Hwacom Ace for Any SYSTEMS INC.

Cyber Monitor

Intelligent Network Management

Hwacom Ace for Any SYSTEMS INC.

Intelligence Network Management System

Quickly x Easily x Visualize

With technology advances, consumer behavior and the business environment are moving towards digitalization. In the digital age, network facilities are the most basic infrastructure, and the network environment has become more complex, so we need a comprehensive and unified interface to monitor our IT infrastructures for network management, database management, service, device management, etc. Therefore, network management should not be a passive solution to failure, but a more proactive role for businesses to grow in digital transformation.

Have you encountered the following problems?

1.The indicators are not precise and interface is unfriendly with text and a string of number only, which makes difficult to grasp the overall situation.

Due to large quantity of devices, cables, and several locations, faults must be manually searched to waste time. After finding out the root cause, it gives administrators heavy loading by spending massive time to update relevant documents.

2.There is no proactive notification mechanism, making response inefficiently and loss from the interruption of service.

Although it comes with managed software by every vendor of equipment, it cannot manage cross the different platform and even need to check each system manually. The passive management is in result of the administrators can not acknowledge the fault of the network in real-time until users report the abnormality, which has usually generated some loss.

3.Limited information for administrator to response late for the abnormality.

Administrators spend much time to collect the various information over different interfaces of the equipment manually. It is time-consuming and limited for the overall scope, therefore, it could result in the slow response.

4.More time-consuming to collect the data and difficult to glance the whole system.

There is no unified management software by multi-vendor equipment, therefore, it is in result of administrators spending much time to log in different systems to collect the data and generate the report. It is also hard to acknowledge the overall topology of the network.

5.Network devices need to be manually added to the management system.

There is no automatic discovery function to search network devices for management, therefore it takes much time to maintain the system manually.

Using this software, all the above problems you encountered can be solved.

Cyber Monitor is your best choice.

Why do you need to choose Cyber Monitor?

▶ Unified & User-Friendly Interface

Monitoring the devices of multi-brands into a unified and user-friendly interface and generating log reports automatically for effective and efficient management.

▶ Real-time notification and advises

Delivering the real-time notification in case of fault or abnormality and issuing the advises for troubleshooting or restore the configuration from last version.

▶ Auto-discovery of the whole system and detection for the topology

Cyber Monitor can automatically discover all devices of the system for management and inventory taking as well as generate the topology map of the network.

