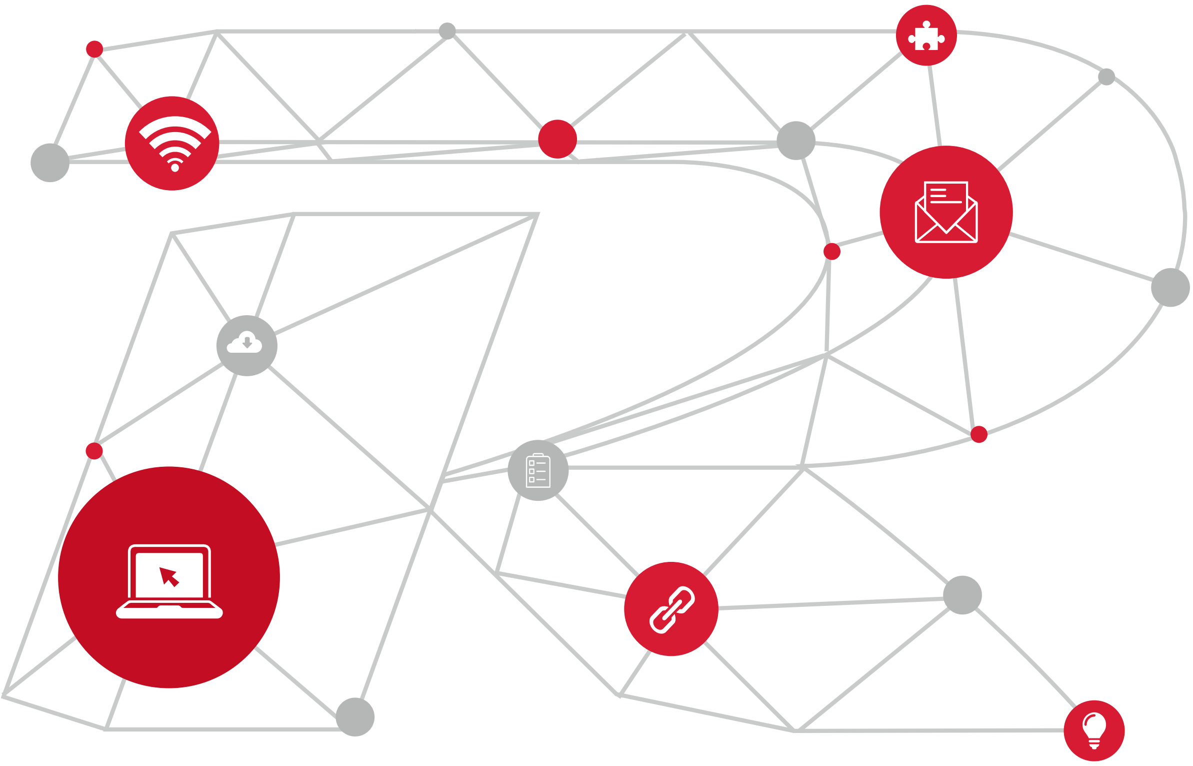
Ruijie Auto Smart Deployment For CCTV

White Paper



Contents

Overview

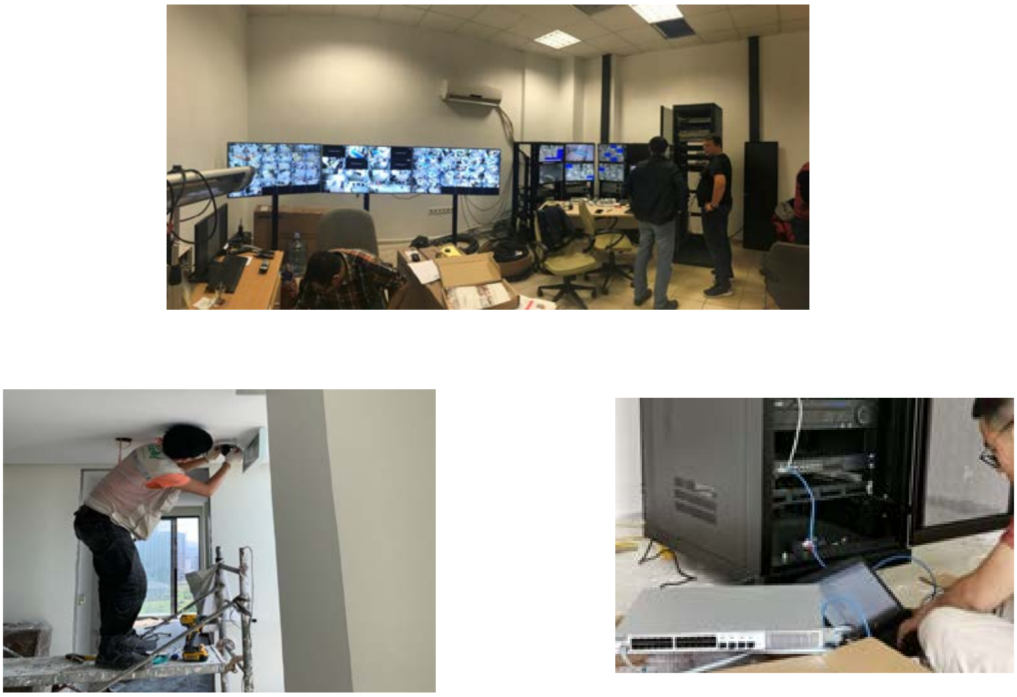
Auto Smart Deployment For CCTV is an automatic configuration solution designed to ensure the video quality of small-sized video surveillance networks. It can automatically identify cameras and network video recorders (NVRs) on a video surveillance network and deliver a series of features to ensure consistent and high video quality and save human labor for configuration and troubleshooting.

