Network Design Basics

Hikvision Certified Security Associate

First Choice for Security Professionals

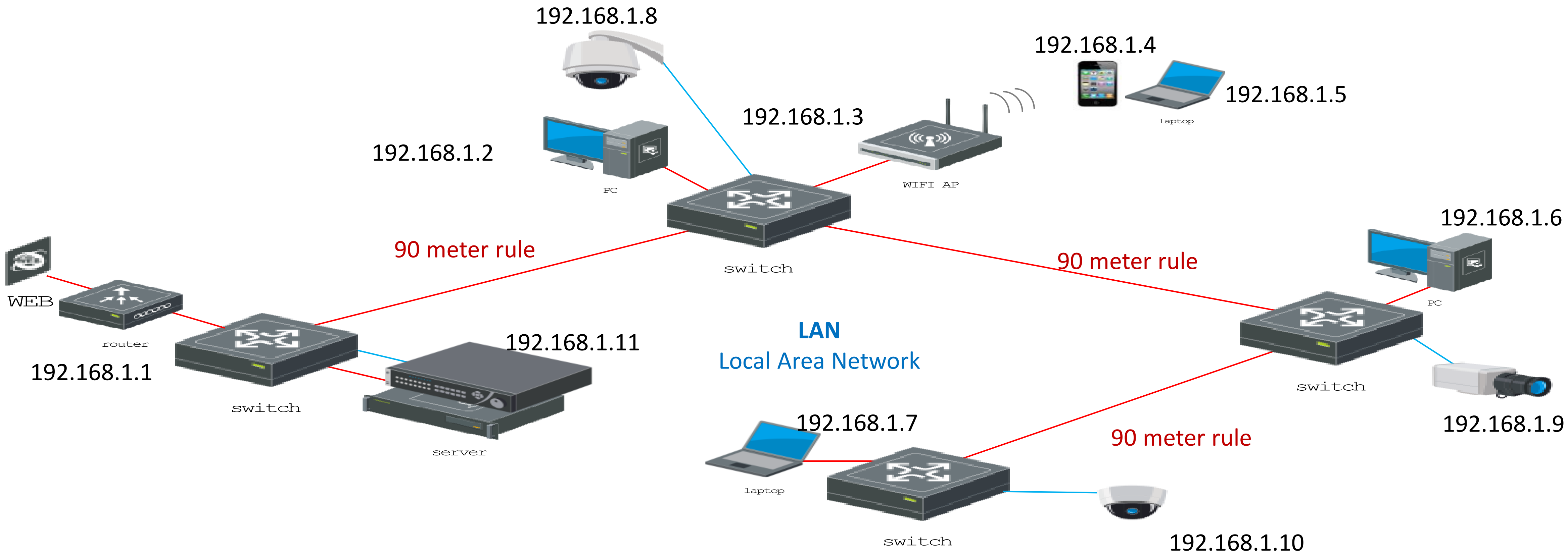
Contents

- **Network Basics**
- Network Device
- Network Planning
- Bandwidth Planning
- Network Security

Network Introduction

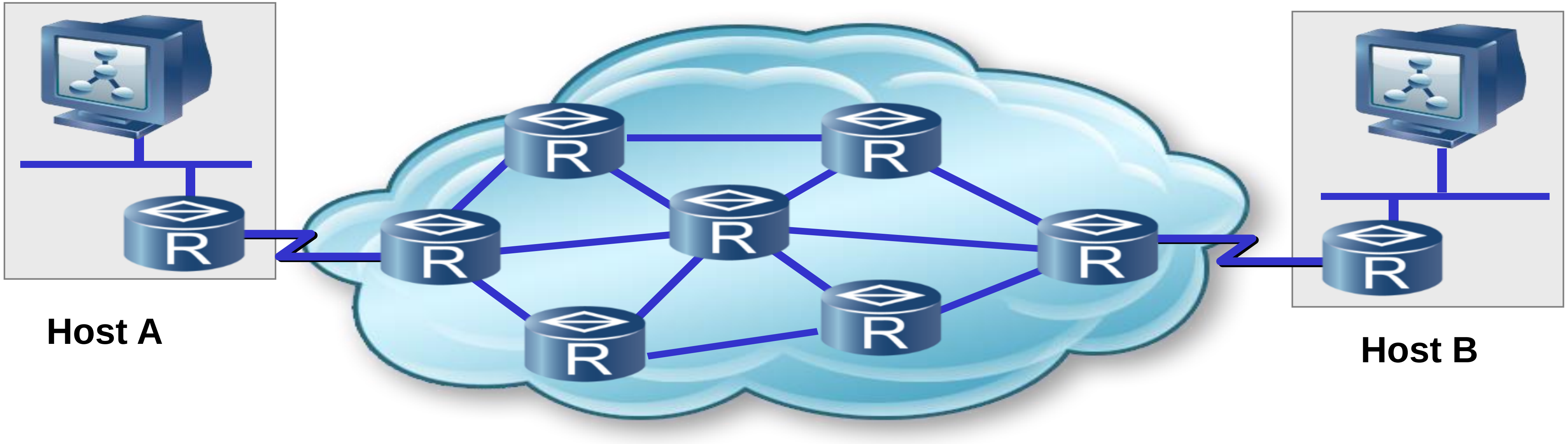
Network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data.

In video surveillance area, the network includes core switch, Ethernet cable, fiber, IP cameras, servers, etc.



IP Address

An IP address is the only way to identify a device in the network.



IPv4 Address

- IPv4 address is classified into 5 types: A, B, C, D, E
  - A: 1.0.0.0~126.255.255.255. The addresses between 127.0.0.0~127.255.255.255 is loopback address, for example, 127.0.0.1 is used for the local loopback test)
  - B:128.0.0.0~191.255.255.255
  - C:192.0.0.0~223.255.255.255
  - D:224.0.0.0~239.255.255.255
  - E:240.0.0.0~255.255.255.255 (255.255.255.255 is the network broadcast address)

- ➢ The addresses of A, B, C type is unicast address, which is used to identify interface. The message of destination address is called unicast message
- ➢ The addresses of D type is multicast address. The message of the addresses whose destination addresses is multicast addresses is multicast message.
- ➢ 255.255.255.255 is the address for broadcast, and the broadcast message will be received by all devices.

Private IPv4 Address

- Private IP address cannot be used on public network.
- On the public network, IP address is unique. While in different private networks, the private IP address can be the same. It is an effective way to save IP address.

10.0.0.0/8— 10.255.255.255/8

172.16.0.0/12— 172.31.255.255/12

192.168.0.0/16— 192.168.255.255/16

Subnet Mask

- Subnet mask is used to distinguish the network address and host address.
- Subnet mask consists of a succession of “1” and a succession of “0”.
  - “1” corresponds to network address and subnet address.
  - “0” corresponds to host address.
  - “1” and “0” cannot show up cross.

Example:

- 128.1.1.1/255.255.0.0
- 128.1.1.1/16

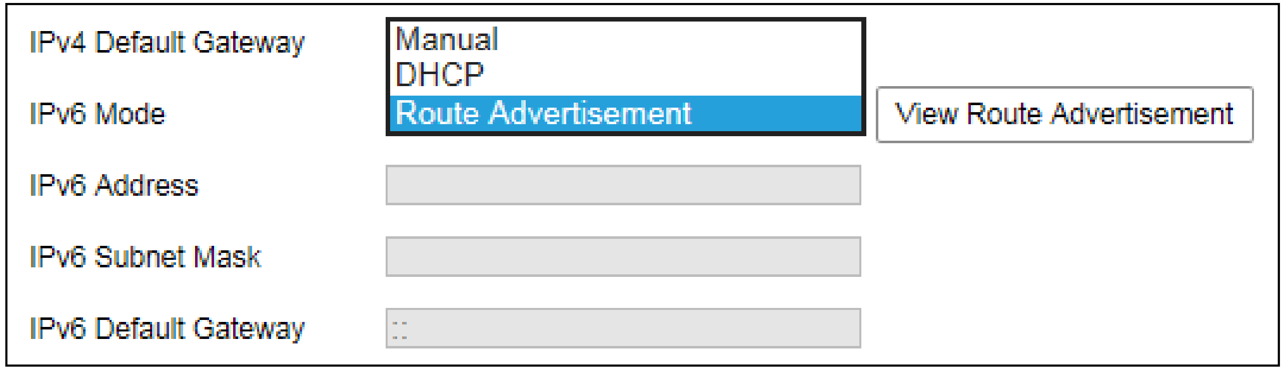
- 192.168.3.2/255.255.224.0
- 192.168.3.2/19

Why IPv6？

- Explosive growth of Internet users, devices, apps creates demand for more IP addresses.
- IPv4 uses 32-bit addresses and can support 4.3 billion devices connected directly to the Internet.
- The replacement protocol IPv6 uses 128-bit addresses and provides such a vast number of addresses that it can only be expressed mathematically: 3.4 x 10 to the 38th power.

IPv6

- An IPv6 address is written in hexadecimal notation with colons subdividing the address into eight blocks of 16 bits each.
- For example: 2001:0da8:65b4:05d3:1315:7c1f:0461:7847
- For Hikvision camera, it supports IPv6 with three mode:
  - Manually: Configure IPv6 address manually
  - DHCP: Get IPv6 address automatically from DHCP server
  - Route Advertisement: Get IPv6 address combining with route advertisement and its mac address.


IPv4 Default Gateway

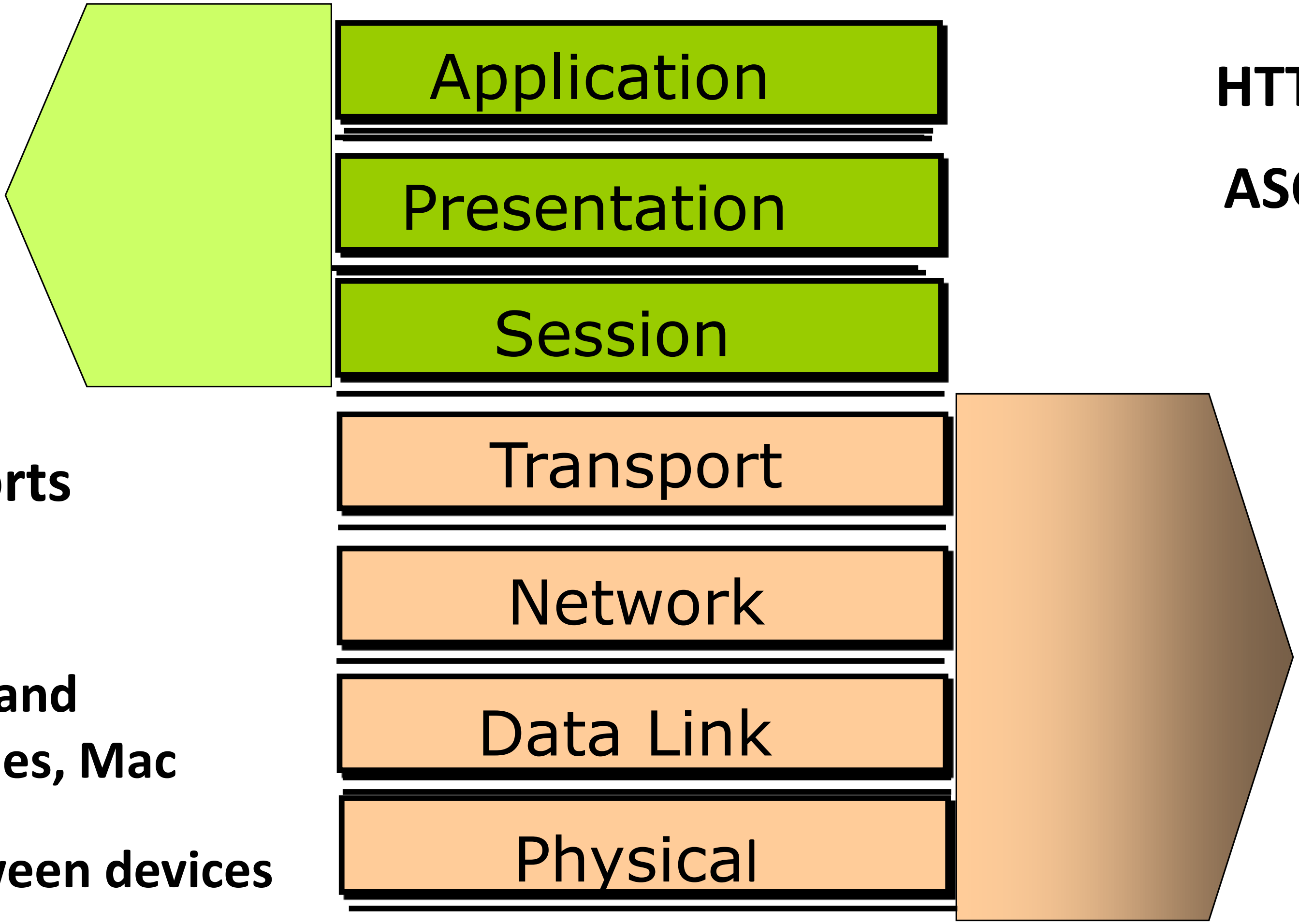
IPv6 Mode: Route Advertisement

IPv6 Address

IPv6 Subnet Mask

IPv6 Default Gateway: ::

OSI Reference Model



Application

Presentation

Session

Transport

Network

Data Link

Physical

Application

HTTP FTP DNS SMTP

ASCII JPEG

TCP UDP Ports

IP

Bits into bytes and bytes into frames, Mac

Move bits between devices

Data Flow

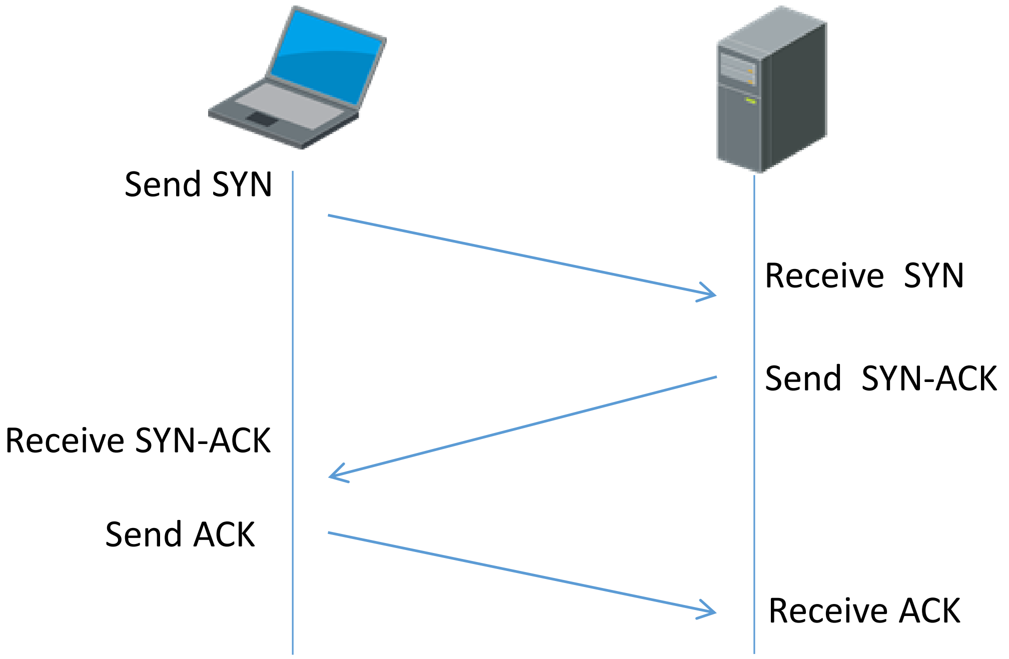
TCP

TCP (Transmission Control Protocol) is communication protocol of transmission layer which is connected and reliable based on a stream of bytes.