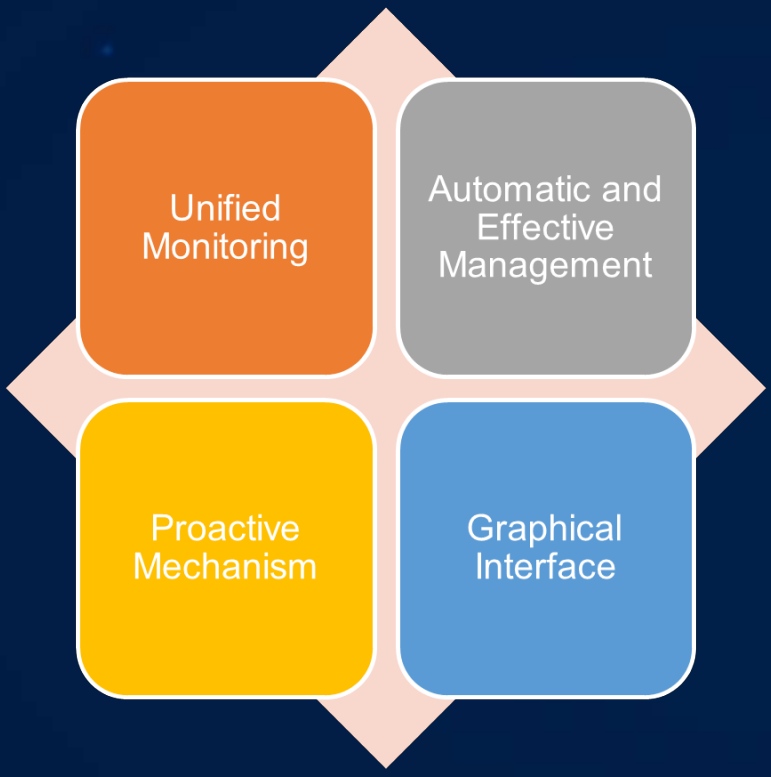
▶ Scalability & Customization

Quickly grasp the network operation status through accurate data and charts, which can be measured as a reference for future expansion. The customization provides a “tailor-made” system in response to customers’ operations.

▶ Performance & ROI

Monitoring the system and notifying the trouble at all times could manage the performance and stability of the network and prevent the operation of the company from interruption, which usually causes a big loss for the business. The automatic monitoring capability can also save the manpower and cost of the administration.

Cyber Monitor Four Features



Cyber Monitor Five Network Management Functions

1.Fault Management

Auto-detection, Auto warning, Log report, Issue tracking

2.Configuration Management

Setting the behavior on ports or devices such as enabled/disabled switch ports and blocked selected Mac/IP addresses. Auto backup configuration of device and comparison difference. Dispatch script to multiple devices.

3.Accounting Management

Statistics traffic of the particular IP and system for billing or expansion purposes.

4.Performance Management

Monitoring for all kinds of measurements on the device, such as traffic, CPU, RAM, Jitter, MOS, RTT, CRC…etc.

5.Security Management

User management & Authorization, Resource Control, Analysis of log report of the firewall.

Cyber Monitor Advantages

▶ Active Directory integration

Existing accounts can be integrated to log into the network management platform, such as LDAP, AD, OpenID...etc. No additional account numbers and passwords are required.

▶ Centralized management of multiple tenants

To establish a network of enterprises/institutions/campuses with a tree structure. Building network architectures include Gateway, DMZ, Routers, VLANs, etc. Account permissions can be set for each management.

▶ Unlimited license

Unlimited authorization can be stable and manage 500 to 1000 devices, 1000 to 2000 or more can also be monitored for optimization management, and more than 2000 can also be monitored through the horizontal expansion of equipment.

▶ Device status monitoring

Monitor the health status of hardware, software, and network activities, including CPU, MEMORY, TRAFFIC, etc.

▶ Early warning function

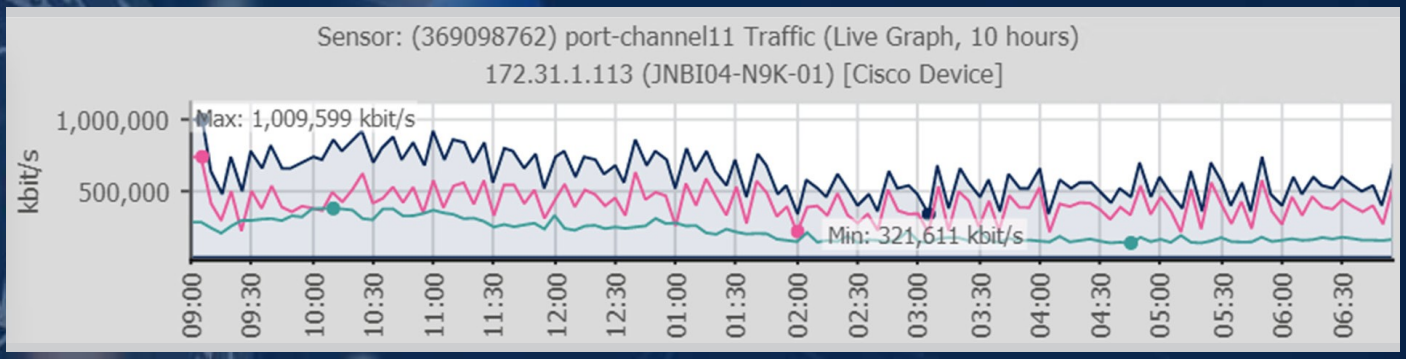
Automatic detection of networks, device values of unusual fluctuations early warning, rather than waiting for obstacles to notify, and automatically block abnormal IP traffic.

