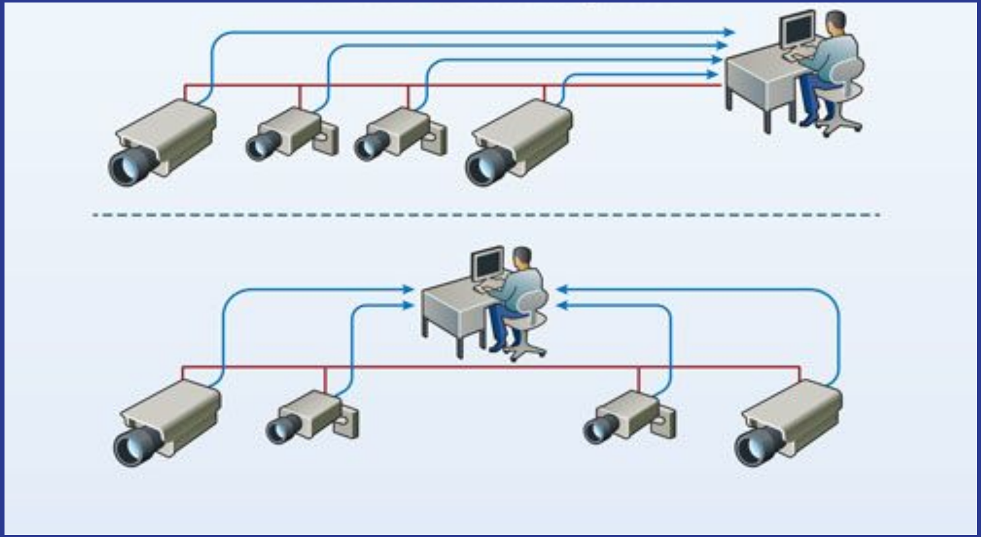
IP Video Surveillance



By
Ferdinand Joseph

Overview

The significant growth of cloud networking and Artificial Intelligence (AI) have gone far beyond simple video surveillance system.

The modern IP CCTV system design will require an in-depth network knowledge to design and implement a successful video surveillance system.

Contents:

1. What is IP Video Surveillance?

2. Introduction to Computer Networks

3. What is a Protocol?

4. What is the difference between an ONVIF and a private protocol?

5. Alarm integration

Chapter 1: What is IP Video Surveillance?

Objective:

The participants will understand what is an IP video surveillance system is and what are the factors to consider before choosing an IP video surveillance system.

Outcomes:

The participants will be able to describe the basic components of an IP video surveillance system.

The participants will be able to identify the different types of IP video surveillance systems available in the market.

Chapter 1: What is IP Video Surveillance?

Why IP video surveillance?

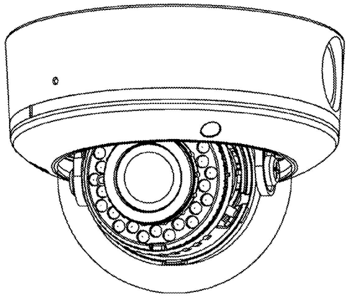
- Remote accessibility
- High image quality
- Event management and intelligent video
- Easy, future-proof integration
- Scalability and flexibility
- Cost-effectiveness

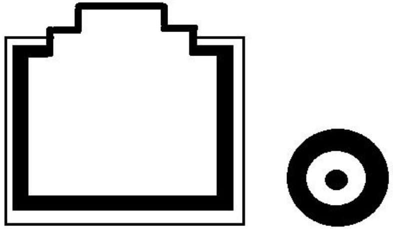
Chapter 1: What is IP Video Surveillance?

What is IP video surveillance?

An Internet Protocol camera, or network camera, is a type of digital video camera that receive and transmit video and other instructions in the form of digital data packets.

Chapter 1: What is IP Video Surveillance?

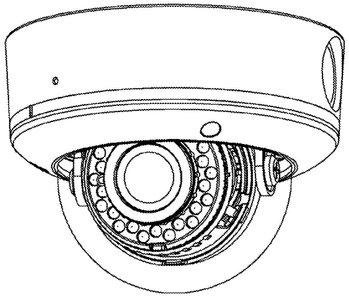


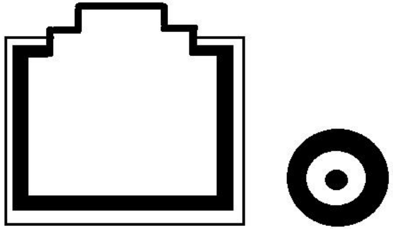


RJ45 Slot

BNC

Chapter 1: What is IP Video Surveillance?