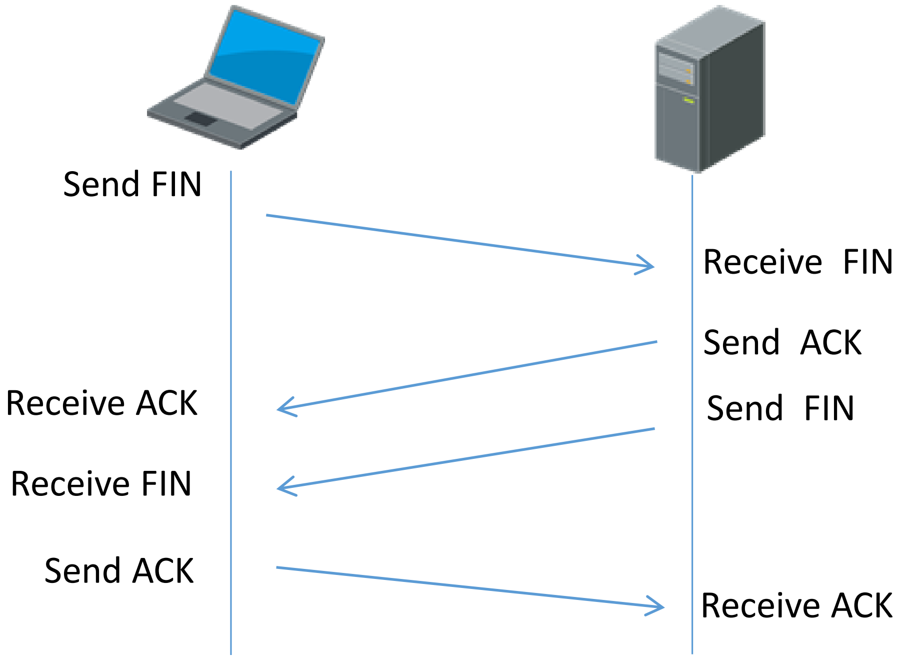
Load level of TCP is decided by MSS (maximum segment size). The transmitting end notices the maximum TCP data of each segmentation that receiving end can get.

MSS value is the difference that MTU value subtracts IPV4 Header (20 Byte) and TCP header (20 Byte). MTU(maximum transmission unit) is defined by hardware, for example, MTU of Ethernet is 1500 bytes.

Connect after three times handshake



Disconnect after four times handshake



TCP vs UDP

- **TCP(Transmission Control Protocol):** Ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected.
- **UDP(User Datagram Protocol):** Provides real-time audio and video streams.

TCP

- Connection oriented
- Provide reliable transmission
- FTP, HTTP

UDP

- Connectionless
- Provide unreliable transmission
- SNMP

Common Port Number

- 20 File Transfer Protocol [Default Data]
- 21 File Transfer Protocol [Control]
- 25 Simple Mail Transfer Protocol
- 80 World Wide Web HTTP
- 443 HTTPS
- 8000 Server(for software access)
- 554 RTSP

Port number range：0—65535

0—254	Public
255—1023	For company
1024 and above	Random

PoE Technology Overview

- IEEE 802.3af Common PoE standard
  - Power sourcing equipment（PoE switch or PoE Module） supply 48VDC, 15.4W power, PSE for short
  - Powered device receive 12.95W, short for PD

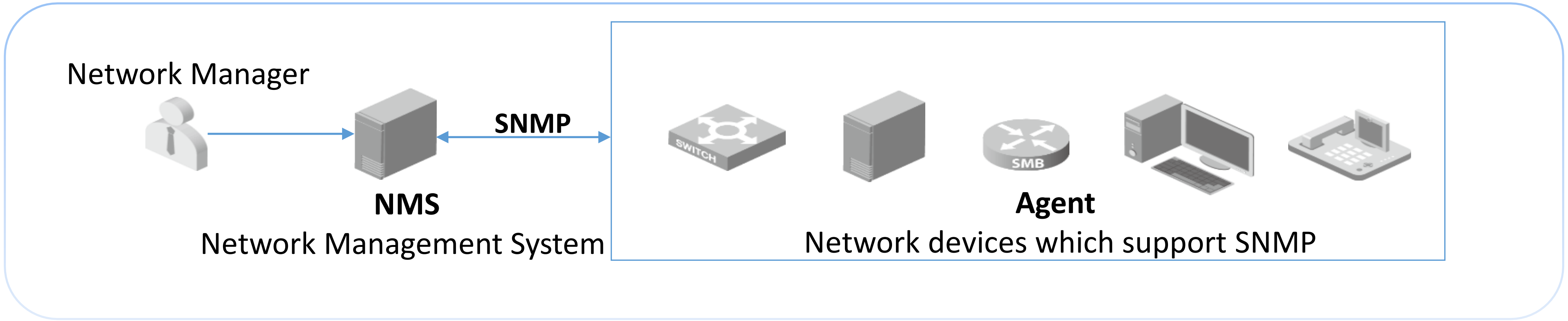
- IEEE802.3at PoE+ standard
  - Power sourcing equipment（PoE switch or PoE Module） supply 48VDC, 30W power
  - Powered device receive 25.5W
- PoE don’t affect cable transmission capability or distance
- It is Compatible with Non-PoE devices

PoE Features

Features	802.3af	802.3at
PD Power	12.95W	25.5W
PSE Power	15.4W	30W
PSE voltage range	44V-57V	50V-57V
PD voltage range	37V-57V	42.5V-57V
Cable type	CAT3 or CAT5	At least CAT5
Wire pairs for power supply	2	2 or 4

SNMP

- SNMP gives us the simplest way to monitor network devices’ working status information. Normally network devices will only offer Mib-2 working status information via SNMP.
- Any network device which supports SNMP can be managed via SNMP management software. These network devices include switches, routers, servers, IP phones and so on. The classic SNMP model is as following:



Network Manager

SNMP

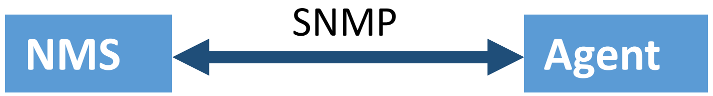
NMS

Network Management System

Agent

Network devices which support SNMP

Simplified SNMP Model:



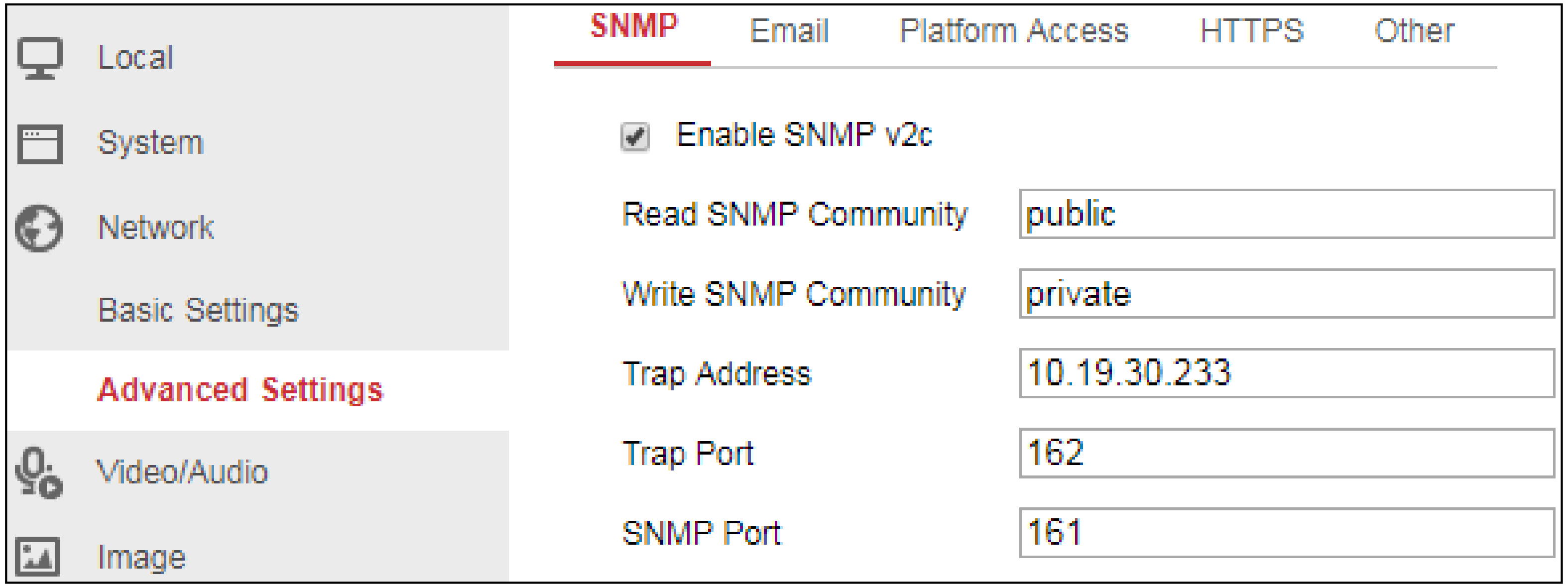
NMS

SNMP

Agent

SNMP

- Many Hikvison hardware devices support SNMP function. Customers can use software(such as SolarWinds) to monitor all devices’ running status via SNMP after enabled this function and typed in the trap Address, the SNMP management software can get all information from the device automatically.
- Some Hikvision software(such as maintenance software) use SNMP protocol to monitor the software component and hardware status.



☑ Enable SNMP v2c

Read SNMP Community: public

Write SNMP Community: private

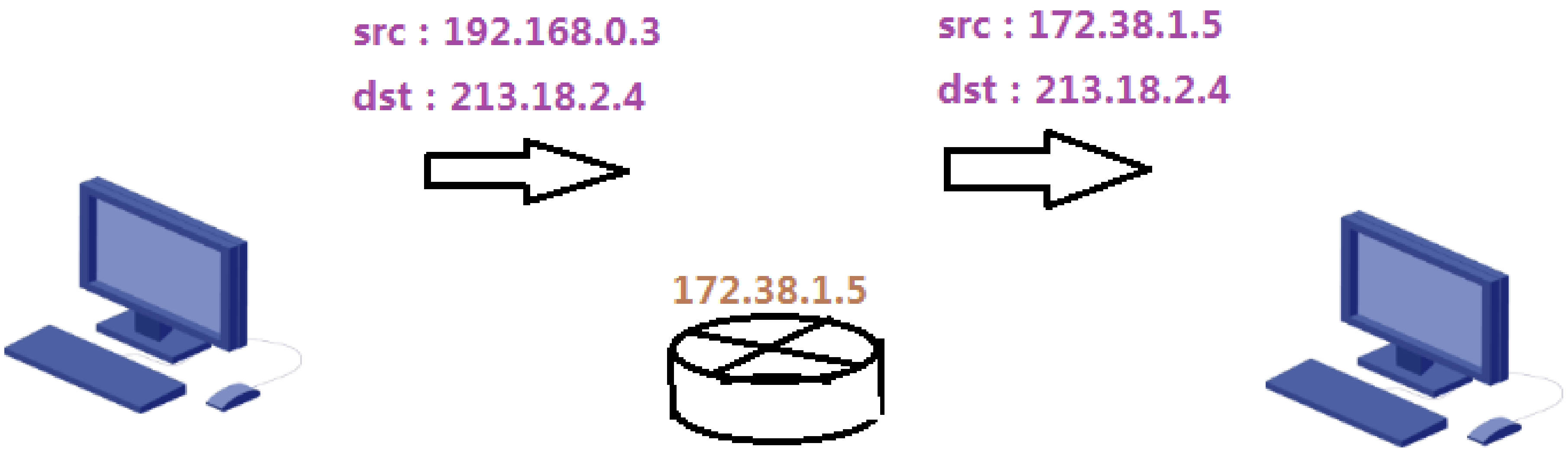
Trap Address: 10.19.30.233

Trap Port: 162

SNMP Port: 161

NAT

- In the computer network, NAT (Network Address Translation) is a technique which rewrites the source/destination IP address when the IP packets pass through a router.
- As the private IP address of local host can't be routed in public network, NAT can also "hide" the private IP address in the LAN so that it can protect internal network.



NAT

1. **Static NAT**

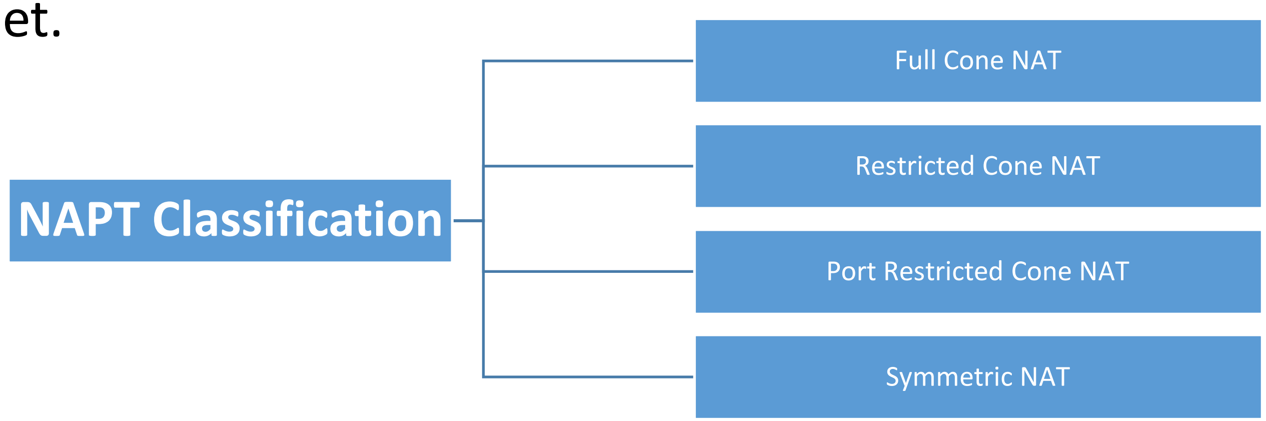
One-to-one mapping between public and private IP address——static configuration.