▶ Automate discovery management

Scheduled scanning of devices in the network segment used the automatic discovery to loop-in devices, managed without manual settings, and regularly scheduled backup device configuration profiles, which can be compared to the differences.

▶ Real-time traffic monitoring

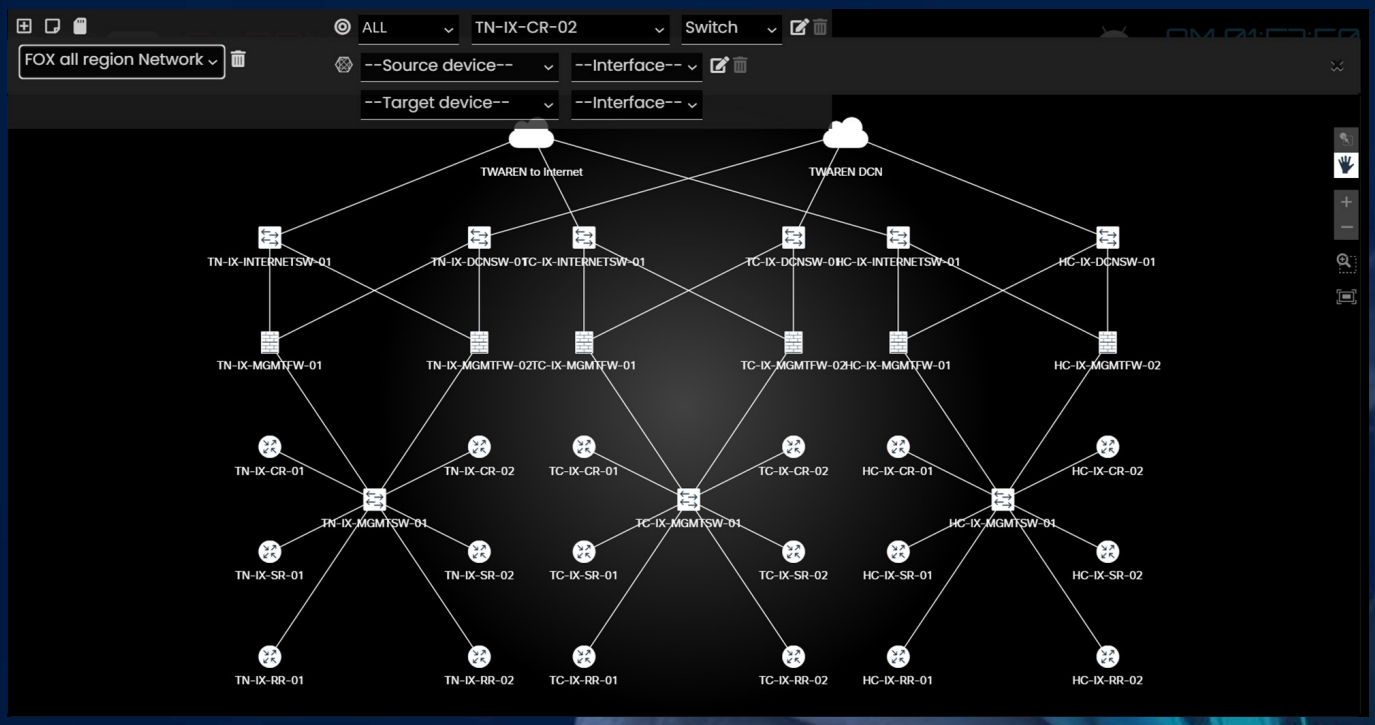
Real-time monitoring of network traffic utilization, and through the traffic chart to show the maximum and minimum value, query each client IP network usage and FLOW network connection source and destination flow.