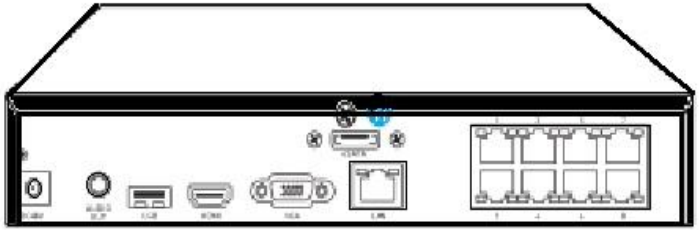


RJ45 Slot

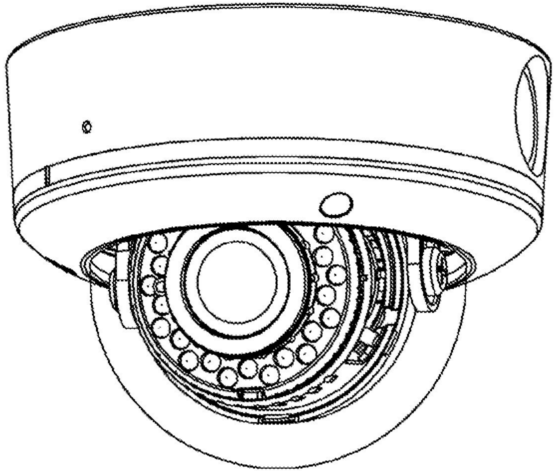
BNC

Chapter 1: What is IP Video Surveillance?

- H.265+ compression
- 8-ch synchronous playback at up to 1080p resolution

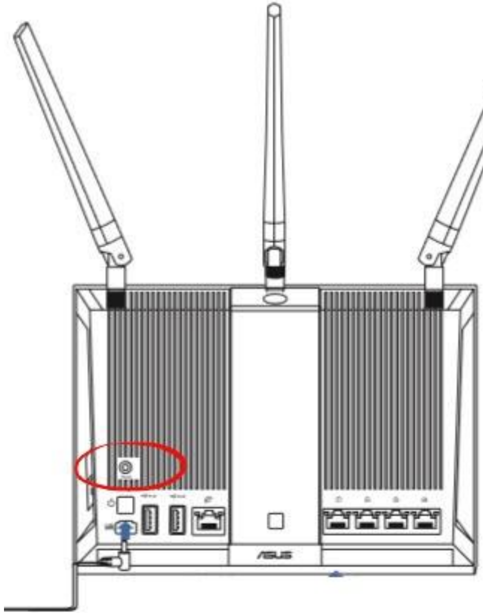


Chapter 1: What is IP Video Surveillance?



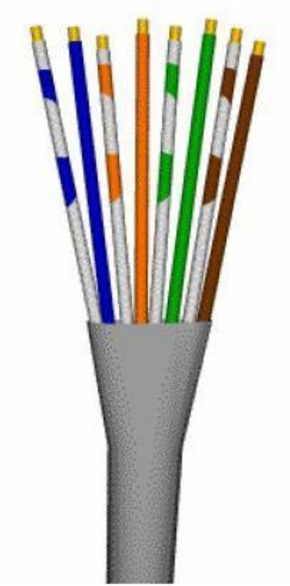
- 1/2.8” Progressive Scan CMOS
- 1080p @ 60fps frame rate High light environment
- Slow shutter
- 140dB WDR
- 3D DNR
- Audio/Alarm IO
- Support 128G on-board storage DC12V/PoE(802.3af)

Chapter 1: What is IP Video Surveillance?



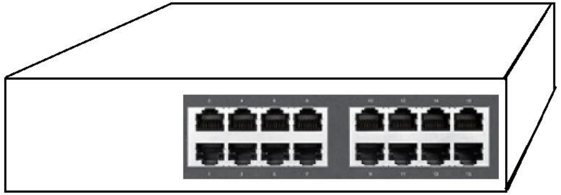
- Router

Chapter 1: What is IP Video Surveillance?



