection 22000/S
Accessory (Optional)	Optical bypass	BMG-BYPASS-M M-D	Dual multimode optical bypass module	
Accessory (Optional)	Optical bypass	BMG-BYPASS-S M-D	Dual single mode optical bypass module	
Accessory (Optional)	Secondary AC power	BMG-POWER-R	Secondary AC power	
Accessory (Optional)	Optical expansion card	BMG-OPTI-GE-4P	4-channel gigabit Ethernet optical interface board	
Accessory (Optional)	Optical expansion card	BMG-OPTI-10GE-4P	4-channel 10 gigabit Ethernet optical interface board	
Accessory (Optional)	Optical module	GSFP-MM-SX-500M	Gigabit multimode SFP optical module, 850nm, transmission distance 500m	
Accessory (Optional)	Optical module	GSFP-SM-LX-10 KM	Gigabit multimode SFP optical module, 1310nm, transmission distance 10kmm	
Accessory (Optional)	Optical module	10GSFP-MM-SX500M	10 Gigabit multimode SFP optical module, 850nm, transmission distance 500m	
Accessory (Optional)	Optical module	10GSFP-SM-LX10KM	10 Gigabit single mode SFP optical module, 1310nm, transmission distance 10kmm	
Accessory (Optional)	Optical fiber	DLC-DLC-MM 3M	Multimode LC-LC fiber jumper, 3M long	
Accessory (Optional)	Optical fiber	DLC-DLC-SM 3M	Single mode LC-LC fiber jumper, 3M long	

LD-BMG-5000C

2U Rack, 6 1000BASE-T interfaces, 2 USB interface, 1 RS232 serial port (RJ-45), 1TB hard disk, single and dual AC power supply configurations are available.				
Project	**Device type**	**Product number**	**Description**	**Performance**
Main System	Hardware Device	LD-BMG-5000	Linkdood Network Access Control System LD-BMG-5000C	Use with to 2000-5000 authenticated users; support max 2.8 Gbps traffic throughput; 1600000 concurrent connections; max connection 32000/S
Accessory (Optional)	Optical bypass	BMG-BYPASS-M M-D	Dual multimode optical bypass module	
Accessory (Optional)	Optical bypass	BMG-BYPASS-S M-D	Dual single mode optical bypass module	
Accessory (Optional)	Secondary AC power	BMG-POWER-R	Secondary AC power	

LD-BMG-5000F

2U Rack, 6 1000BASE-T interfaces, 4 optical interface, 2 USB interface, 1 RS232 serial port (RJ-45), 1TB hard disk, single and dual AC power supply configurations are available.				
Project	**Device type**	**Product number**	**Description**	**Performance**
Main System	Hardware Device	LD-BMG-5000	Linkdood Network Access Control System LD-BMG-5000F	Use with to 2000-5000 authenticated users; support max 2.8 Gbps traffic throughput; 1600000 concurrent connections; max connection 32000/S
Accessory (Optional)	Optical bypass	BMG-BYPASS-M M-D	Dual multimode optical bypass module	
Accessory (Optional)	Optical bypass	BMG-BYPASS-S M-D	Dual single mode optical bypass module	
Accessory (Optional)	Secondary AC power	BMG-POWER-R	Secondary AC power	
Accessory (Optional)	Optical expansion card	BMG-OPTI-GE-4P	4-channel gigabit Ethernet optical interface board	
Accessory (Optional)	Optical expansion card	BMG-OPTI-10GE-4P	4-channel 10 gigabit Ethernet optical interface board	
Accessory (Optional)	Optical module	GSFP-MM-SX-500M	Gigabit multimode SFP optical module, 850nm, transmission distance 500m	
Accessory (Optional)	Optical module	GSFP-SM-LX-10 KM	Gigabit multimode SFP optical module, 1310nm, transmission distance 10kmm	
Accessory (Optional)	Optical module	10GSFP-MM-SX500M	10 Gigabit multimode SFP optical module, 850nm, transmission distance 500m	
Accessory (Optional)	Optical module	10GSFP-SM-LX10KM	10 Gigabit single mode SFP optical module, 1310nm, transmission distance 10kmm	
Accessory (Optional)	Optical fiber	DLC-DLC-MM 3M	Multimode LC-LC fiber jumper, 3M long	
Accessory (Optional)	Optical fiber	DLC-DLC-SM 3M	Single mode LC-LC fiber jumper, 3M long	

LD-BMG-10000

2U Rack, 6 1000BASE-T interfaces, 4 optical interface, 2 USB interface, 1 RS232 serial port (RJ-45), 1TB hard disk, single and dual AC power supply configurations are available.				
Project	**Device type**	**Product number**	**Description**	**Performance**
Main System	Hardware Device	LD-BMG-10000	Linkdood Network Access Control System LD-BMG-10000	Use with to 5000-10000 authenticated users; support max 3.5 Gbps traffic throughput; 3000000 concurrent connections; max connection 48000/S
Accessory (Optional)	Optical bypass	BMG-BYPASS-M M-D	Dual multimode optical bypass module	
Accessory (Optional)	Optical bypass	BMG-BYPASS-S M-D	Dual single mode optical bypass module	
Accessory (Optional)	Secondary AC power	BMG-POWER-R	Secondary AC power	
Accessory (Optional)	Optical expansion card	BMG-OPTI-GE-4P	4-channel gigabit Ethernet optical interface board	
Accessory (Optional)	Optical expansion card	BMG-OPTI-10GE-4P	4-channel 10 gigabit Ethernet optical interface board	
Accessory (Optional)	Optical module	GSFP-MM-SX-500M	Gigabit multimode SFP optical module, 850nm, transmission distance 500m	
Accessory (Optional)	Optical module	GSFP-SM-LX-10 KM	Gigabit multimode SFP optical module, 1310nm, transmission distance 10kmm	
Accessory (Optional)	Optical module	10GSFP-MM-SX500M	10 Gigabit multimode SFP optical module, 850nm, transmission distance 500m	
Accessory (Optional)	Optical module	10GSFP-SM-LX10KM	10 Gigabit single mode SFP optical module, 1310nm, transmission distance 10kmm	
Accessory (Optional)	Optical fiber	DLC-DLC-MM 3M	Multimode LC-LC fiber jumper, 3M long	
Accessory (Optional)	Optical fiber	DLC-DLC-SM 3M	Single mode LC-LC fiber jumper, 3M long	