Date Time	Traffic Total (volume)	Traffic Total (speed)	Traffic In (volume)	Traffic In (speed)	Traffic Out (volume)	Traffic Out (speed)	Coverage
2022/8/30 上午 11:00:06	550 MB	154 Mbit/s	288 MB	81 Mbit/s	262 MB	73 Mbit/s	100 %
2022/8/30 上午 11:00:36	414 MB	116 Mbit/s	216 MB	60 Mbit/s	198 MB	55 Mbit/s	100 %
2022/8/30 上午 11:01:06	232 MB	65 Mbit/s	128 MB	36 Mbit/s	104 MB	29 Mbit/s	100 %
2022/8/30 上午 11:01:36	289 MB	81 Mbit/s	155 MB	43 Mbit/s	135 MB	38 Mbit/s	100 %
2022/8/30 上午 11:02:06	335 MB	94 Mbit/s	181 MB	51 Mbit/s	154 MB	43 Mbit/s	100 %
2022/8/30 上午 11:02:36	245 MB	68 Mbit/s	134 MB	38 Mbit/s	111 MB	31 Mbit/s	100 %

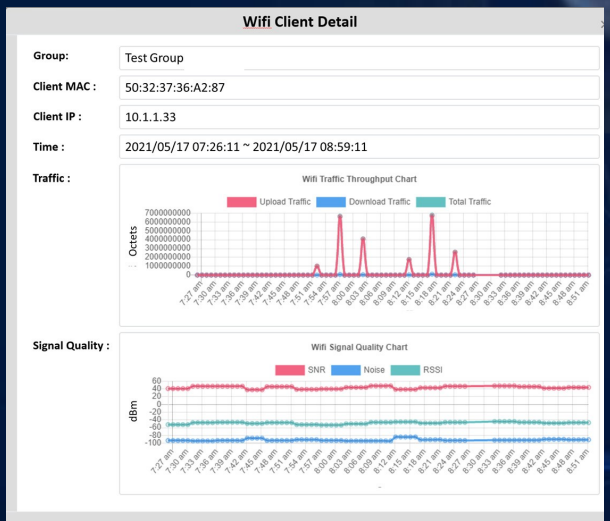
▶ Network topology (Pro Version)

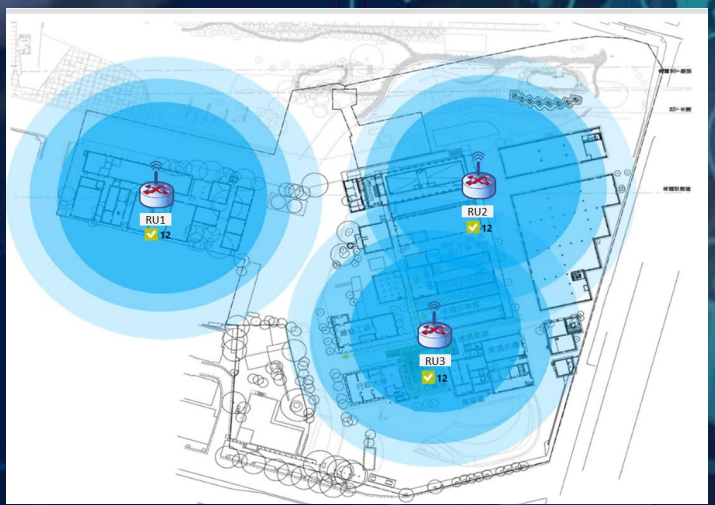
Automatically detect the connectivity of monitoring devices and draw network topology diagrams to visually view the monitoring status of the device and the status of the connection between the devices.