2. **Dynamic NAT**

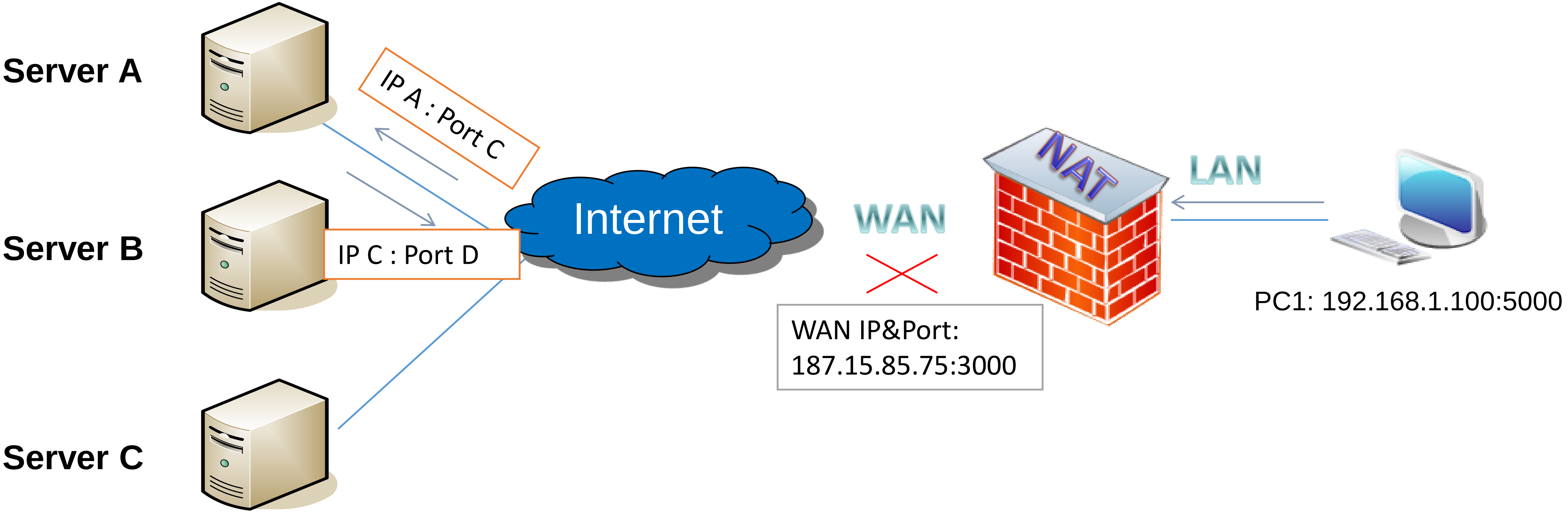
Setting a mapping between a public IP address and private IP address, it can build a shared IP address pool. We can select an IP address from the IP address pool and assign to a certain host, and the host will release the IP address after use.

3. **NAPT (Network Address Port Translation)**

Based on “IP + Port” address translation, building a mapping between {private IP, private Port } and {public IP, public Port}, so as to realize that multiple private IP can use a public IP to access the Internet.



NAT

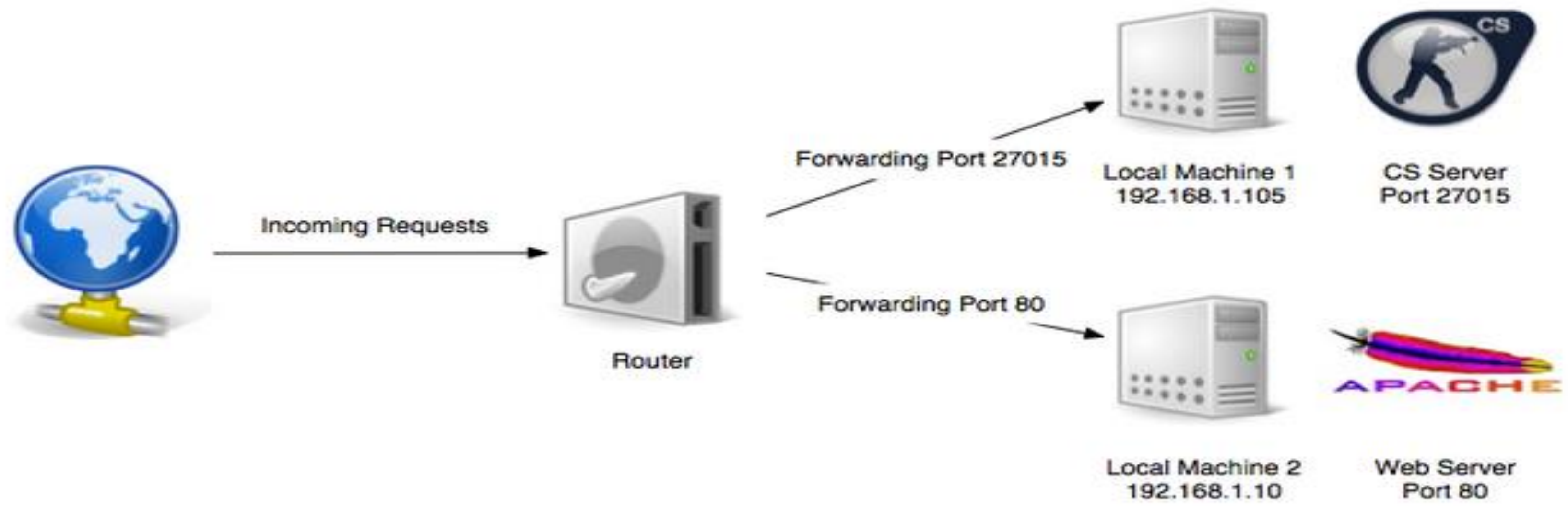


NAT will convert client address {192.168.1.100:5000} into a public address {187.15.85.75:3000} and bind them.

Only after the internal host 192.168.1.100 sends a data packet to the server A, then 192.168.1.100 can receive data packet sent by Server A to 187.15.85.75:3000.

Port Forwarding

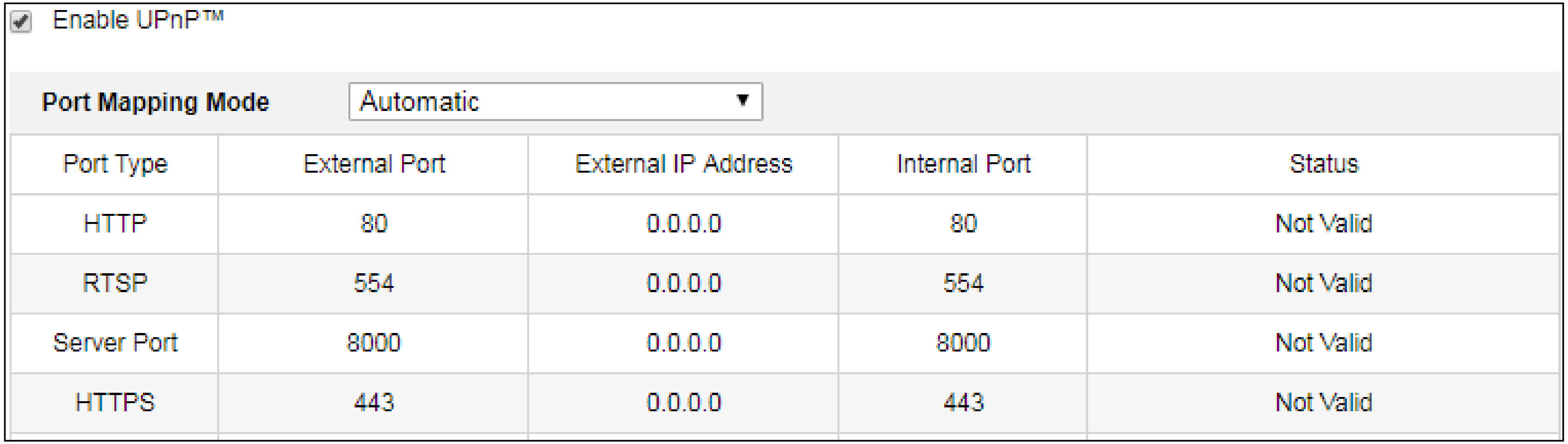
- What’s Port Forwarding?
  - Due to the presence of NAT,   the initiative access data flow of the external network will be discarded by NAT. In order to let the external initiative access reach the server behind NAT by Port Forwarding.
  - In short, Port Forwarding allows remote computer to connect to the certain computer or service in the internal network.



Port Forwarding

UPNP

UPNP can open the specific ports automatically by UPNP protocol, but it can only support monolayer NAT. You can see this function on hardware device, such as NVR and IPC.



☑ Enable UPnP™

Port Mapping Mode Automatic ▼

Port Type	External Port	External IP Address	Internal Port	Status
HTTP	80	0.0.0.0	80	Not Valid
RTSP	554	0.0.0.0	554	Not Valid
Server Port	8000	0.0.0.0	8000	Not Valid
HTTPS	443	0.0.0.0	443	Not Valid

Contents

- Network Basics
- **Network Device**
- Network Planning
- Bandwidth Planning
- Network Security

Common Transmission Media

Twisted pair cable

Fiber cable

Coaxial Cable

Wireless

Features of Different Media

Type	Data rate	Transmission media	Transmission distance
100BASE-TX	100MBit/s	CAT5	100M
100BASE-TX	100MBit/s	Multi Mode Fiber	2000M
1000BASE-SX	1000MBit/s	Multi Mode Fiber	500M
1000BASE-LX	1000MBit/s	Multi or Single Mode Fiber	2M to 5KM
1000BASE-T	10,000MBit/s	CAT5E	100M
10G BASE-LX4	10,000MBit/s	Multi or Single Mode Fiber	2M to 10KM
10G BASE-T	10,000MBit/s	CAT6 or CAT7	100M

Network Interface Card

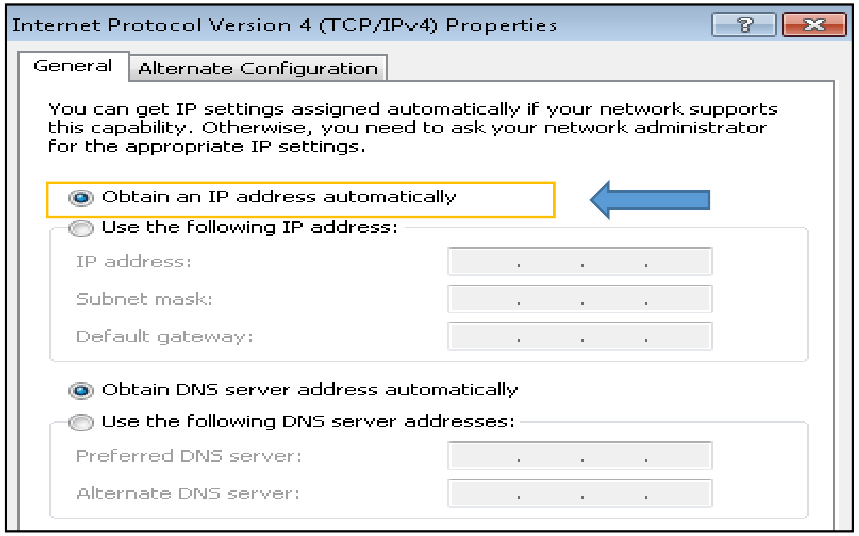
- NIC Interface Type includes PCI, PCI-E, USB
- Each NIC has a unique 48 bit hex address, which is call MAC address
- NIC allows devices to be communicate through network

How does the PC obtain an IP address

Dynamic Host Configuration Protocol (DHCP)

NIC can access available IP address from DHCP server, and DHCP server is usually the router or switch with IP allocation function.

Select *obtain an IP address automatically* in NIC properties.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

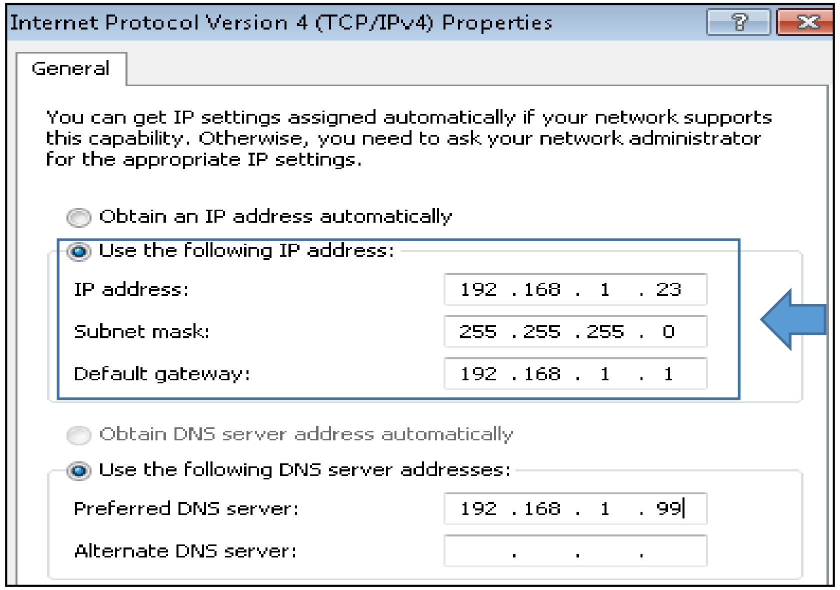
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Configure IP address manually

You can configure IP address manually, and please make sure that the IP address is available, and the subnet mask and gateway is correct.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 23

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

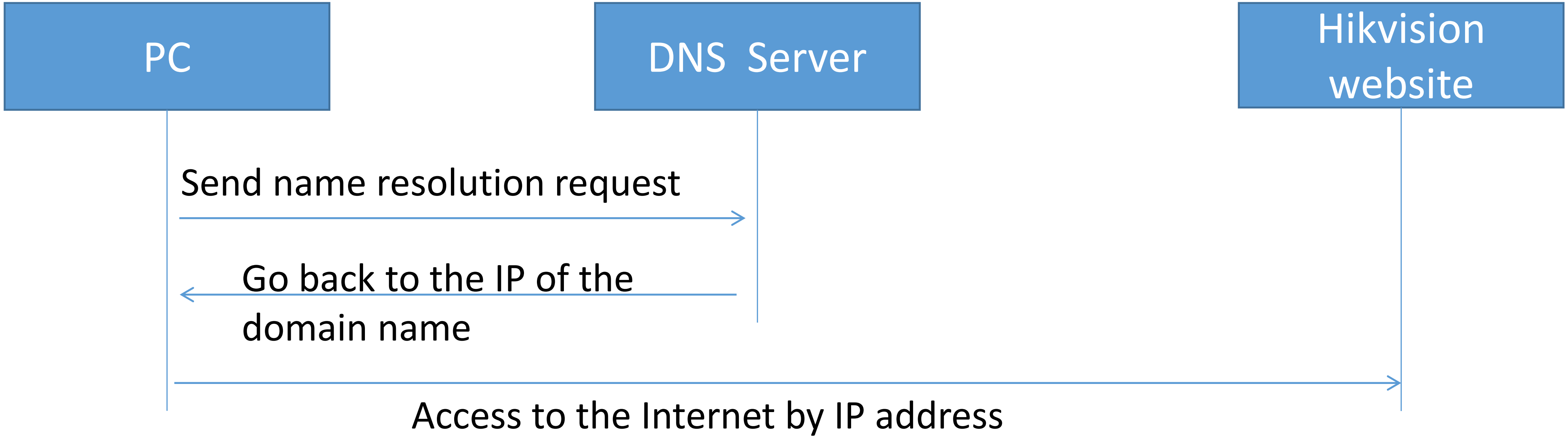
Preferred DNS server: 192 . 168 . 1 . 99

Alternate DNS server: . . .