• SMEs' Video Surveillance Challenges

When video surveillance networks are constructed in hotels and offices, IP cameras (IPCs) with a data rate of 2 Mbit/s to 4 Mbit/s are used for the video surveillance subsystem. Survey results show that many users once encountered frame freezing or pixelization. Theoretically, 100M access switches and 1000M aggregation switches currently used for networking support switching capacities far beyond communication requirements of cameras and NVRs. However, network O&M personnel are still confronted with frame freezing.

Before principle introduction, this document clarifies typical deployment of SMEs' video surveillance networks.

Figure 1-1 Typical Deployment of SMEs' Video Surveillance Networks



(1) Less than 100 cameras, one or two NVRs, and an independent surveillance room are used.

(2) A video surveillance network uses an independent broadcast domain. However, a network device may access the video surveillance network, wireless network, and office network at the same time.

(3) On-site network deployment engineers only need to master simple configuration and network interconnection operations, for example, network cable preparation and interconnection, VLAN configuration, and basic port configuration.

However, when frame freezing or pixelization occurs during video surveillance network deployment or maintenance, engineers shall have high troubleshooting capabilities. Most engineers employed for deploying and maintaining SMEs' video surveillance networks from the construction party or integrator play multiple roles and are incapable of professional network troubleshooting. They may spend much time on random guessing and verification, affecting their reputation.

Actually, most frame freezing and pixelization problems on simple video surveillance networks can be resolved centrally using few configurations. However, these configurations are not related logically. Missing or incorrect configuration easily occurs. In addition, these configurations need to be performed for devices one by one. The function of each configuration will be explained later. The configurations include:

- Flow control
- Jumbo frame
- Port isolation

• Ruijie Auto Smart Deployment For CCTV Solution

To resolve the preceding problems, Ruijie provides the Auto Smart Deployment For CCTV solution to automatically identify IPCs and NVRs on a video surveillance network and deliver mandatory configurations to ensure the video quality, making the deployment of IP-based video surveillance networks simple and intelligent.

Basic Principles

• SMEs' Video Surveillance Network Deployment Procedure

A typical IP-based video surveillance network has the following features:

• In typical surveillance scenarios, for example, offices and hotels, cameras are deployed at aisles on different floors and public halls.

• Cameras are connected to the box-type switches through network cables. The number of ports on a switch ranges from 8 to 24. Typically, the camera accesses the network at a bandwidth of 100 Mbit/s in power over Ethernet (PoE) mode. PoE dramatically reduces the cabling cost.

• The access switches are converged at a core switch. Typically, the two-tier architecture is capable of supporting a video surveillance network with less than 100 cameras.

• The whole video surveillance network is in one broadcast domain. Engineers only need one surveillance VLAN and one management VLAN for Telnet access during device O&M.

• Theoretically, 100M access switches and 1000M box-type aggregation switches are far enough for video surveillance at the 4 Mbit/s data rate and 1080P definition. The redundant bandwidth may be used by other networks, such as Wi-Fi networks.

To construct a complete video surveillance network, perform the following steps in sequence:

(1) Plan IP addresses. Plan information, such as the locations, IP addresses, and SNs of cameras and configure the information on the Web UI one by one. The detailed procedure is as follows:

Unpacking > Startup > Web configuration > Restart for confirmation > Sealing > Packing

a) Alternatively, use the DHCP server function of NVRs or the Hikvision's SADP software to directly assign IP addresses to cameras. However, such a case does not apply to projects with complex scenarios in which IP addresses need to be planned in advance.

(2) Ship materials to the installation site and make and route network cables. Installation personnel start to configure network devices.

(3) Construction personnel install cameras, and deployment personnel configure the Wi-Fi network or office network.

(4) After cameras are installed and connected to the video surveillance network, deployment personnel start to use the IP address scanning function on NVRs to scan the cameras' IP addresses and deliver images.

If frame freezing or pixelization occurs, engineers will call the corresponding construction site and ask installation personnel to remove and insert or replace the network cables. If the network cables are normal, deployment personnel cannot resolve the problem.

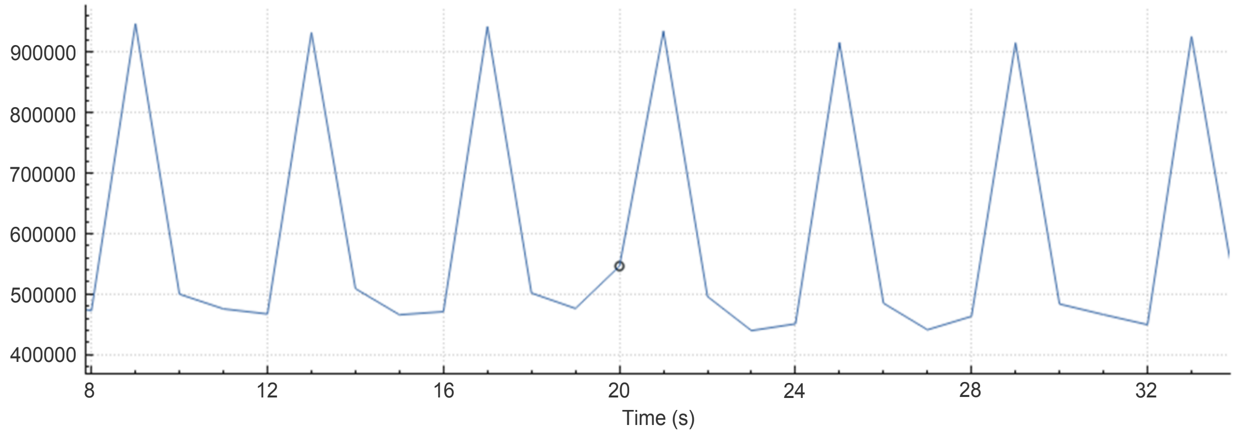
• Video Surveillance Problems

The following analyzes the frame freezing or pixelization problem occurring when the port bandwidth is enough as mentioned in section "SMEs' Video Surveillance Challenges."

Video Stream Waveform Analysis

Each IPC with H.264 encryption, 2 Mbit/s data rate, and 720P definition will send 25 image frames to the NVR every second. When the NVR communicates with a single camera and samples video stream packets at 1s intervals, the waveforms are shown in the following figure.