▶ Wireless network monitoring (Plus Version)

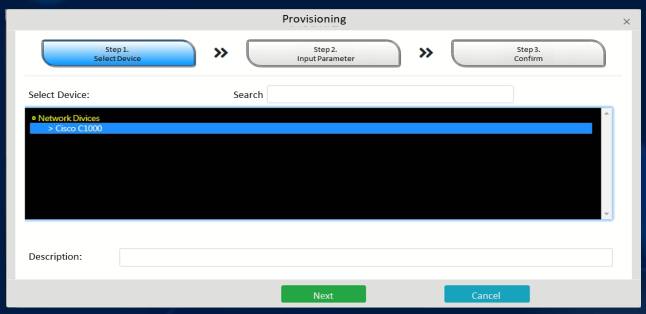
Overview of the WIFI situation of user usage, analyze WIFI traffic of user usage, device type, application distribution, and signal strength, support loading the floor plan of the enterprise to generate a heat map and provide the administrator with a visual view of AP status.

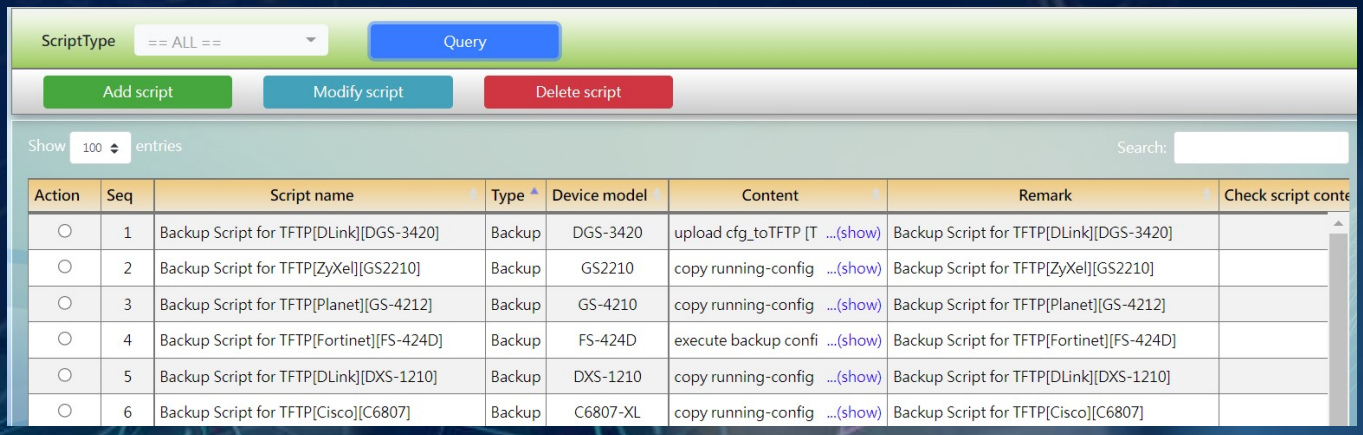




▶Self-defined Script dispatch (Pro Version)

Self-defined script commands can dispatch to different brands and mass equipment to execute to achieve batch modification, such as account and password of equipment, SSID, IPMAC binding, and other purposes. It only uses a unified interface that can operate all equipment, default several device models script including IP, MAC, Switchports enable or disable which scripts can control these.