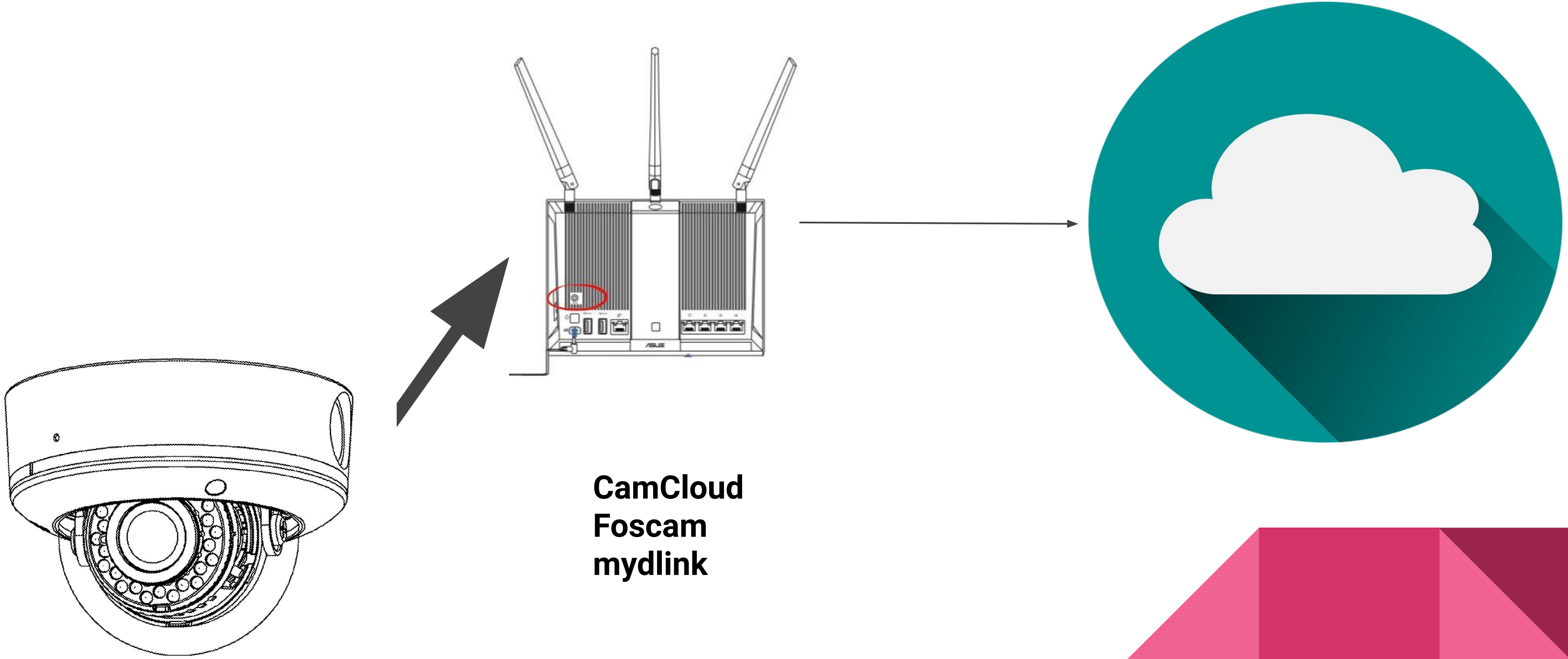
- Ethernet cable

Chapter 1: What is IP Video Surveillance?