Figure 2-1 Video Streams Sampled at 1s Intervals



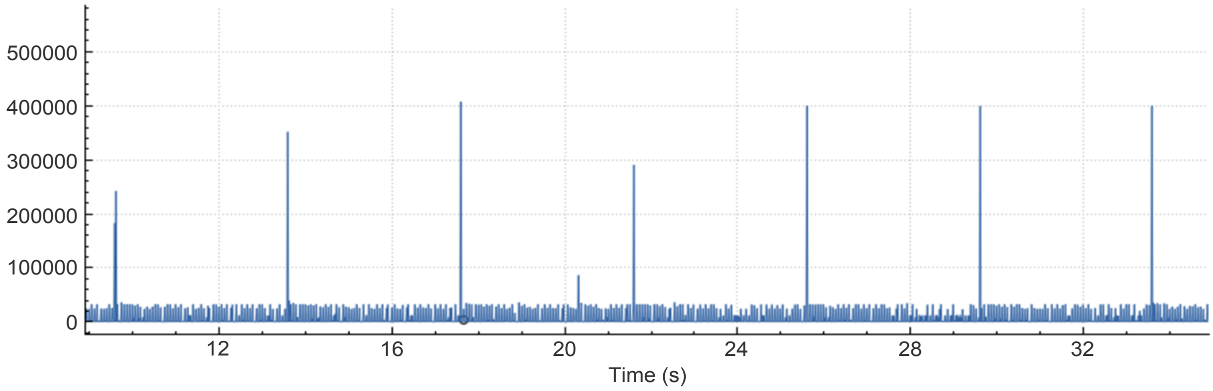
Typically, IP-based video streams present jagged I/O waveforms because of the H.264 or H.265 compression method. The peaks indicate I frame transmission, and the valleys indicate P frame transmission.

- I frame: a key frame that contains a complete image and a basic data frame used for video stream decoding.

- P frame: contains only information different from the previous neighboring I or P frame to indicate the difference between frames.

At 1s sampling intervals, the packet traffic at peaks is 900 kbit/s, which is not heavy. However, if the sampling period is set to 10 ms for the same video streams, the waveforms are shown in the following figure.

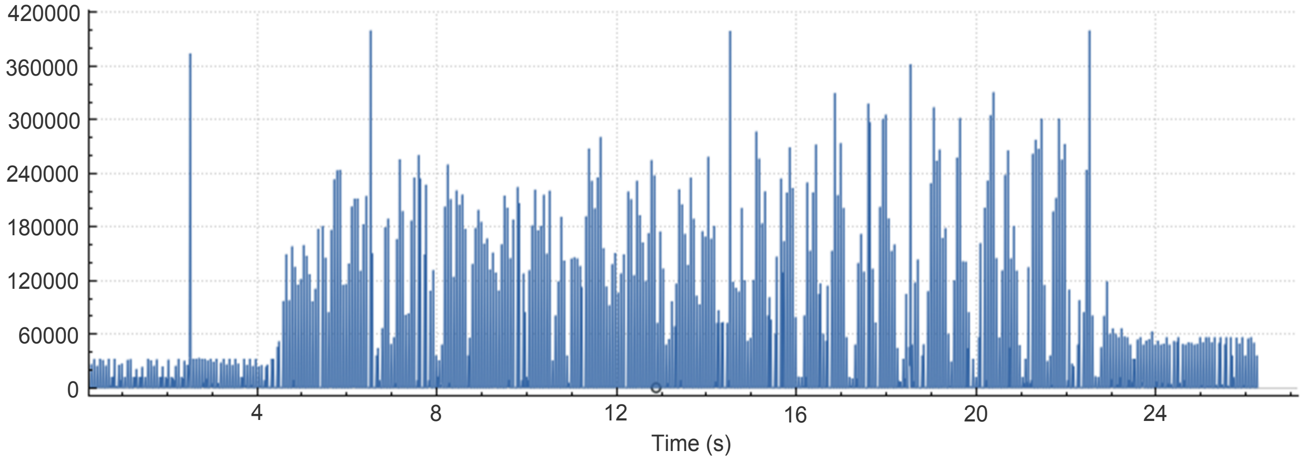
Figure 2-2: Video Streams Sampled at 10 ms Intervals



At 10 ms sampling intervals, the burst traffic of the I frames reaches 40 Mbit/s. When the traffic is used as the transient traffic of a camera, the impact on the network is small. According to description in section "SMEs' Video Surveillance Network Deployment Procedure," 8 to 24 cameras may be connected to the same switch. I frames of different cameras may overlay to form continuous and large-size I frame data.

In addition, the preceding traffic features appear only when the cameras detects no motion. When a large number of dynamic images exist on one camera, the I/O waveforms are shown in the following figure.

Figure 2-3: Video Streams Sampled at 10 ms Intervals with a Large Number of Dynamic Images



When a camera collects a large number of shaking images, the P frame length will increase obviously and approaches that of the I frame and a single camera will bring large traffic fluctuation. In addition, cameras connected to the same switch are physically close to each other. Multiple cameras possibly collect same videos with shaking images, resulting in burst packet traffic and severe vibration. The burst packet traffic and severe vibration very likely consume bandwidth exceeding the maximum processing bandwidth of the NVR in a short period of time and use up available space in the internal buffer of the switch. As a result, video stream losses or jitters may occur, causing frame freezing.