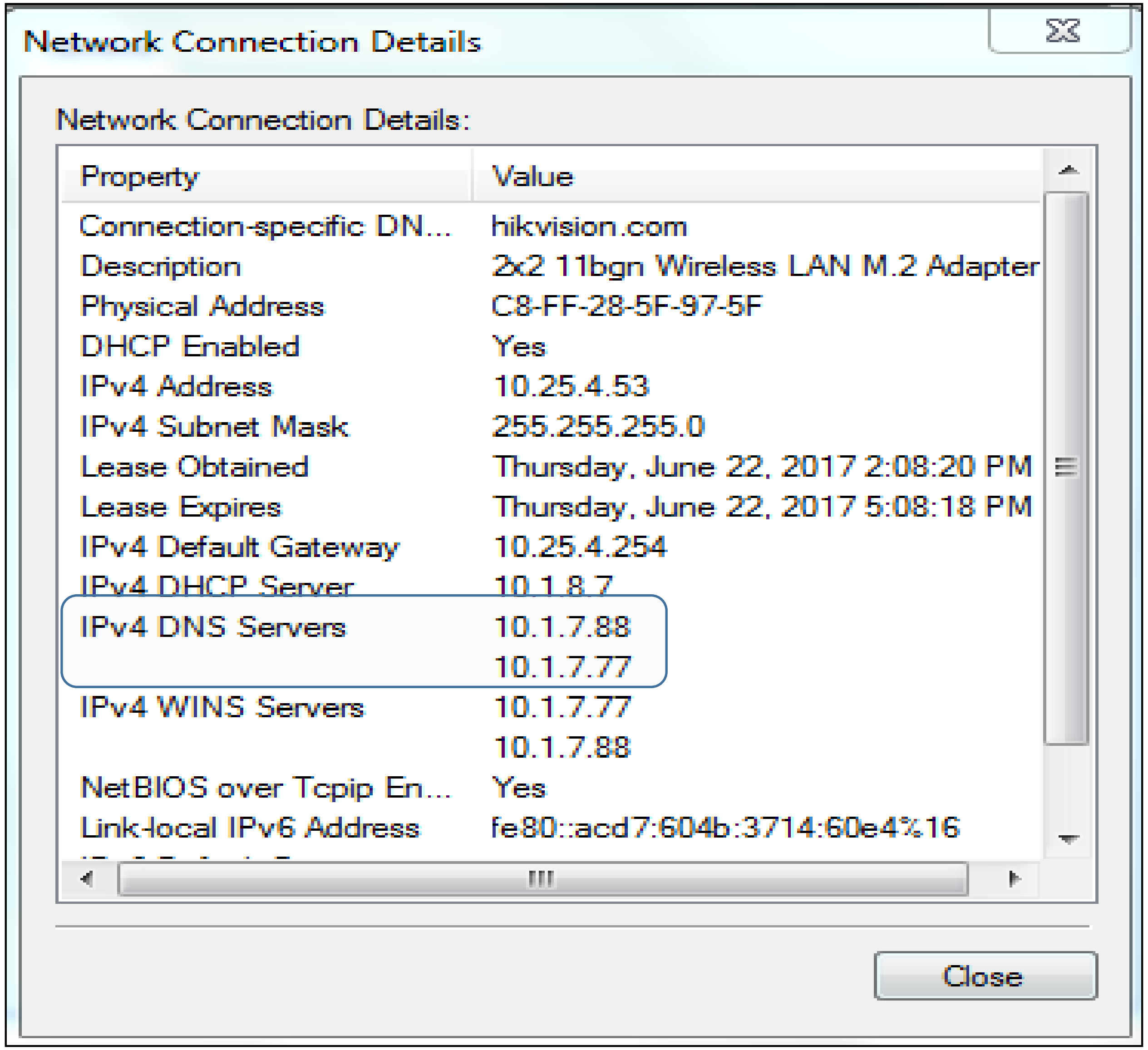
Domain Name & Domain Name System

A domain name is an identification string that defines a realm of administrative autonomy within the Internet (such as hikvision.com). Domain names are used in various networking contexts and for addressing purposes. In general, a domain name represents an IP address on Internet.

When you access to www.hikvision.com, the domain will be transformed into an IP address by the DNS server first, then your computer will access to the website via the IP address.


PC
DNS Server
Hikvision website
Send name resolution request
Go back to the IP of the domain name
Access to the Internet by IP address

DNS Configuration



Network Connection Details:

Property	Value
Connection-specific DN...	hikvision.com
Description	2x2 11bgn Wireless LAN M.2 Adapter
Physical Address	C8-FF-28-5F-97-5F
DHCP Enabled	Yes
IPv4 Address	10.25.4.53
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Thursday, June 22, 2017 2:08:20 PM
Lease Expires	Thursday, June 22, 2017 5:08:18 PM
IPv4 Default Gateway	10.25.4.254
IPv4 DHCP Server	10.1.8.7
IPv4 DNS Servers	10.1.7.88 10.1.7.77
IPv4 WINS Servers	10.1.7.77 10.1.7.88
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::acd7:604b:3714:60e4%16

DNS can be obtained by DHCP from the router automatically or it can be set manually as static IP address configuration

Commonly used DNS server 8.8.8.8 (overseas)

Obtain from ISP(Internet Service Provider)

Switch

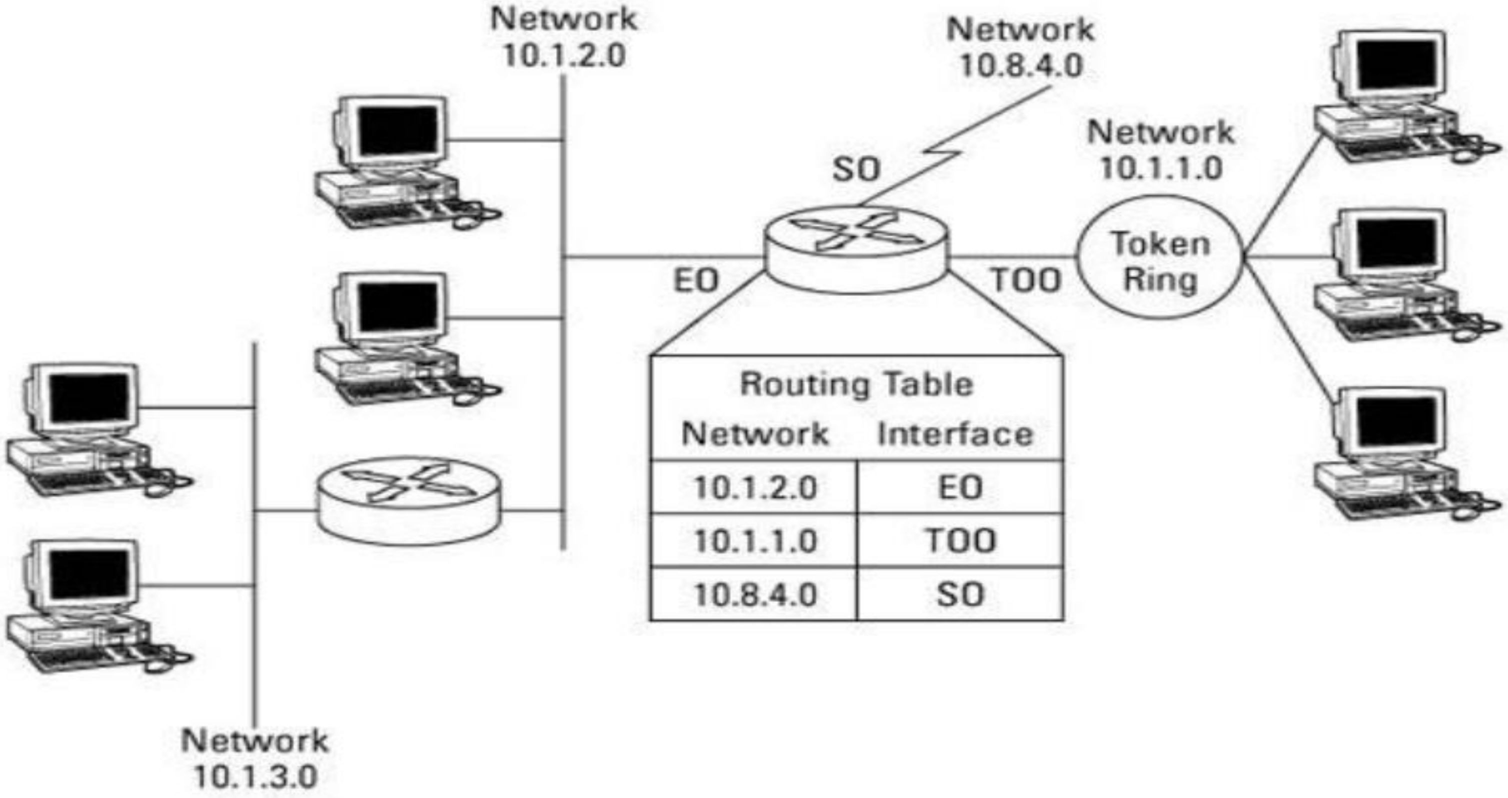
- Main Function: Extend Network, Repeater
- Large network: core switch and edge switch
- Small network: one switch
- Basic switch: supply connection
- Management switch: supply security/address/power management and QoS

Switch Model Selection

- Backplane bandwidth- (Gbps)
  - The Max throughput data between switch interface processor and data bus.
  - Bandwidth of Backplane is the data amount that switch can handle. It should be twice as the quickest speed of all the ports of switch. This value can be used to judge the forwarding performance.
- Packet forwarding rate(Mpps)
  - How many mega packets can be forwarded by switch in one second.
  - It indicates the exchange capacity of switch.

Router

- Main Function: Data output gateway to connect to the Internet



Routing Table

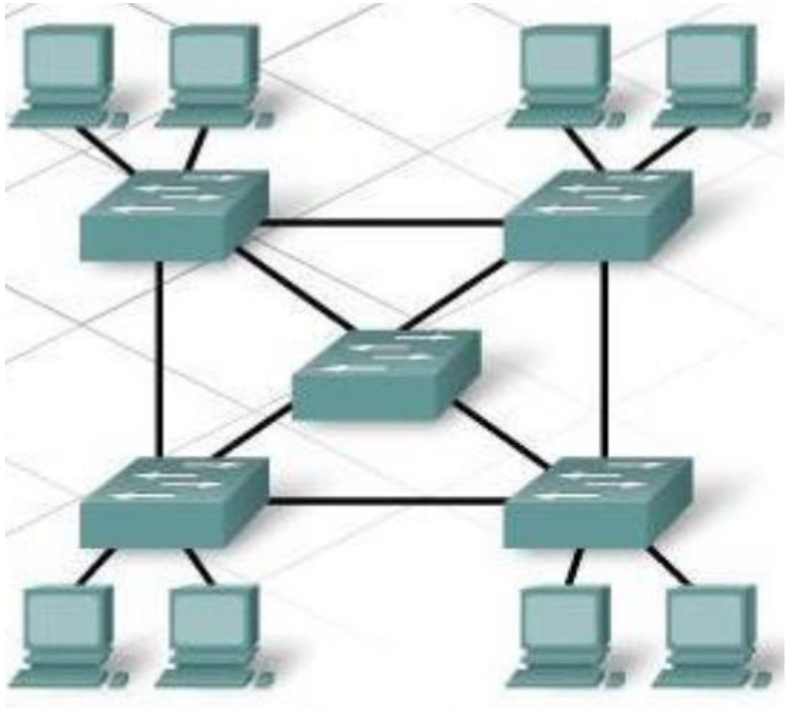
Network	Interface
10.1.2.0	E0
10.1.1.0	T00
10.8.4.0	S0

Contents

- Network Basics
- Network Device
- **Network Planning**
- Bandwidth Planning
- Network Security

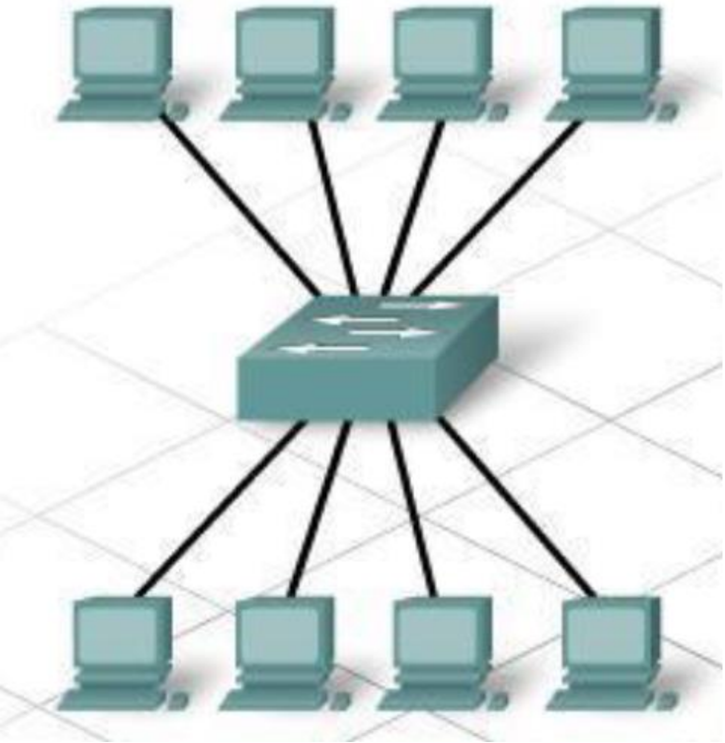
Network Structure-Full Mesh

- Advantage
  - Highest redundant level
  - Reduce network load
- Disadvantage
  - Need more switches and cables .