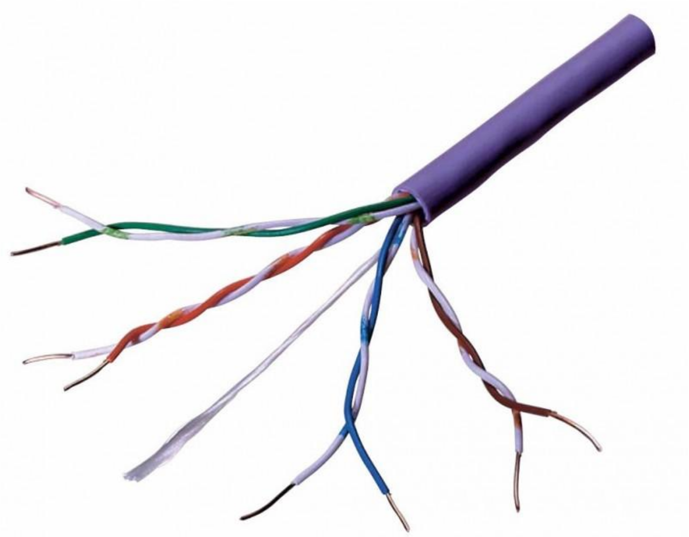
- Network switch

Chapter 1: What is IP Video Surveillance?



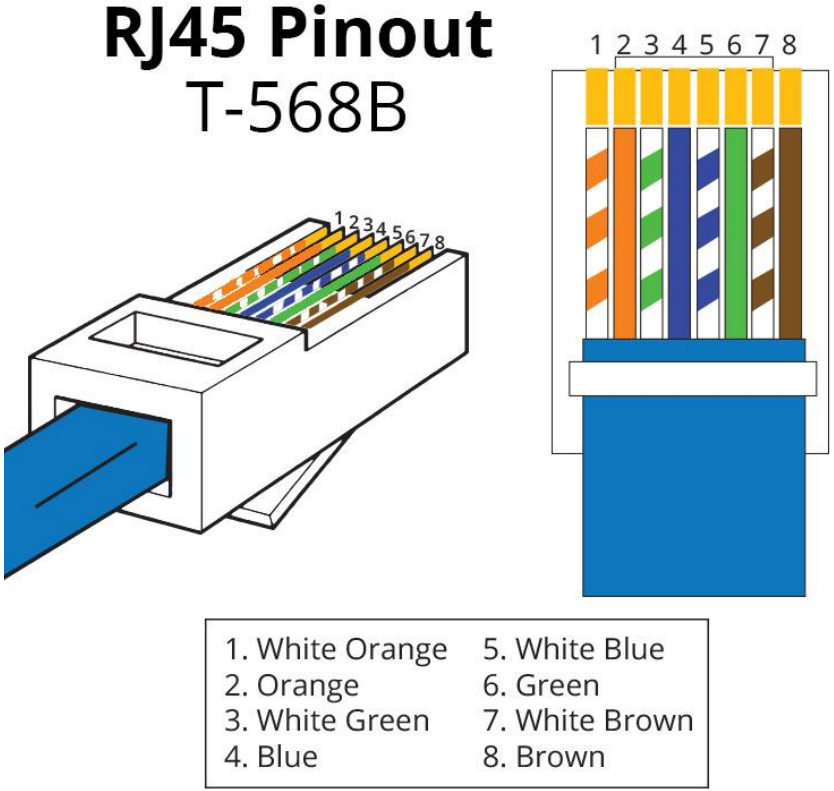
CamCloud
Foscam
mydlink

Chapter 1: What is IP Video Surveillance?



Ethernet cables

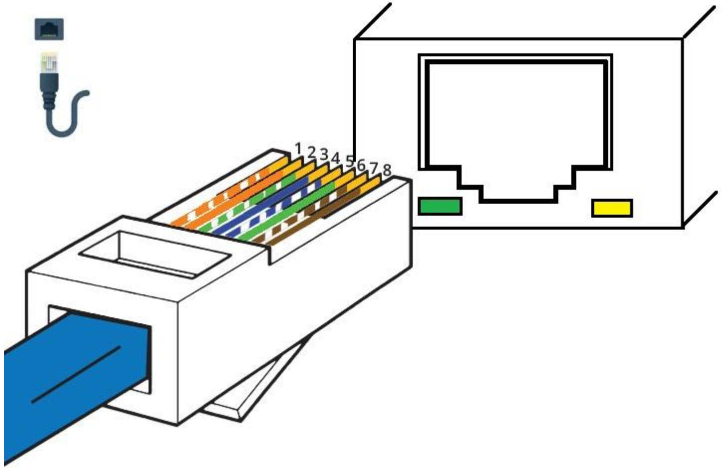
Chapter 1: What is IP Video Surveillance?