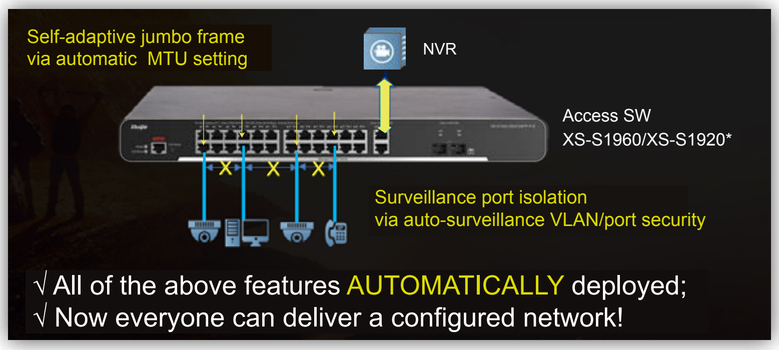
As a unified broadcast domain (VLAN) is planned for a video surveillance network, all cameras are in the same broadcast domain. In addition to directional unicast video streams to NVRs, the cameras periodically send multicast, broadcast, and unknown unicast packets, such as IGMP, ARP, MDNS, and auto IP packets. These packets do not have specified next-hop ports on the switch and will be flooded in the whole broadcast domain. According to the video surveillance network topology, only southbound-northbound packet exchange occurs when the NVR schedules surveillance traffic. Eastbound-westbound packet exchange (between cameras) is not required. The periodically flooded packets between cameras are invalid but occupy network bandwidth, which will affect the video surveillance quality in extreme conditions.

Principles of the Ruijie Auto Smart Deployment For CCTV Solution

To resolve the preceding problems, Ruijie provides the Auto Smart Deployment For CCTV solution to automatically identify connected IP cameras and NVRs and deliver key configurations to optimize the video quality. The configurations include:

- Flow control
- Jumbo frame
- Port isolation

Figure 3-1 Auto Smart Deployment For CCTV Solution Process


Self-adaptive jumbo frame
via automatic MTU setting
NVR
Access SW
XS-S1960/XS-S1920*
Surveillance port isolation
via auto-surveillance VLAN/port security
√ All of the above features AUTOMATICALLY deployed;
√ Now everyone can deliver a configured network!

With the Auto Smart Deployment For CCTV solution, the running switch system detects IP-based surveillance devices that access the network, and automatically delivers different surveillance optimization configurations over different ports. The solution ensures smart detection and deployment.

The Auto Smart Deployment For CCTV solution is designed for video surveillance image quality problems on SMEs' video surveillance networks. Typically, deployment engineers do not need to be capable of specific video surveillance network troubleshooting, and only need to deploy cameras and NVRs on the network based on the conventional operation process. The Auto Smart Deployment For CCTV solution will automatically identify devices and deliver configurations. The following describes implementation principles of the solution.

• Intelligent Device Identification

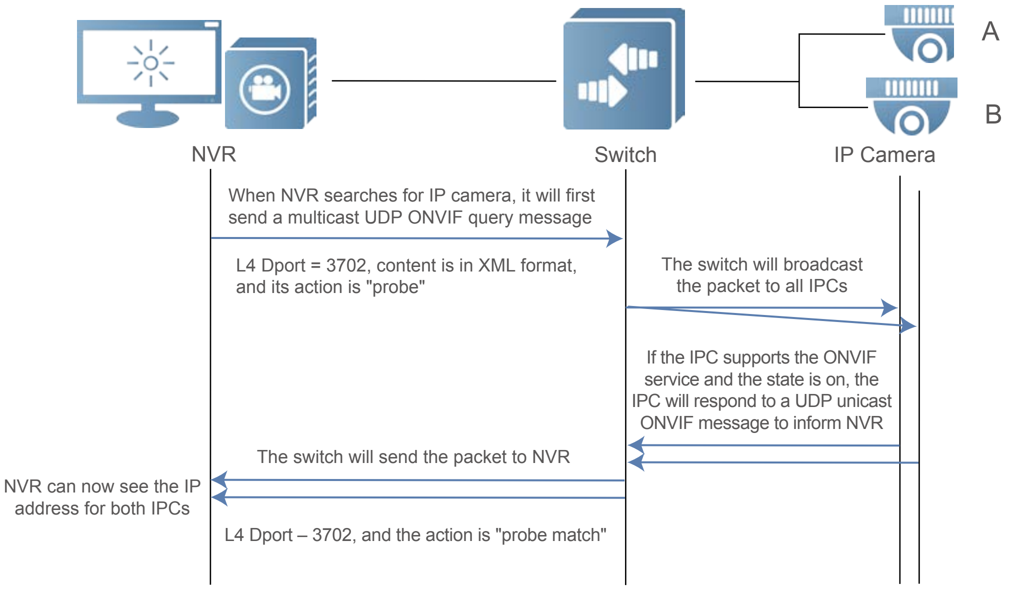
Accurate surveillance device identification is a difficult point in the Auto Smart Deployment For CCTV solution. First, the OUI field in MAC addresses cannot be used to effectively distinguish surveillance devices from non-surveillance devices, let alone NVRs from IPCs. Second, there are various surveillance device suppliers who comply with different handshake protocols for NVR and IPC interconnection.

To improve the identification accuracy, Ruijie combines multiple detection methods.

ONVIF Detection

Open Network Video Interface Forum (ONVIF) was an open forum for standard network video device interfaces jointly founded by Axis, Bosch, and Sony in 2008. It formulates common protocols for information exchange between network video devices based on the principle of openness. Mainstream suppliers privatize the standard ONVIF protocol to different extents. Typically, the NVR uses the ONVIF protocol to detect IPCs in compliance with the following process.

Figure 3-2 ONVIF Device Detection Process


A
B
NVR
Switch
IP Camera
When NVR searches for IP camera, it will first send a multicast UDP ONVIF query message
L4 Dport = 3702, content is in XML format, and its action is "probe"
The switch will broadcast the packet to all IPCs
If the IPC supports the ONVIF service and the state is on, the IPC will respond to a UDP unicast ONVIF message to inform NVR
The switch will send the packet to NVR
NVR can now see the IP address for both IPCs
L4 Dport – 3702, and the action is "probe match"

During the process, the switch captures ONVIF device detection packets, identifies the communication parties' roles, and delivers optimization configurations by role.