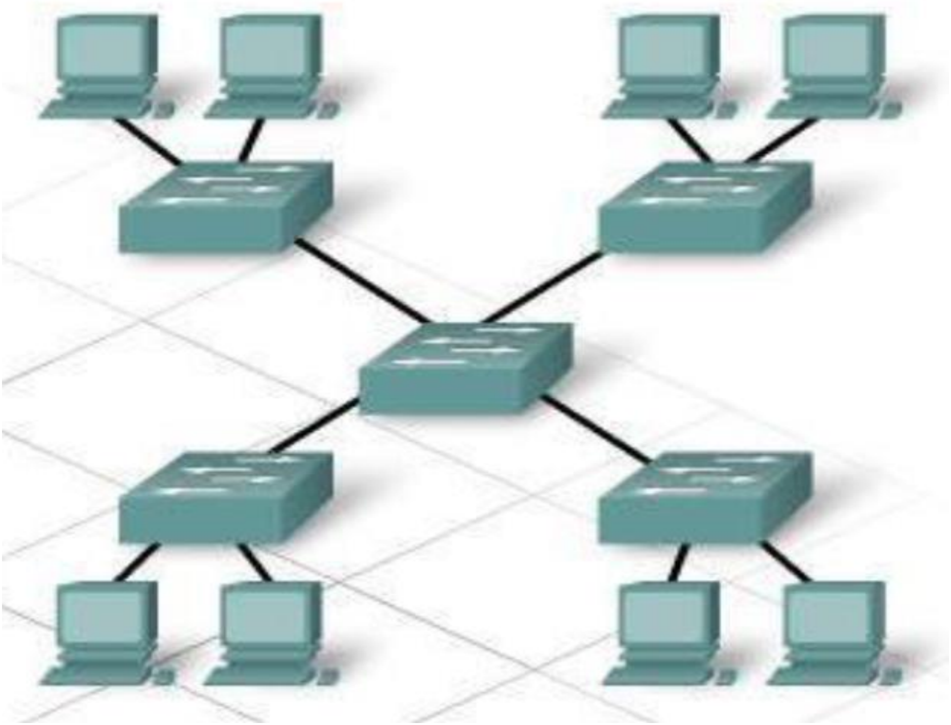
Network Structure-Star

- Advantage
  - Easy for management and maintenance
- Disadvantage
  - There may be network bottle neck.
  - No redundancy.



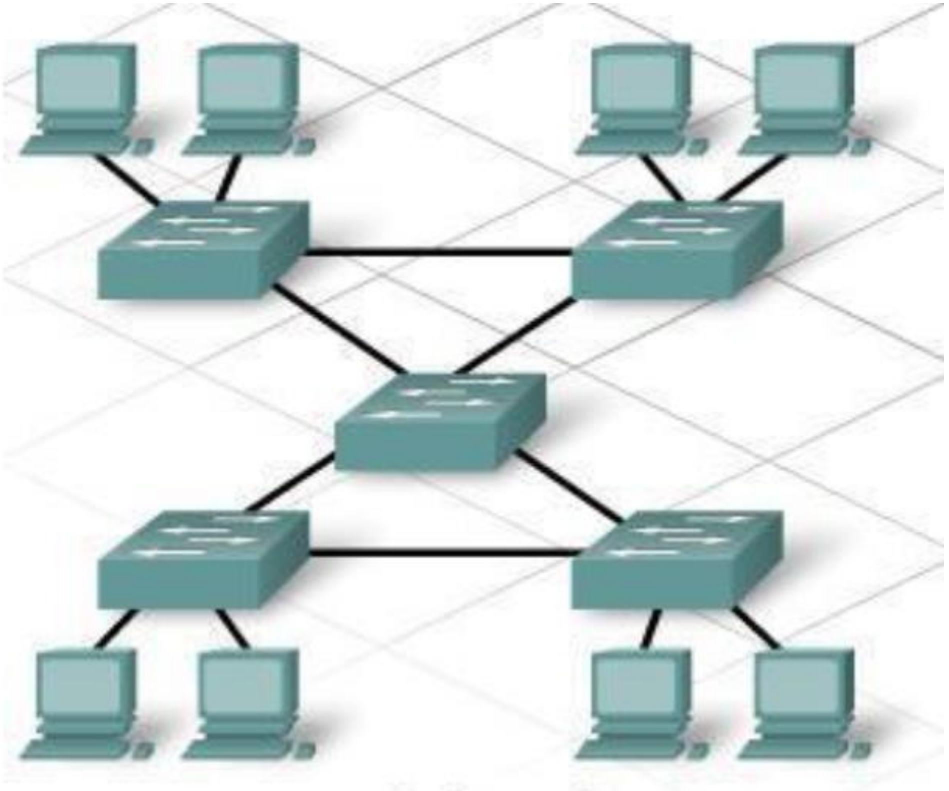
Network Structure-Extended Star

- Advantage
  - Supply some redundancy
  - Supply some load balancing
- Disadvantage
  - Need more switches and cables .



Network Structure-Partial Mesh

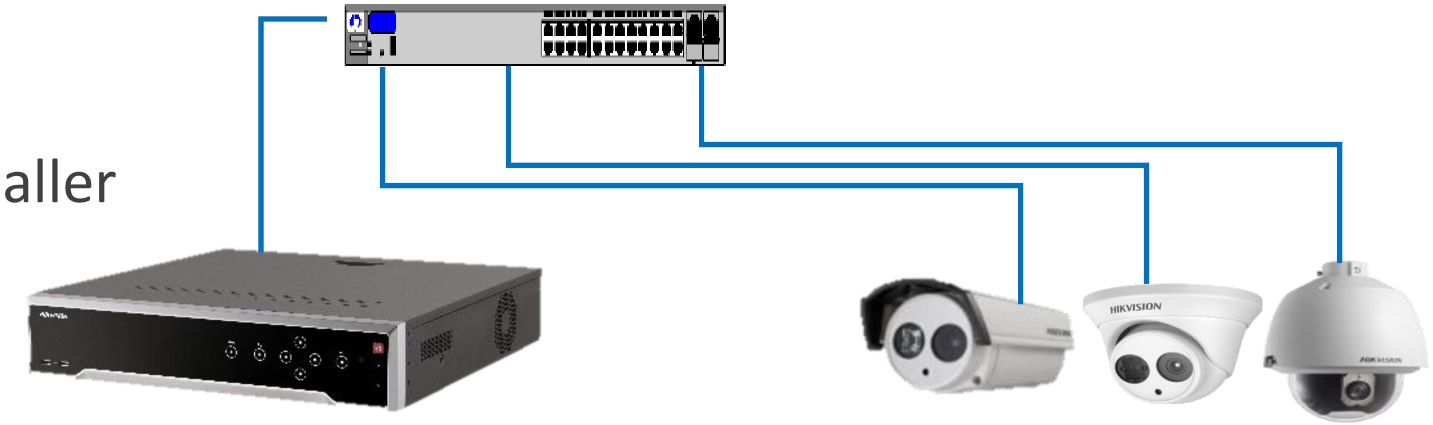
- Advantage
  - There is redundant linkage between devices
  - Easy to be extended without affecting current users
- Disadvantage
  - Need more switches and cables .



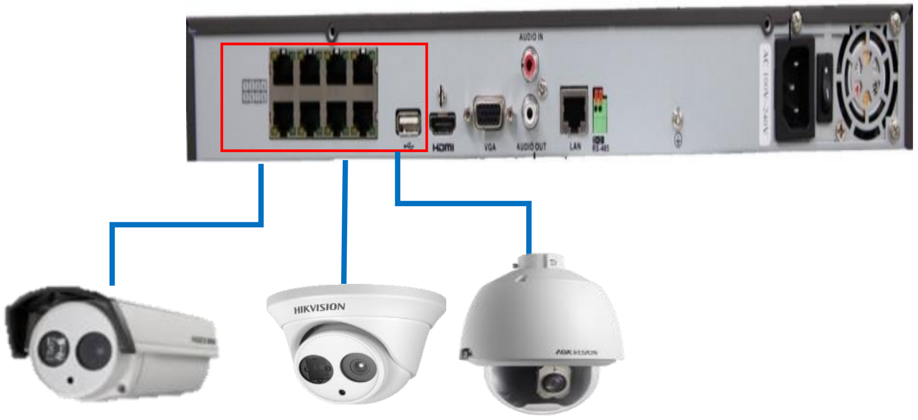
Network Design-Small System

- Single Switch
  - POE could be used.
  - Transmission distance smaller than 100M
  - Easy to install
  - No redundancy

Switch



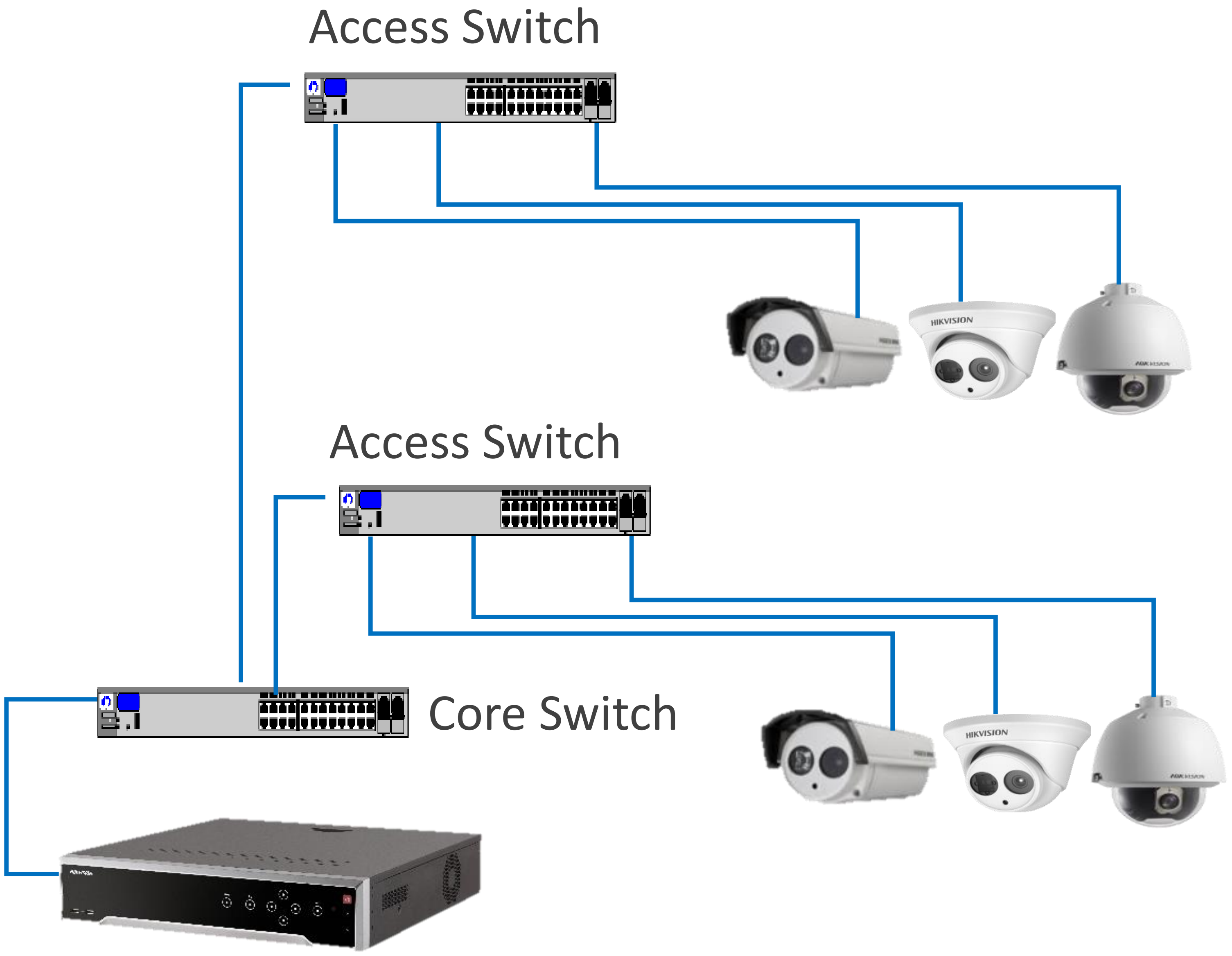
NVR without POE



NVR with POE

Network Design-Flexible System Scale

- Two layer structure
  - POE could be used.
  - System upgraded
  - Easy to install
  - redundancy is available



Contents

- Network Basics
- Network Device
- Network Planning
- **Bandwidth Planning**
- Network Security

Stream URL Calculation

- Common video parameters of IPC

1. **Resolution ratio**
   Common resolution ratio: 3840*2160(4K/8MP), 1920*1080(1080P/2MP), 1280*720(720P), 704*576(4CIF/D1), 352*288(CIF)