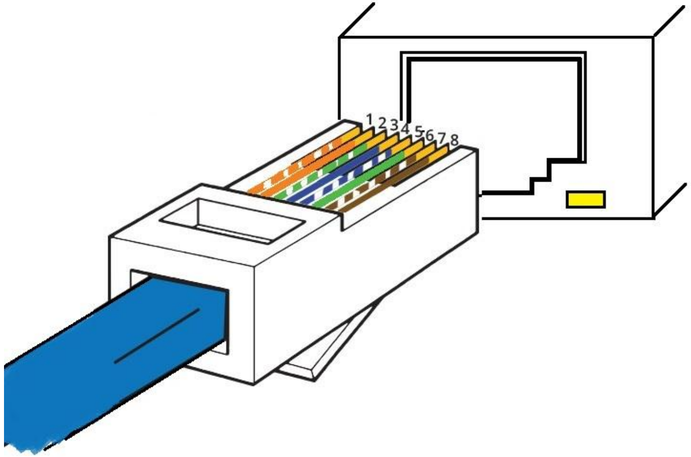
Chapter 1: What is IP Video Surveillance?

Fibre Optic cables

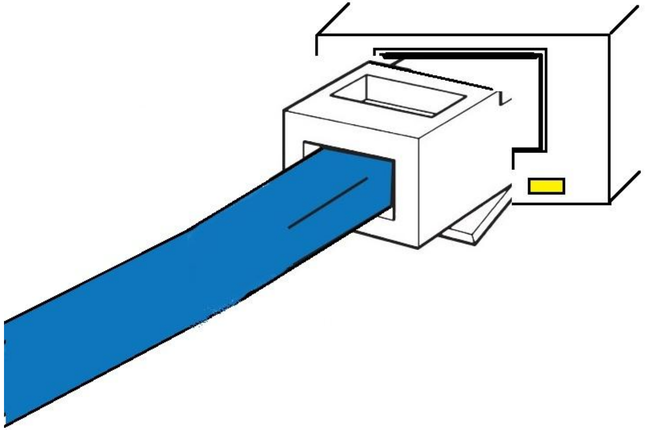
Chapter 1: What is IP Video Surveillance?



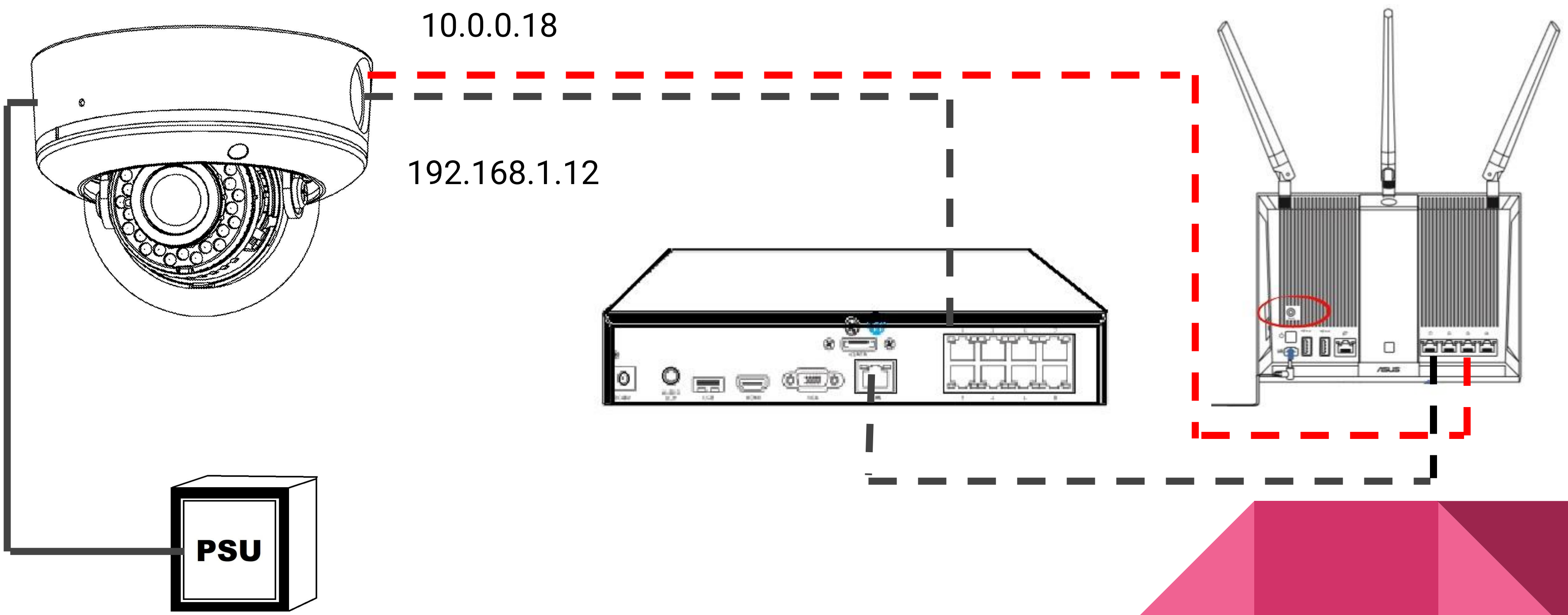
Chapter 1: What is IP Video Surveillance?