However, only ONVIF detection may have the following problems:

• ONVIF device detection packets exist only when the NVR adds cameras. If the NVR has added cameras before the video surveillance network is deployed, the NVR will not perform ONVIF device detection during deployment. As a result, the switch may fail to capture ONVIF device detection packets.

• To meet proprietary requirements, some suppliers disable the standard ONVIF protocol by default and use their own private device detection mechanisms. With only ONVIF detection, some surveillance devices may fail to be identified. As a result, the configuration effect cannot be achieved.

To deal with the ONVIF detection defects, Ruijie also adopts the following two methods:

Traffic Characteristic Dictionary

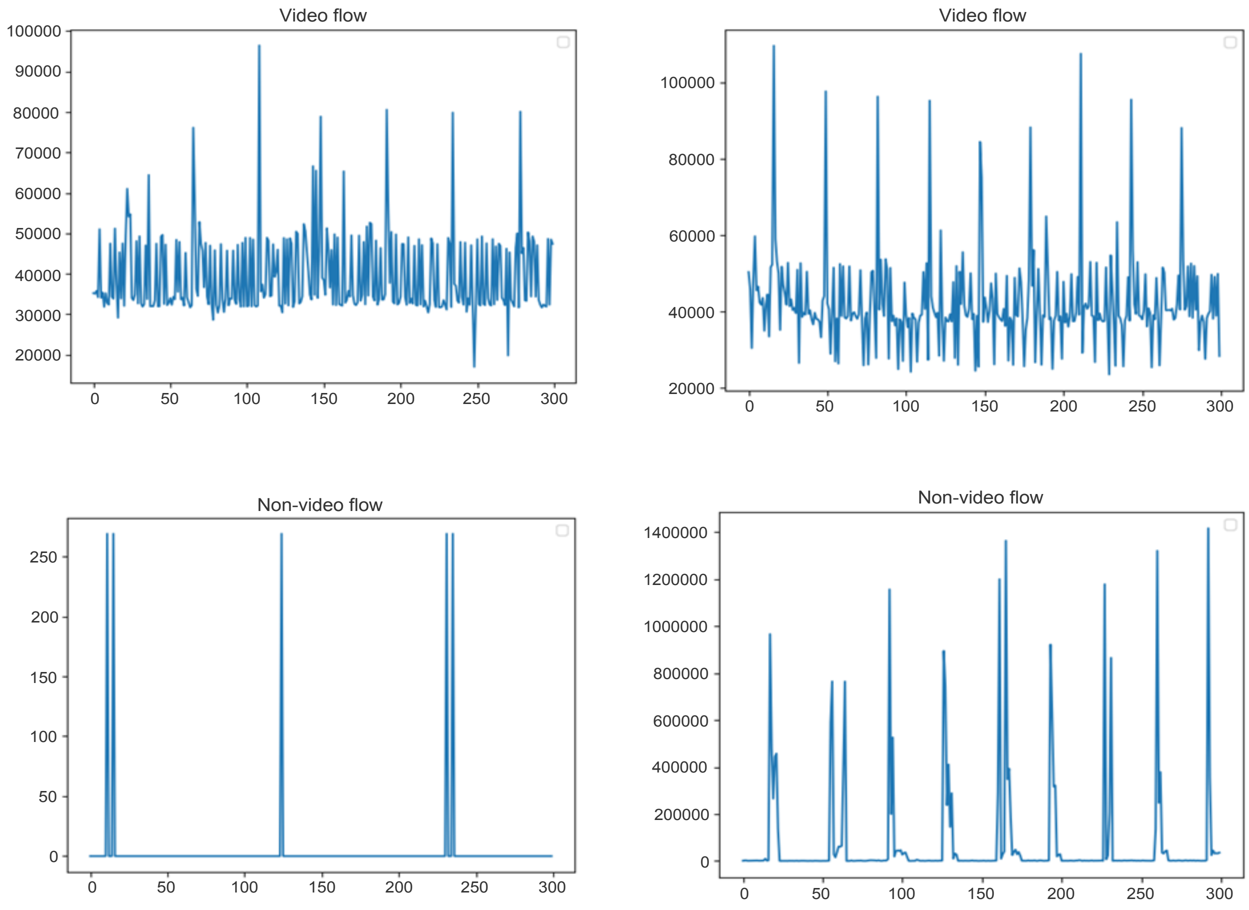
As video streams are continuous and have alternate I and P frames, the switch can identify the features of received video streams.

A single video packet does not have obvious features. Both NVRs and cameras support variable RTSP port configurations on RTSP video stream communication ports except port 554 defined in the standard. In addition, ACL matching domain selection for a low-end layer-2 switch is incomplete. Video stream features can be identified using a simple neural network classifier due to their particularity.

In the implementation process, video stream data sets are trained on the server. After parameter optimization, the classification formulas are input to the switch. The switch periodically collects and determines the traffic features, such as the rate.

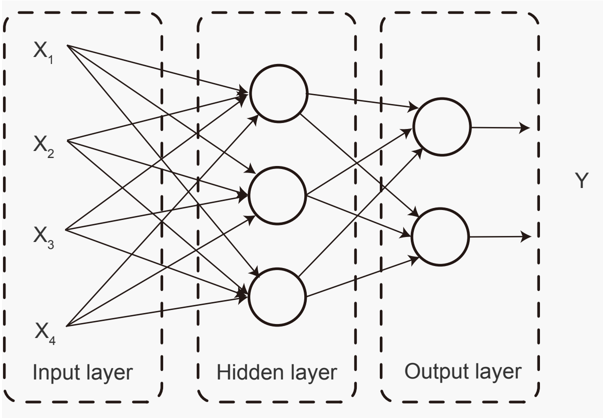
In actual processing, the Auto Smart Deployment For CCTV solution will measure traffic over the input and output ports and calculates the traffic over the ports every 100 ms. Figure 3-3 shows part of the data. The former two figures indicate the video surveillance traffic, and the latter two figures indicate other traffic.