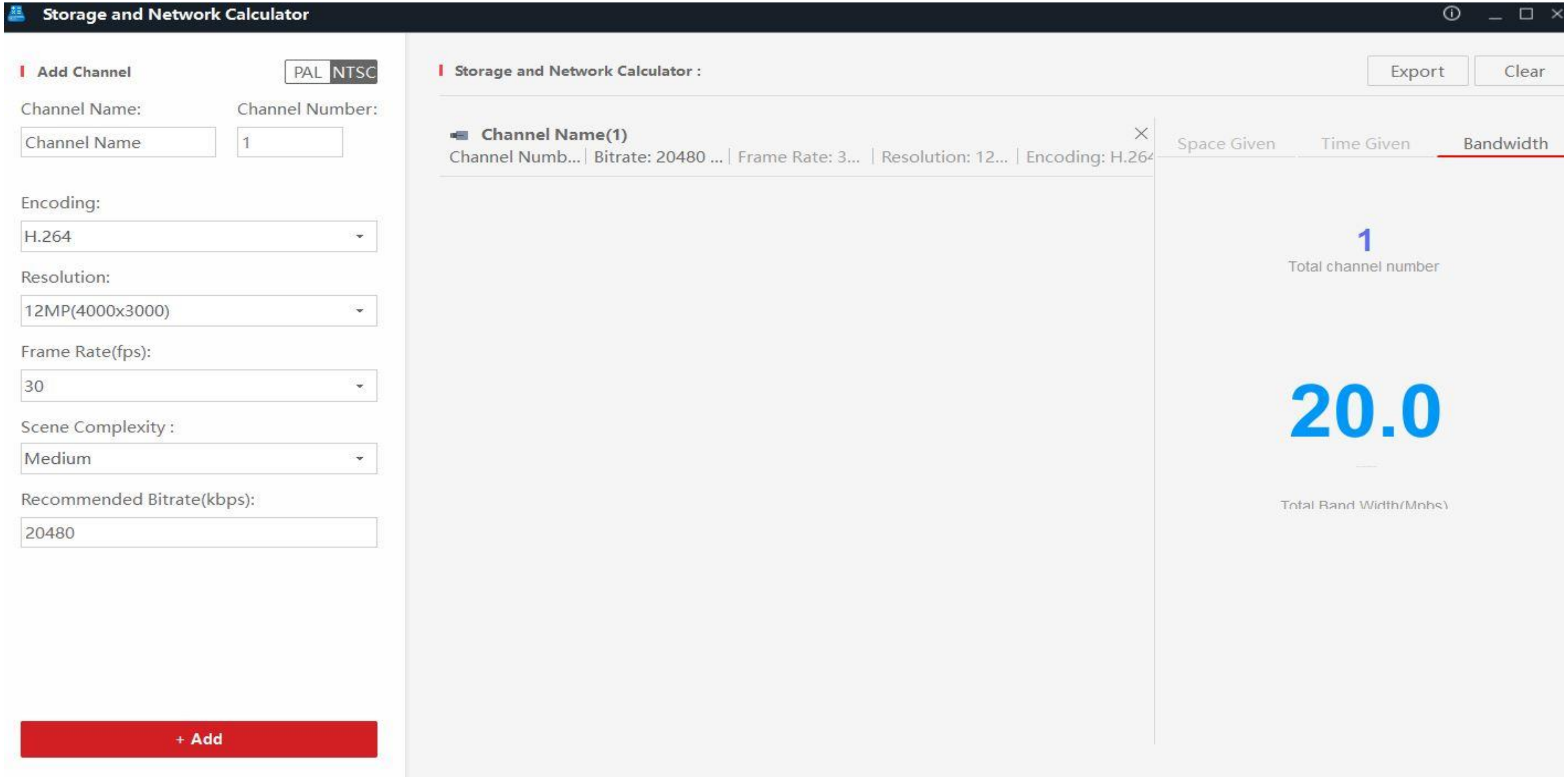
2. Frame rate (fps): the frequency at which consecutive images called frames appear on a display. The higher the frame rate is, the smoother the image is; when the rate is below 15, human eyes can feel that the image is not constant. Bit stream will be decreased by lower frame rate, but the video quality will be influenced if the frame rate is too low.

3. Encoding mode：MPEG4< H.264< H.264+ < H.265< H.265+ (encoding efficiency)

Video Encoding	Resolution Frame Rate	30 fps	25 fps	20 fps	15 fps	12.5 fps	10 fps	1 fps
H.264 Recommended Bit Rate	**3840×2160**	16384	16384	12288	8192	8192	6144	6144
	1080P(1920×1080)	4096	4096	3072	2048	2048	1536	1536
	720P(1280×720)	2048	2048	1536	1024	1024	768	768
	4CIF(704×576)	1024	1024	768	512	512	384	384
	352×288	320	320	192	192	192	128	128
H.265 Recommended Bit Rate	**3840×2160**	8192	8192	6144	4096	4096	3072	3072
	1080P(1920×1080)	2048	2048	1536	1024	1024	768	768
	720P(1280×720)	1024	1024	768	512	512	384	384
	4CIF(704×576)	704	704	512	384	384	256	256
	352×288	320	320	192	192	192	128	128

How To Calculate Bandwidth and Storage

- Hikvison design tool



Storage and Network Calculator

Add Channel

PAL NTSC

Channel Name: Channel Name

Channel Number: 1

Encoding: H.264

Resolution: 12MP(4000x3000)

Frame Rate(fps): 30

Scene Complexity : Medium

Recommended Bitrate(kbps): 20480

+ Add

Storage and Network Calculator :

Export Clear

Channel Name(1)

Channel Numb... | Bitrate: 20480 ... | Frame Rate: 3... | Resolution: 12... | Encoding: H.264

Space Given Time Given Bandwidth

1

Total channel number

20.0

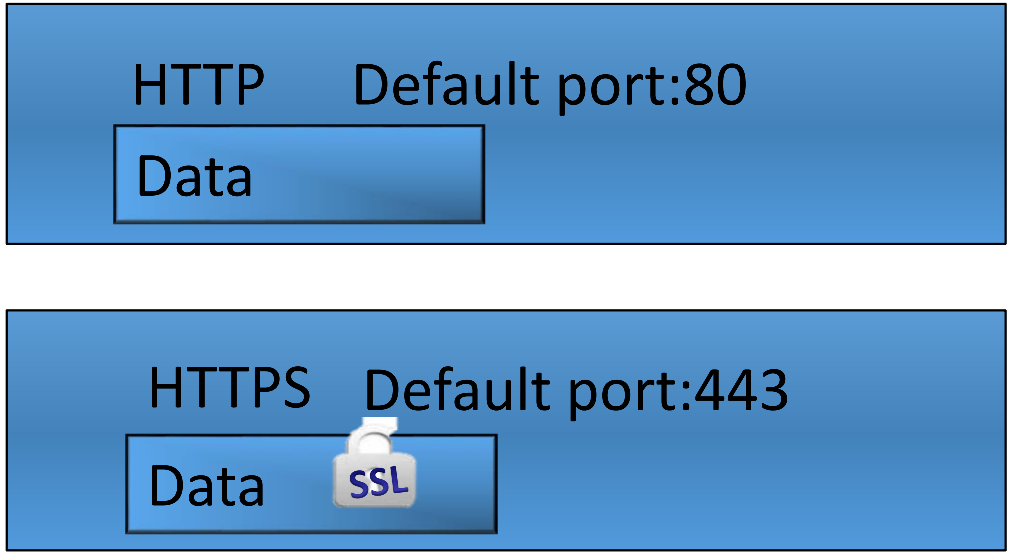
Total Band Width(Mpbs)

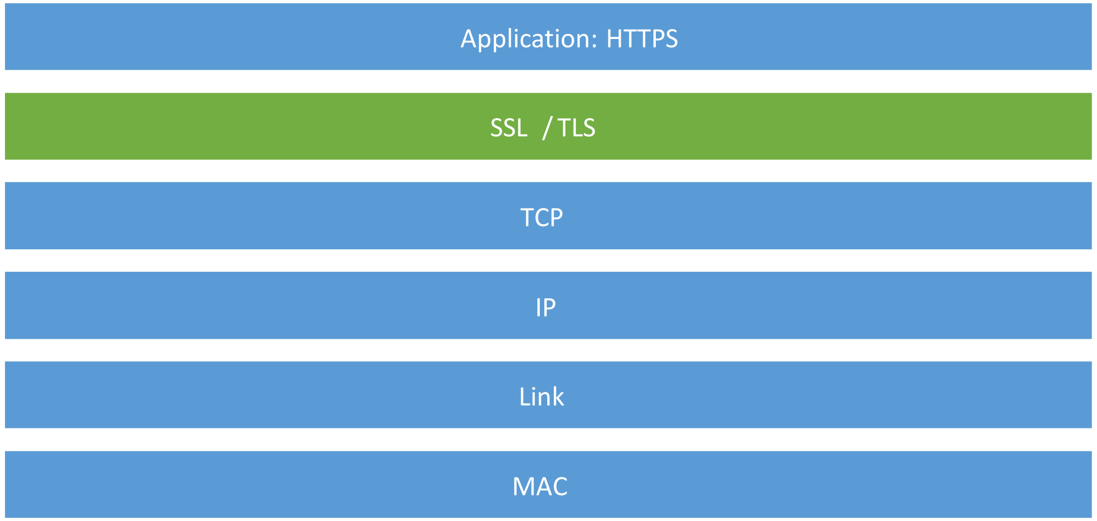
Contents

- Network Basics
- Network Device
- Network Planning
- Bandwidth Planning
- **Network Security**

HTTPS

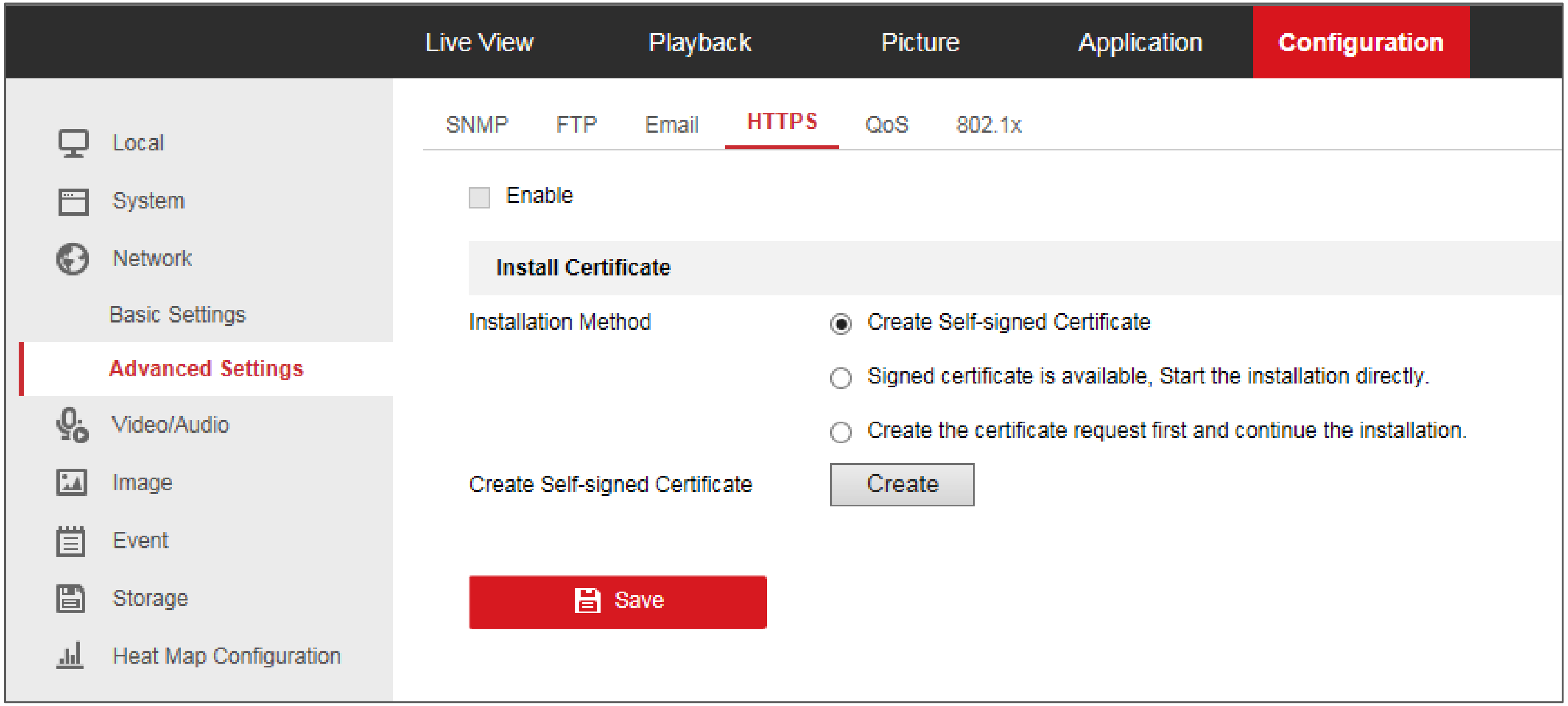
- Hyper Text Transfer Protocol over Secure Socket Layer
  - communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. It adds the security capabilities of SSL/TLS to standard HTTP communications.
  - The main motivation for HTTPS is to prevent wiretapping and man-in-the-middle attacks.
  - Default port number: 443
  - The HTTPS port can be changed if desired (port numbers range from 1-65535)





HTTPS – Create Self-signed Certificate

- 1. In the web UI, enter HTTPS configuration menu by going to *Configuration -> Network -> Advanced Configuration -> HTTPS*.
- 2. Click on Create button “Create self-signed certificate”



□ Enable

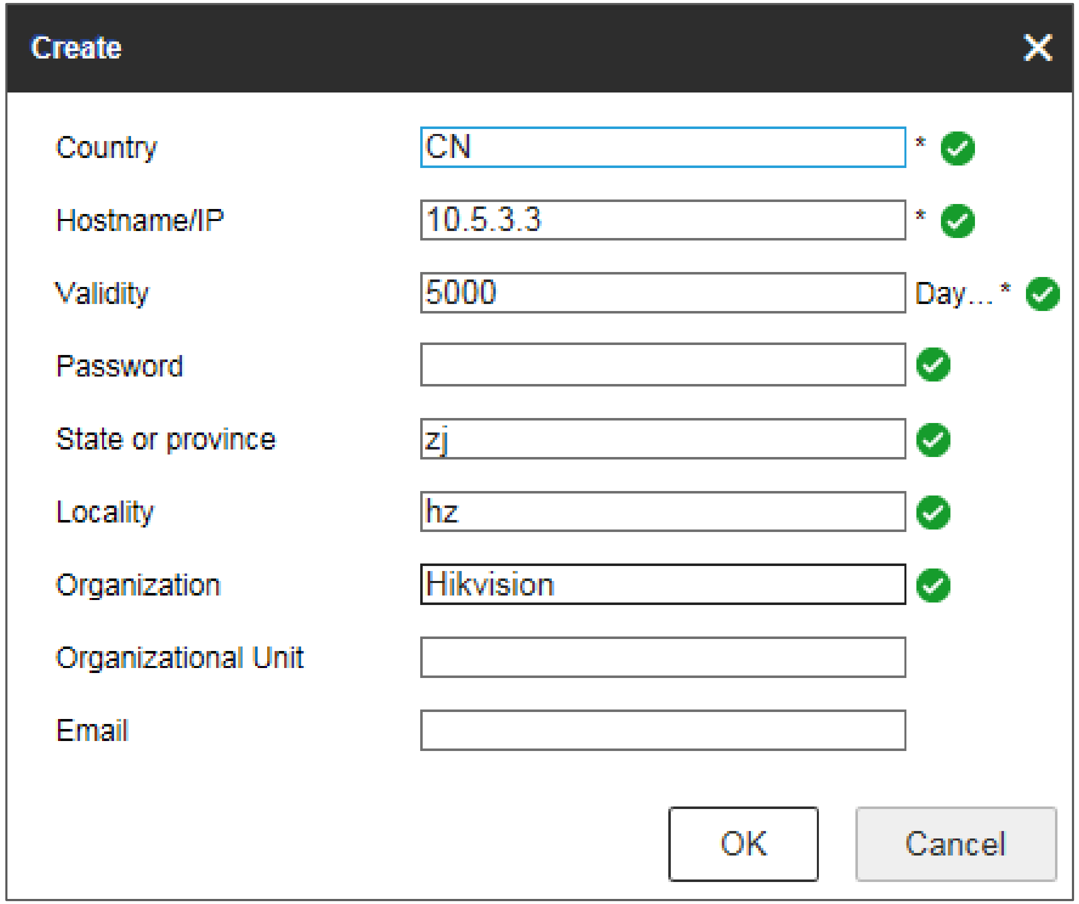
Install Certificate

Installation Method
● Create Self-signed Certificate
○ Signed certificate is available, Start the installation directly.
○ Create the certificate request first and continue the installation.