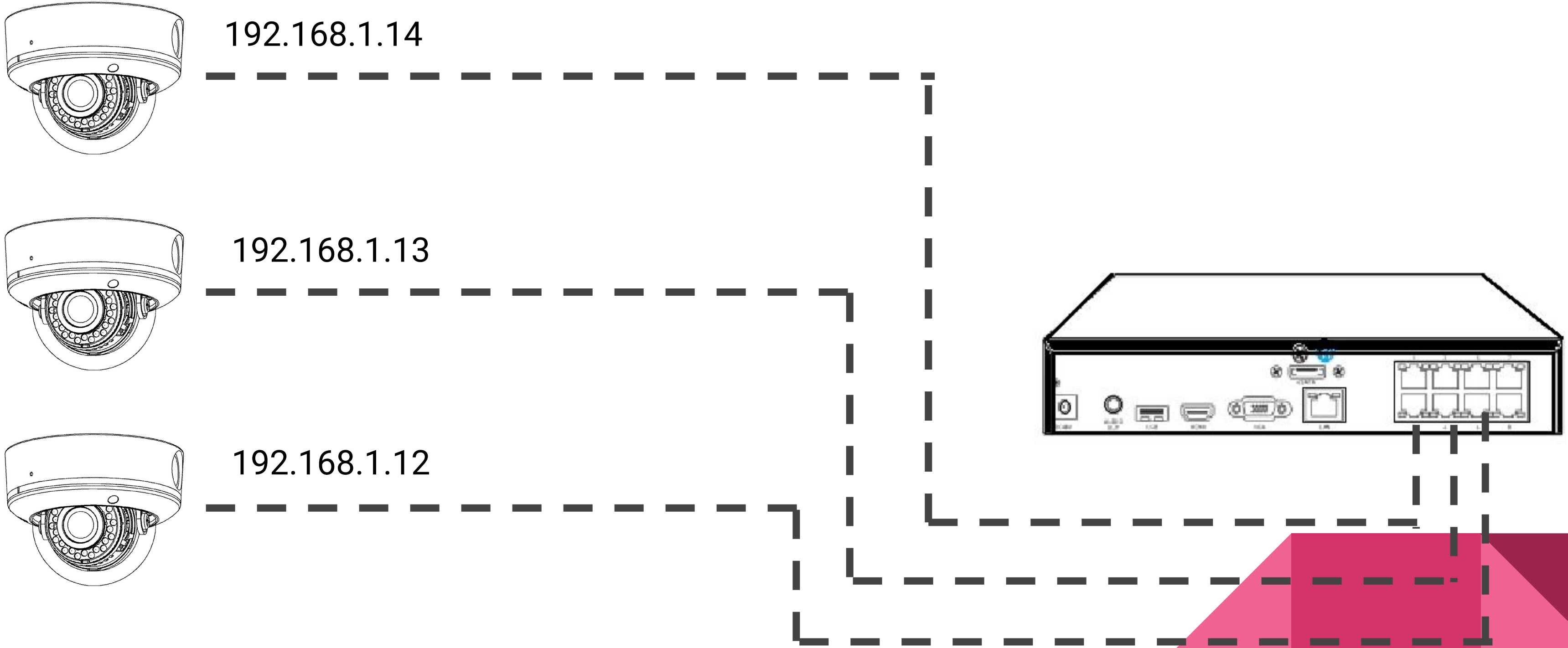
Chapter 1: What is IP Video Surveillance?