Figure 3-3 Statistical Traffic Characteristics



Whether a device connected to a port is a surveillance device can be determined according to the differences of traffic over a port. The neural network training library in use is TensorFlow. It provides the Python-based neural network training solution, based on which the customer can deploy the training environment and convert obtained results into mathematical models and import them to the switch. Figure 3-4 shows the neural network training model.

Figure 3-4 Neural Network Training Model



The learned model is imported to the switch as the traffic determination basis. Then, traffic collected in the switch is processed and input to the model for traffic determination.

OUI Field Library

In addition to classification formulas exported using neural network training models, the Auto Smart Deployment For CCTV solution inputs the OUI fields in the MAC addresses of video surveillance devices provided by mainstream suppliers to improve the video surveillance device identification rate. The OUI field library covers the following suppliers:

- Hikvision
- Dahua
- Honeywell
- Hanwha
- Uniview
- Bosch
- Axis
- ASSA ABLOY
- FLIR
- Johnson Controls
- Aiphone
- Samsung
- Panasonic
- Sony

Through the preceding identification measures, the Auto Smart Deployment For CCTV solution can accurately identify NVRs and IPCs. Then, optimization configurations will be delivered automatically.

• Automatic Optimization

After video surveillance devices are identified, the Auto Smart Deployment For CCTV solution delivers several key configurations to reduce the impact of burst traffic caused by I frame overlay.

Flow Control: Effective Utilization of the Device Buffer

In IP-based video surveillance scenarios, the switch receives multiple packet streams from cameras. When I frames overlay frequently, the inbound traffic will exceed the maximum processing bandwidth of the outbound NVR quickly. Then, the switch's internal buffer will be used up, and a packet loss may occur for a short period of time. This is a typical producer-consumer problem. Then, the optimal solution to it is to use buffers of IP cameras. In typical scenarios, the buffers of IP cameras can be used to resolve the burst traffic problem. To use the NIC chip of IP cameras for buffering, the flow control mechanism is required.

Figure 3-5 A Simplified Video Surveillance Scenario

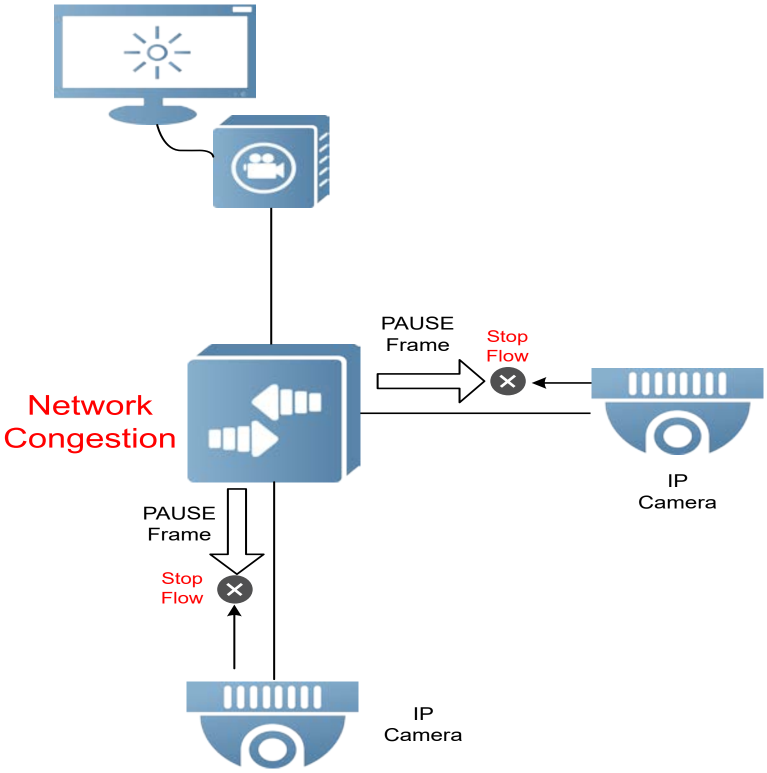


Figure 3-5 shows a simplified video surveillance scenario. Four NVRs are connected to one switch and four 720P IP cameras. The maximum video stream processing bandwidth of an NVR is 50 Mbit/s. The four IP cameras are deployed along an aisle. When a large number of people move along the aisle, the four IP cameras will capture continuous motion, and may transmit over 50 Mbit/s traffic to the NVR, resulting in video frame losses.

In this case, the flow control mechanism takes effect: the IP cameras receive PAUSE frames. Then, the cameras buffer the exceeded packets and send these packets with a slight delay, thus preventing packet loss. By adopting this mechanism, even when traffic overlay causes burst traffic, video frame losses and freezing can be eliminated.

Port Isolation: Removal of Eastbound-Westbound Traffic

As mentioned in section "Video Stream Waveform Analysis", IPCs on a video surveillance network will periodically send multicast, broadcast, and unknown unicast packets, such as IGMP, ARP, MDNS, and auto IP packets. These packets do not have specified next-hop ports on the switch and will be flooded in the whole broadcast domain, resulting in a bandwidth waste.

To resolve the problem, the Auto Smart Deployment For CCTV solution delivers the port isolation feature to ports connected to IPCs detected. Isolated network ports cannot forward layer-2 packets to each other. However, non-isolated ports can communicate with isolated ports. This ensures that eastbound-westbound traffic on a video surveillance network does not occupy additional bandwidth and O&M personnel can access the Web UI of IPCs for routine O&M.

Jumbo Frame: Compatible Adaptation

Typically, the length of a complete I frame exceeds the maximum Ethernet frame length stipulated in the IEEE 802.3x standard. IPCs will split the I frame into fragments and send the fragments to the NVR. During project deployment, it is found that IPCs provided by some suppliers have the jumbo frame feature enabled by default to improve the video traffic bandwidth utilization.