Create Self-signed Certificate [Create]

HTTPS – Create Self-signed Certificate

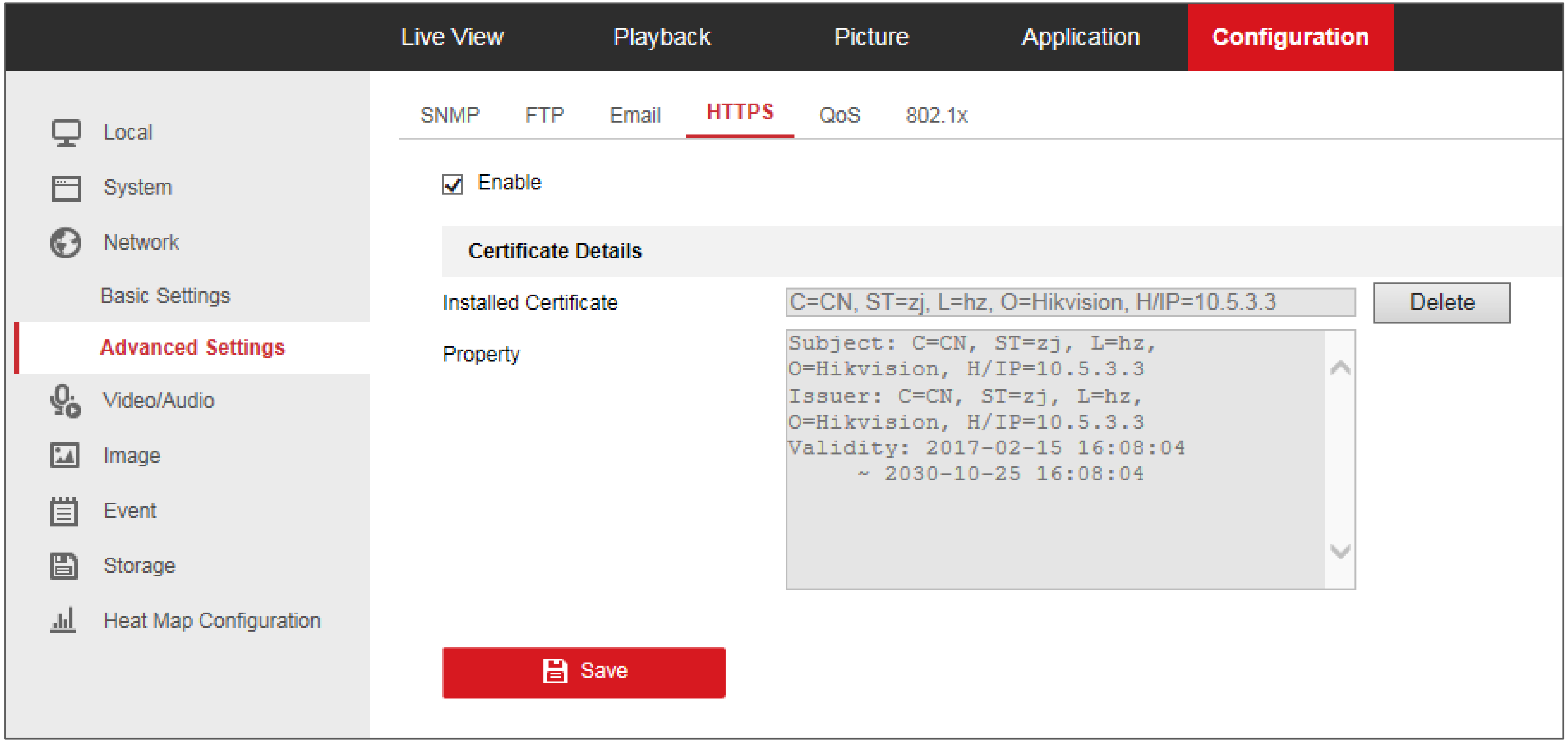
- 3. Type in parameters such as country, hostname/IP, and validity as shown below, then Click on OK (there is no need to provide any other information, just the first three fields, as specified).



Country	CN	* ✓
Hostname/IP	10.5.3.3	* ✓
Validity	5000	Day... * ✓
Password		✓
State or province	zj	✓
Locality	hz	✓
Organization	Hikvision	✓
Organizational Unit		
Email		

HTTPS – Create Self-signed Certificate

- 4. Check Enable HTTPS checkbox, and then click on Save button



☑ Enable

Certificate Details

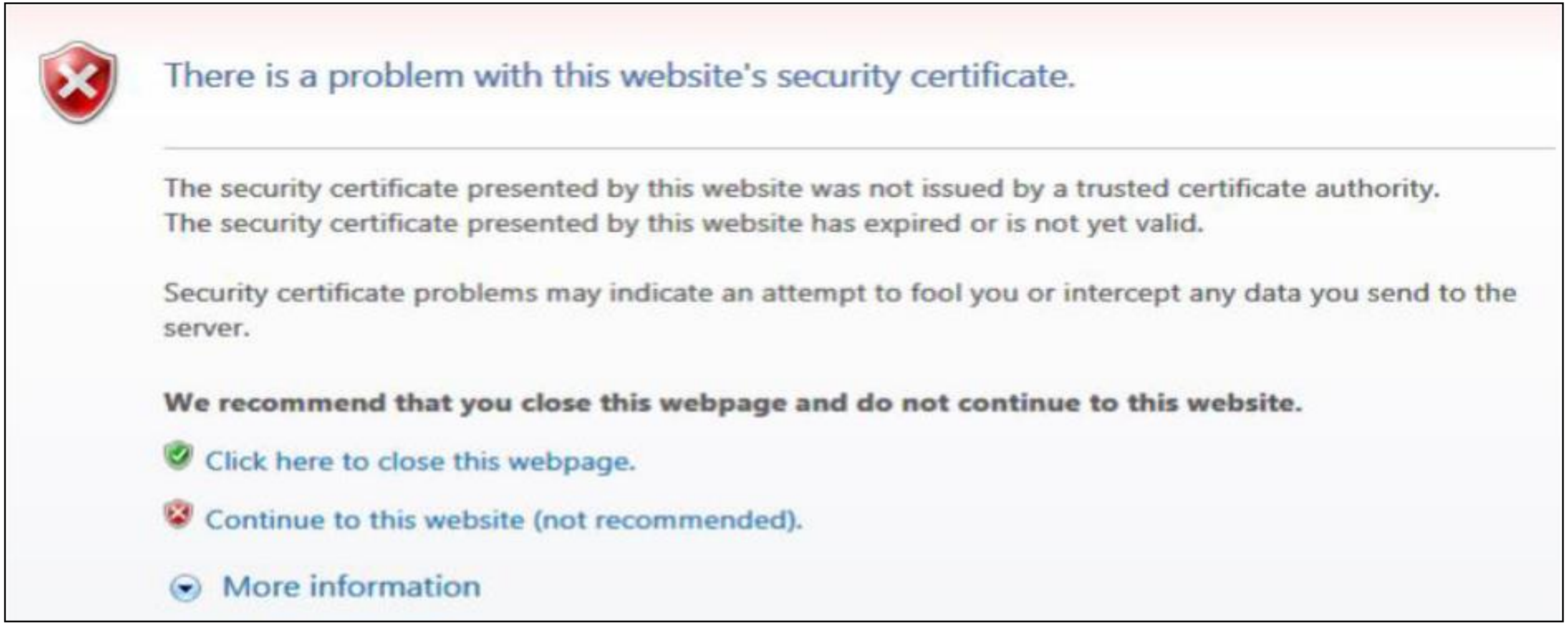
Installed Certificate: C=CN, ST=zj, L=hz, O=Hikvision, H/IP=10.5.3.3

Property:

```
Subject: C=CN, ST=zj, L=hz,
O=Hikvision, H/IP=10.5.3.3
Issuer: C=CN, ST=zj, L=hz,
O=Hikvision, H/IP=10.5.3.3
Validity: 2017-02-15 16:08:04
     ~ 2030-10-25 16:08:04
```

HTTPS – Create Self-signed Certificate

- When using HTTPS to access the device, type ***https://IP address:port number*** into the web browser address bar (e.g. *https://192.0.0.64:443*).
- If self-signed certificate is used, web browser may pop up warning notification like shown below.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website has expired or is not yet valid.

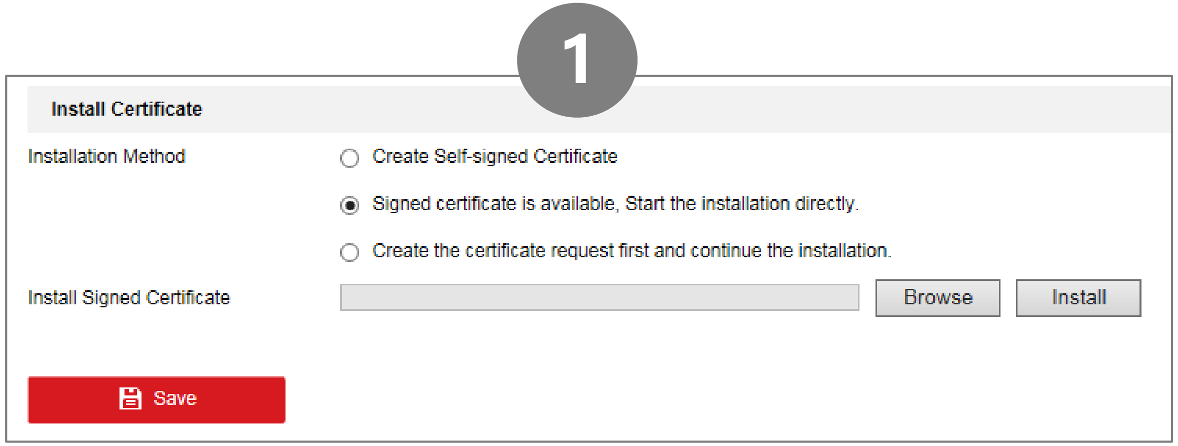
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
Continue to this website (not recommended).
More information

HTTPS – Create Self-signed Certificate

- Users can install the certificate signed by CA (Certificate Authority) to enhance the safety level. (reputable CA organizations always need charging)
  - 1 **gned certificate is available, Start the installation directly**: For the customer who already has the ertificate.
  - 2 **reate the certificate request first and continue the installation**: For the customer who wants to eate certificate request by himself. After creation, one can download the file and send it to CA to sign. After getting the certificate, simply install the certificate to enable HTTPS.

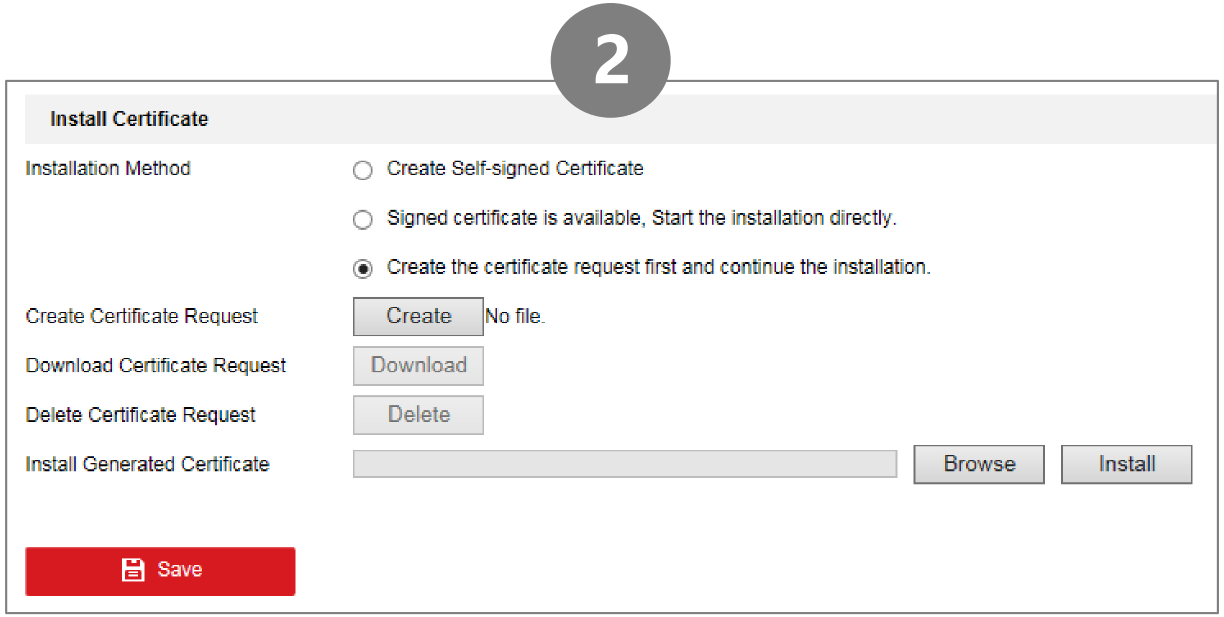


Install Certificate

Installation Method
○ Create Self-signed Certificate
● Signed certificate is available, Start the installation directly.
○ Create the certificate request first and continue the installation.

Install Signed Certificate [ ] Browse Install

Save



Install Certificate

Installation Method
○ Create Self-signed Certificate
○ Signed certificate is available, Start the installation directly.
● Create the certificate request first and continue the installation.

Create Certificate Request: Create No file.