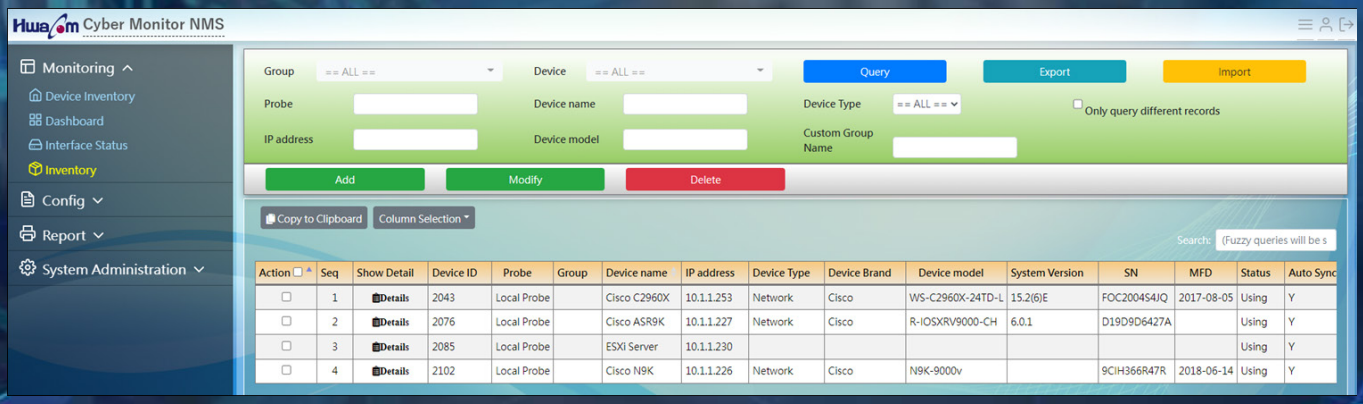




Action	Seq	Script name	Type	Device model	Content	Remark	Check script conte
○	1	Backup Script for TFTP[DLink][DGS-3420]	Backup	DGS-3420	upload cfg_toTFTP [T ...(show)	Backup Script for TFTP[DLink][DGS-3420]	
○	2	Backup Script for TFTP[ZyXel][GS2210]	Backup	GS2210	copy running-config ...(show)	Backup Script for TFTP[ZyXel][GS2210]	
○	3	Backup Script for TFTP[Planet][GS-4212]	Backup	GS-4210	copy running-config ...(show)	Backup Script for TFTP[Planet][GS-4212]	
○	4	Backup Script for TFTP[Fortinet][FS-424D]	Backup	FS-424D	execute backup confi ...(show)	Backup Script for TFTP[Fortinet][FS-424D]	
○	5	Backup Script for TFTP[DLink][DXS-1210]	Backup	DXS-1210	copy running-config ...(show)	Backup Script for TFTP[DLink][DXS-1210]	
○	6	Backup Script for TFTP[Cisco][C6807]	Backup	C6807-XL	copy running-config ...(show)	Backup Script for TFTP[Cisco][C6807]	

▶Device Inventory

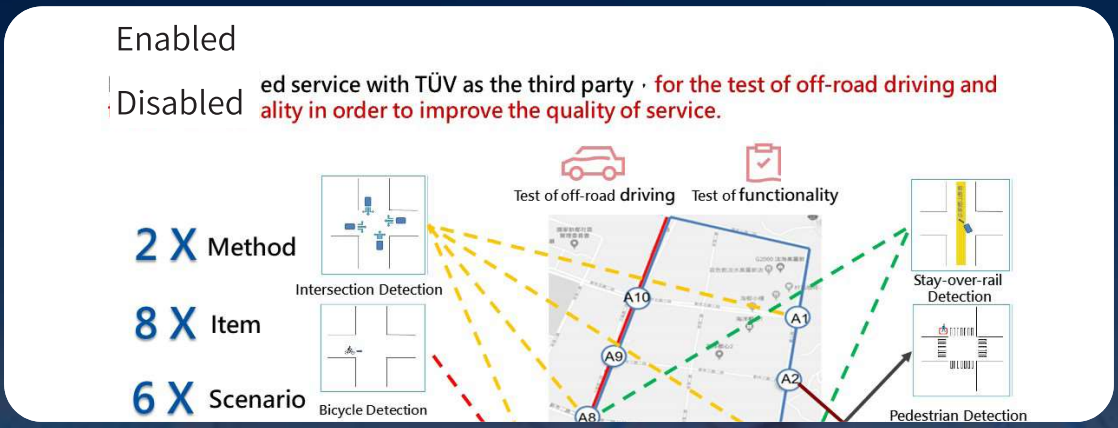
It provides the device list, including device brand, model name, serial number, production date, and other related information of devices. Through query function to view detailed information of monitor devices, and also provides import assets files to the system or export device lists for assets inventory.