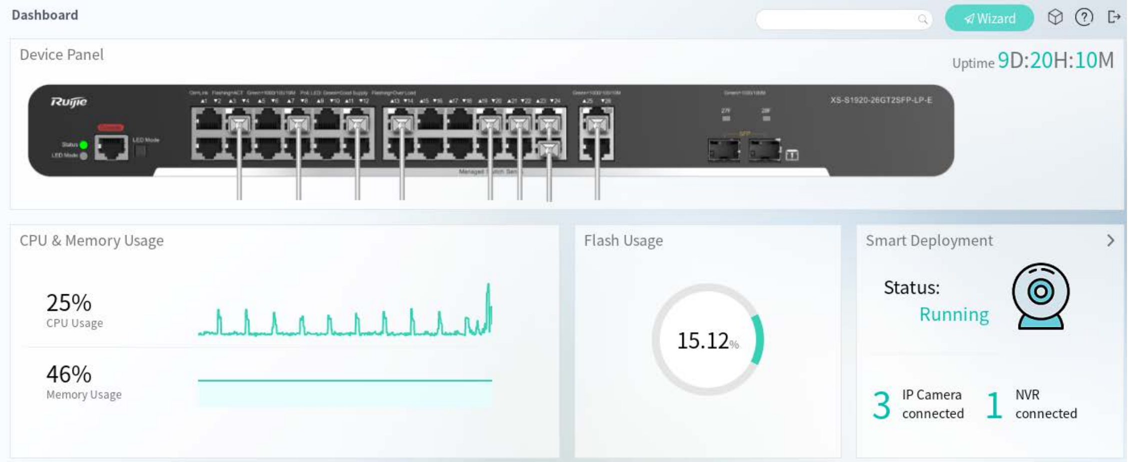
When an IPC with the jumbo frame feature enabled sends the complete I frame, packets will be lost and frame freezing occurs if the switch port does not enable the jumbo frame feature.

The Auto Smart Deployment For CCTV solution automatically delivers the jumbo frame feature to ports connected to IPCs, so that IPCs with the jumbo frame feature enabled are compatible.

Auto Smart Deployment For CCTV Application Case

As shown in the following figures, two IPCs and one NVR are connected to the switch. The switch automatically identifies the locations, roles, go-online time, and IP addresses of the IPCs and NVR and the PoE power consumption of IPCs.