Download Certificate Request: Download

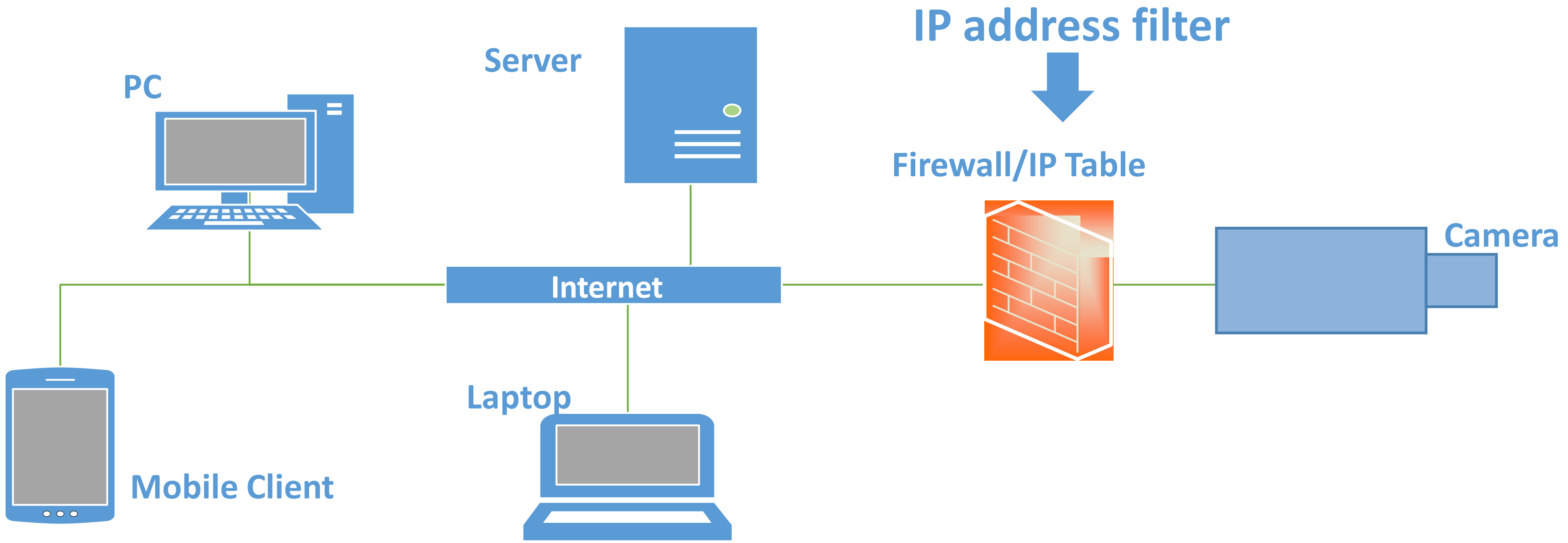
Delete Certificate Request: Delete

Install Generated Certificate [ ] Browse Install

Save

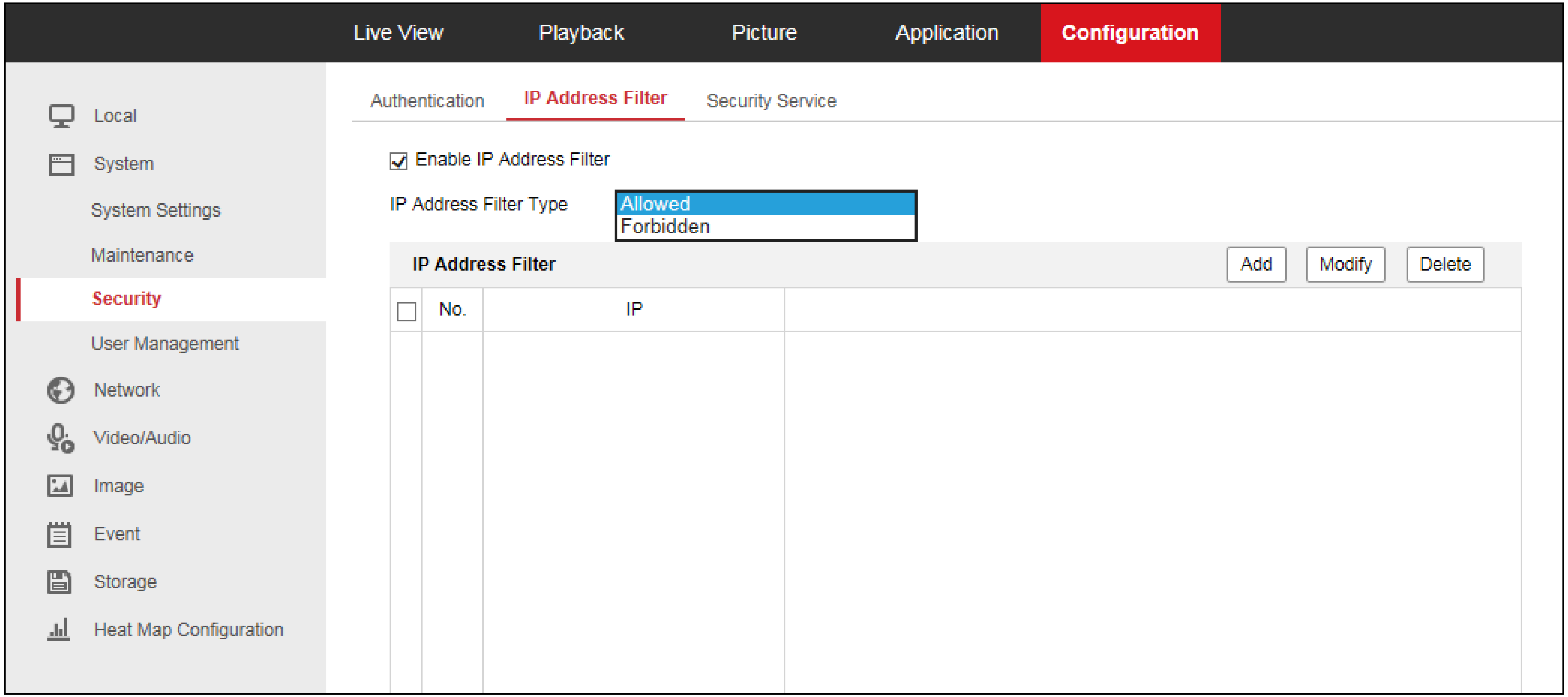
IP Address Filter

- Hikvision network products provide IP address filtering, which allows or forbids access rights to defined IP address(es).
- A typical configuration is to configure the device to allow only the IP address of the server that is hosting the VMS to access.



IP Address Filter

- Configuration -> System->Security-> IP Address Filter



☑ Enable IP Address Filter

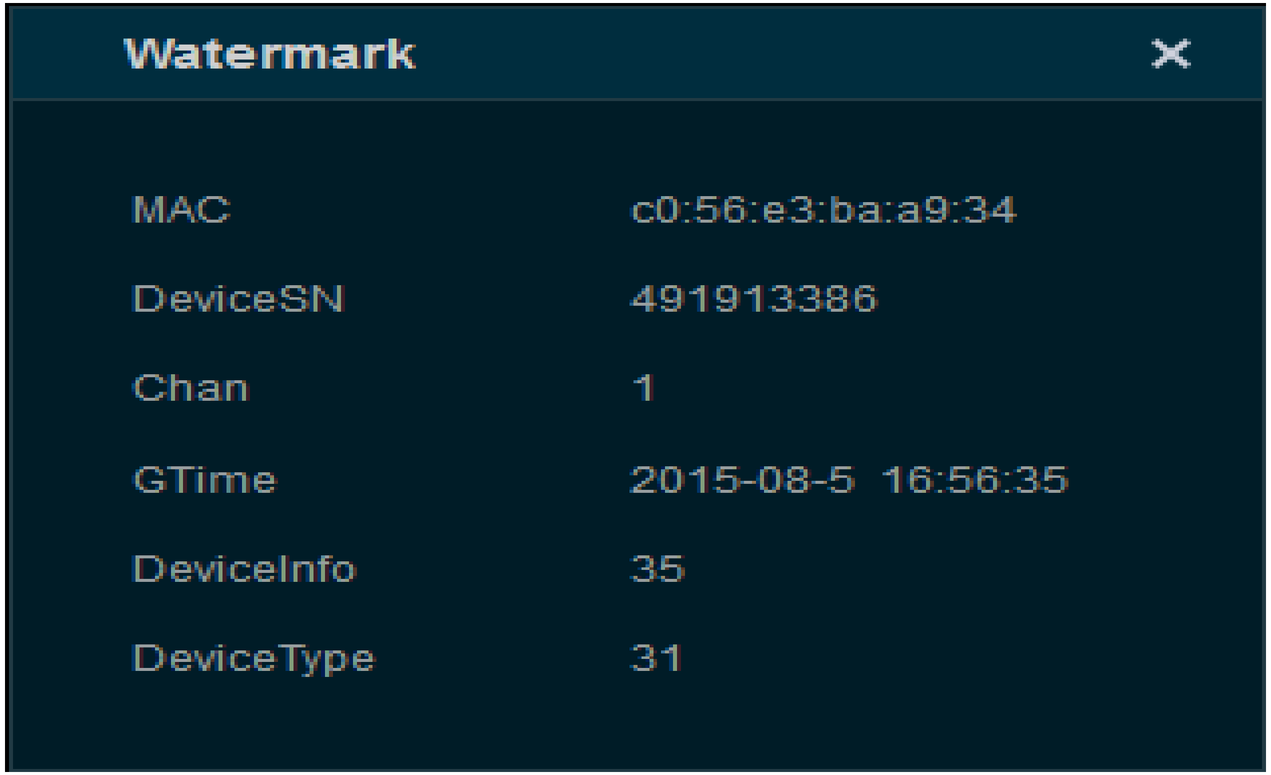
IP Address Filter Type: Allowed / Forbidden

IP Address Filter

□	No.	IP

Digital Watermark

- Digital watermark technology embeds the device information onto the recorded video.
- Digital watermarks may be used to verify the authenticity or integrity of the video or to show the identity of its owners.

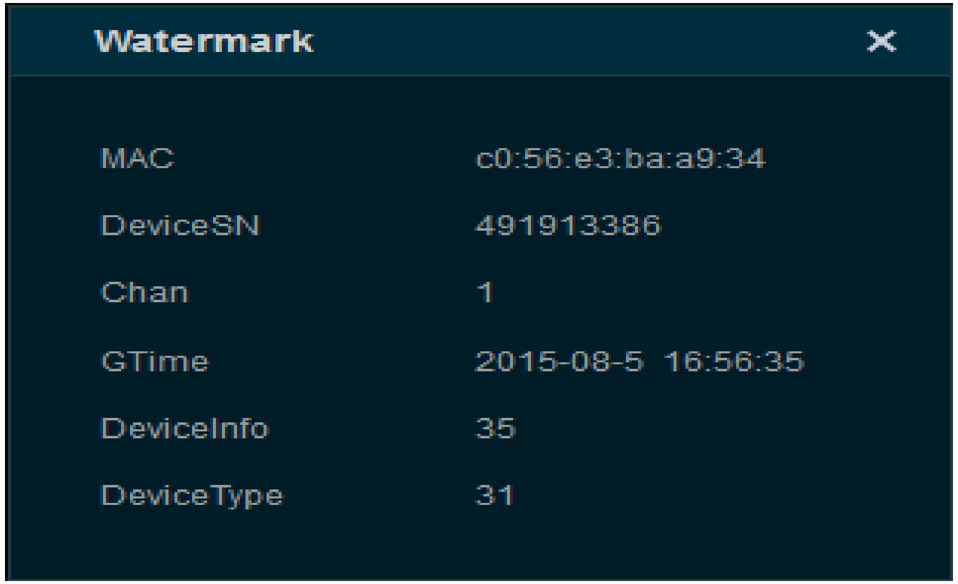


Watermark

MAC	c0:56:e3:ba:a9:34
DeviceSN	491913386
Chan	1
GTime	2015-08-5 16:56:35
DeviceInfo	35
DeviceType	31

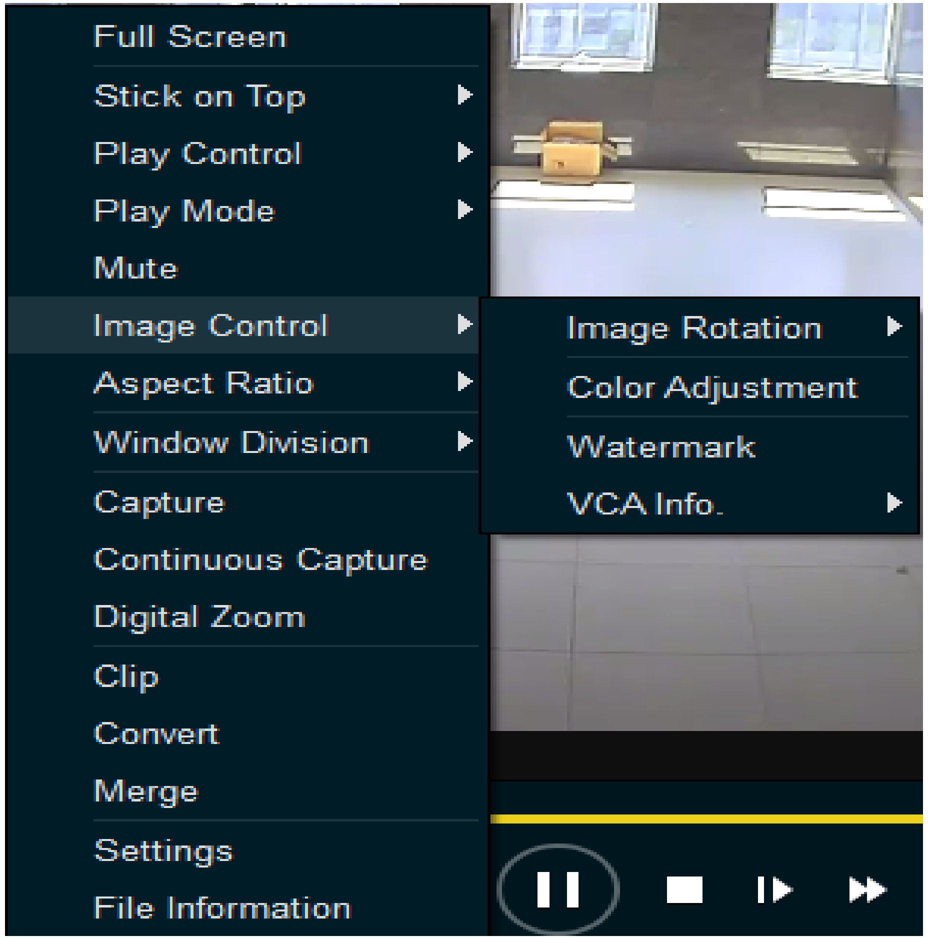
Watermark

- Open VSPlayer and play one video clip from Hikvision camera.
- Right click on the video: Image Control -> Watermark
- The watermark information will be displayed on the video.



Watermark ×

MAC	c0:56:e3:ba:a9:34
DeviceSN	491913386
Chan	1
GTime	2015-08-5 16:56:35
DeviceInfo	35
DeviceType	31



NOTE

- Only Hikvision VSPlayer can check and display the watermark of video stream.

Thank You