Action	Seq	Show Detail	Device ID	Probe	Group	Device name	IP address	Device Type	Device Brand	Device model	System Version	SN	MFD	Status	Auto Sync
☐	1	Details	2043	Local Probe		Cisco C2960X	10.1.1.253	Network	Cisco	WS-C2960X-24TD-L	15.2(6)E	FOC2004S4JQ	2017-08-05	Using	Y
☐	2	Details	2076	Local Probe		Cisco ASR9K	10.1.1.227	Network	Cisco	R-IOSXRV9000-CH	6.0.1	D19D9D6427A		Using	Y
☐	3	Details	2085	Local Probe		ESXi Server	10.1.1.230							Using	Y
☐	4	Details	2102	Local Probe		Cisco N9K	10.1.1.226	Network	Cisco	N9K-9000v		9CIH366R47R	2018-06-14	Using	Y

▶ Customized equipment monitoring templates/items (Pro Version)

Simulation device panel to see real-time port usage - connected, disconnected, enabled, disabled, and monitoring data. We have customized services to provide monitoring templates for special devices such as DB, VMs, service devices, etc. Of course, to let the enterprise administrator understand important service data.



▶ Historical records of IP usage (Plus Version)

Collect IP and MAC addresses of connected devices in the network and record the online usage time of user IP, switch device name and port number of IP connection, which is convenient for administrators to query internal IP usage issues such as IP conflicts, IP usage allocation, and connection device location.

▶ Query Syslog

It can receive the system logs from different brand devices, output the result in regularized format after analyzing the log event categories, and realize the querying logs function of various equipment on a single interface.

▶ Network error detection (Plus Version)

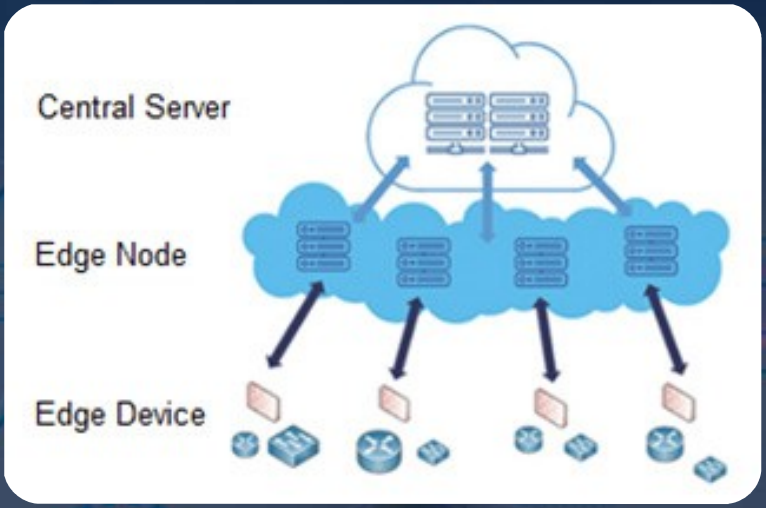
Detecting network errors occurring on devices, helping administrators find out network latency issues, thereby reducing the incidence of network problems such as LOOPBACK, CRC error, and ERRORDISABLE occur detection.

▶Simulate user behavior

Through simulating user behavior to detect abnormal system services, such as user login to the website behavior, simulating requirements DHCP, DNS..., etc.

▶Edge computing

For system design in special environments such as education networks and large enterprises with many branches, the edge computing server can become a regional management system and upload data to the central server for centralized control.



▶Various notification types

Support Messages, E-mail, Window POP-UP, Sound alarm, LINE Messages, Customize Trigger Actions…etc.

▶Application Programming Interface (API)

The network management system provides various REST API, and it can quickly grab out all the monitoring data from the system through the API so that enterprises are more accessible to integrate their systems, such as reporting systems, repair systems, etc.

Hwacom *Ace for Any*
SYSTEMS INC.

www.hwacom.com