Figure 4-1 Auto Smart Deployment For CCTV on the Homepage of the Switch Web UI



Uptime 9D:20H:10M

CPU & Memory Usage

25% CPU Usage

46% Memory Usage

Flash Usage

15.12%

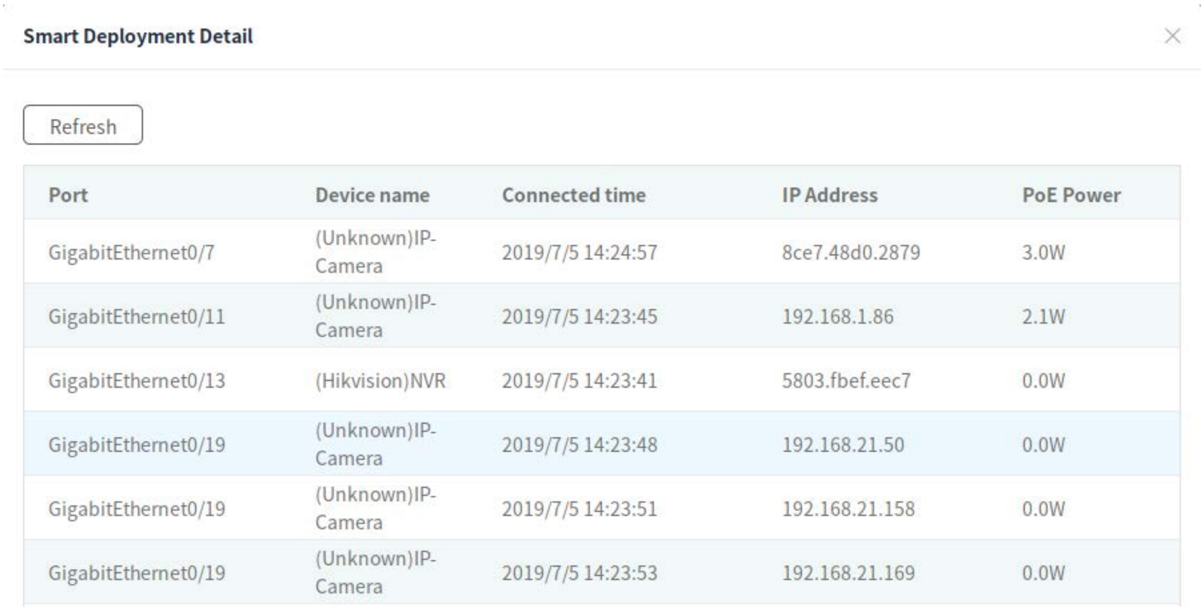
Smart Deployment

Status: Running

3 IP Camera connected

1 NVR connected

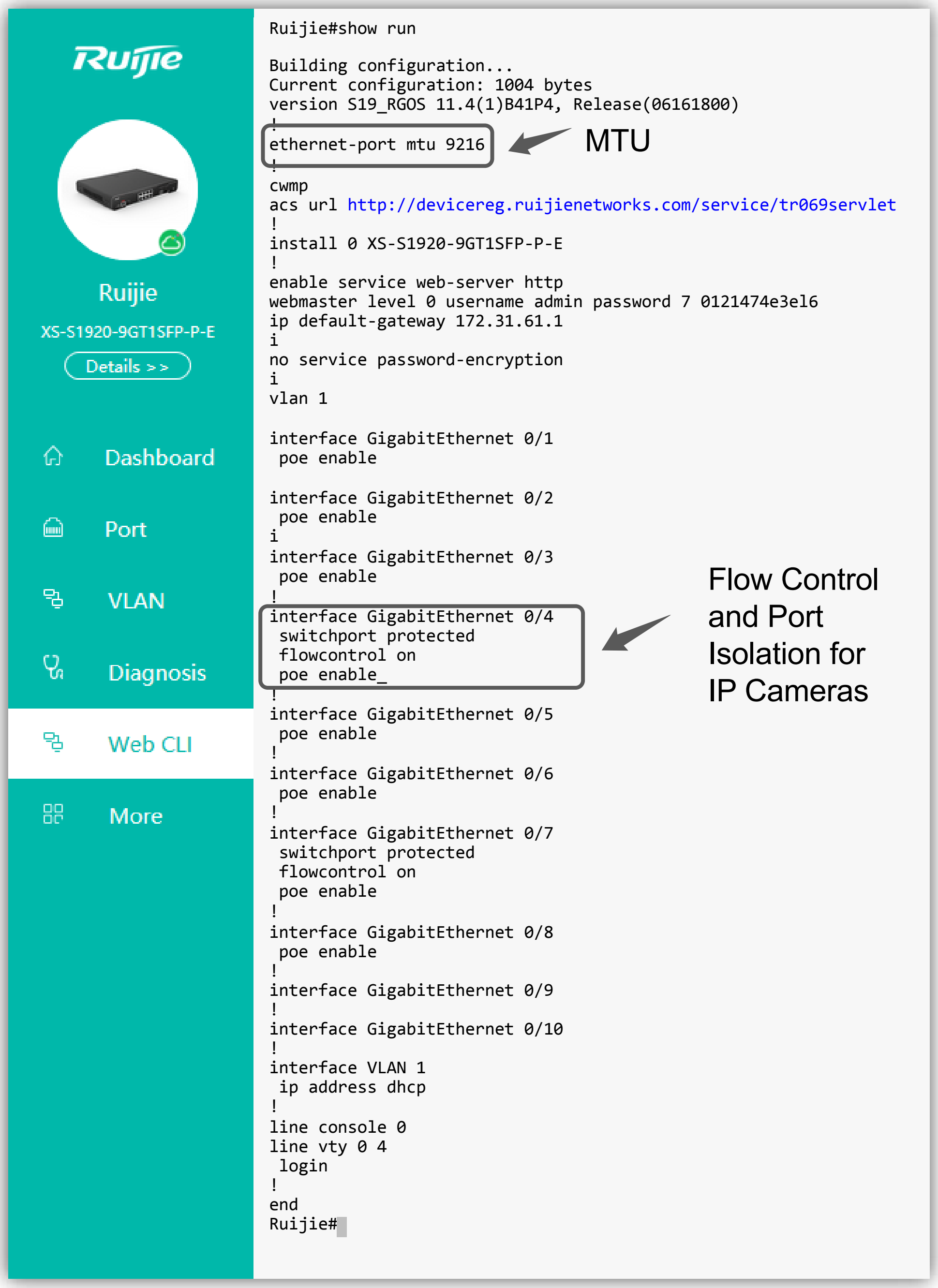
Figure 4-2 Auto Smart Deployment For CCTV Details on the Switch Web UI



Port	Device name	Connected time	IP Address	PoE Power
GigabitEthernet0/7	(Unknown)IP-Camera	2019/7/5 14:24:57	8ce7.48d0.2879	3.0W
GigabitEthernet0/11	(Unknown)IP-Camera	2019/7/5 14:23:45	192.168.1.86	2.1W
GigabitEthernet0/13	(Hikvision)NVR	2019/7/5 14:23:41	5803.fbef.eec7	0.0W
GigabitEthernet0/19	(Unknown)IP-Camera	2019/7/5 14:23:48	192.168.21.50	0.0W
GigabitEthernet0/19	(Unknown)IP-Camera	2019/7/5 14:23:51	192.168.21.158	0.0W
GigabitEthernet0/19	(Unknown)IP-Camera	2019/7/5 14:23:53	192.168.21.169	0.0W

When IPCs are identified, related optimization configurations are delivered.

Figure 4-3 Configuration Interpretation on the Web CLI Tab



```
Ruijie#show run

Building configuration...
Current configuration: 1004 bytes
version S19_RGOS 11.4(1)B41P4, Release(06161800)
!
ethernet-port mtu 9216
!
cwmp
acs url http://devicereg.ruijienetworks.com/service/tr069servlet
!
install 0 XS-S1920-9GT1SFP-P-E
!
enable service web-server http
webmaster level 0 username admin password 7 0121474e3el6
ip default-gateway 172.31.61.1
i
no service password-encryption
i
vlan 1

interface GigabitEthernet 0/1
 poe enable

interface GigabitEthernet 0/2
 poe enable
i
interface GigabitEthernet 0/3
 poe enable
!
interface GigabitEthernet 0/4
 switchport protected
 flowcontrol on
 poe enable_
!
interface GigabitEthernet 0/5
 poe enable
!
interface GigabitEthernet 0/6
 poe enable
!
interface GigabitEthernet 0/7
 switchport protected
 flowcontrol on
 poe enable
!
interface GigabitEthernet 0/8
 poe enable
!
interface GigabitEthernet 0/9
!
interface GigabitEthernet 0/10
!
interface VLAN 1
 ip address dhcp
!
line console 0
line vty 0 4
 login
!
end
Ruijie#
```

For details about the video surveillance effect after the Auto Smart Deployment For CCTV solution is used, see the following video:

https://www.ruijienetworks.com/about/videos/1711

Conclusion

Auto Smart Deployment For CCTV is an automatic configuration solution designed to save the human labor for configuration and troubleshooting and ensure the video quality on small-sized video surveillance networks. It can automatically identify cameras and NVRs on a video surveillance network and deliver a series of features to ensure consistent and high video quality.

During video surveillance network deployment and maintenance, there are still many conventional low-efficient configuration and troubleshooting procedures. Ruijie will continue to explore optimization methods for video surveillance networks and provide more effective solutions to ensure simpler and more efficient video surveillance.

Ruijie Networks Co.,Ltd

For further information,please visit our website **http://www.ruijienetworks.com**