Chapter 1: What is IP Video Surveillance?



Chapter 1: What is IP Video Surveillance?

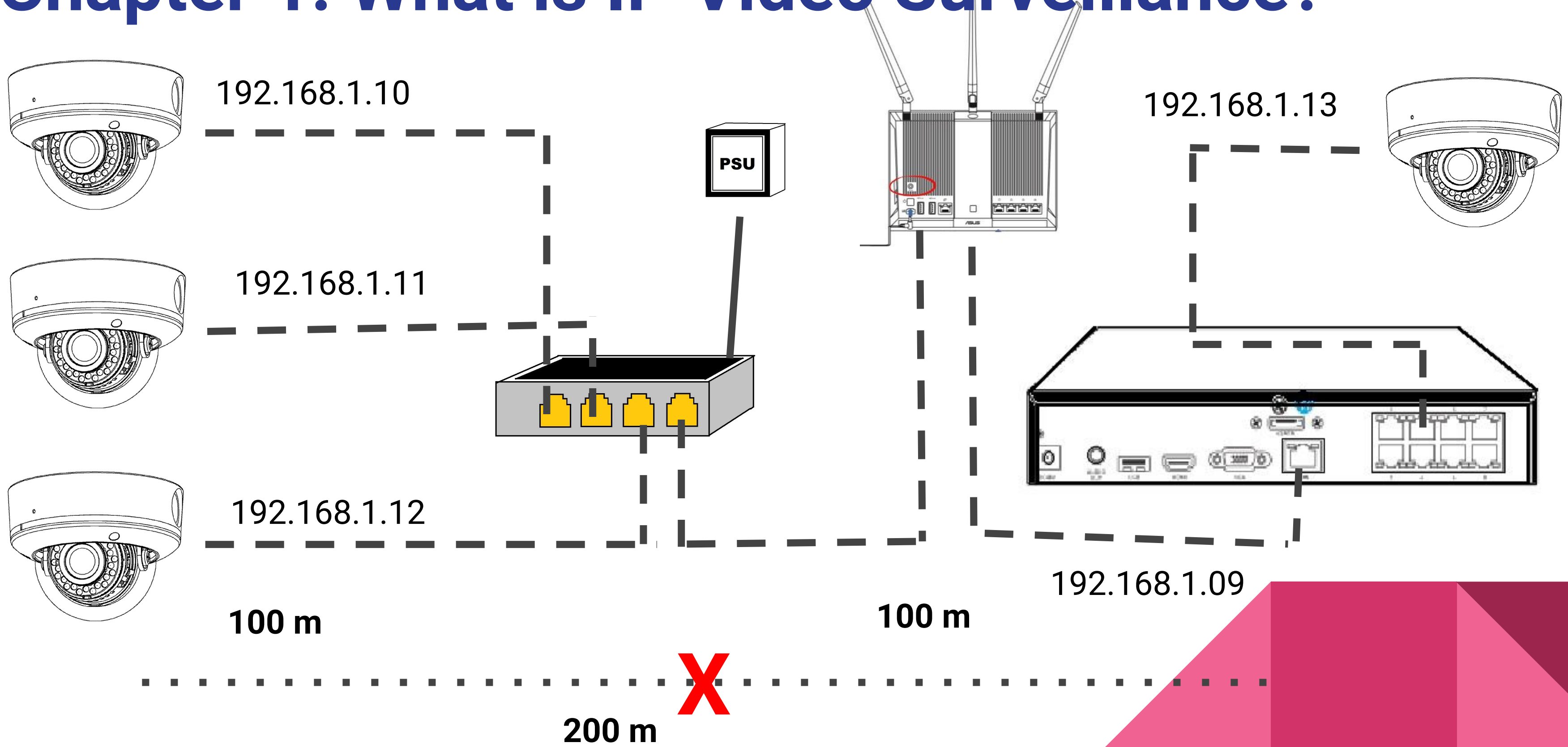


192.168.1.14

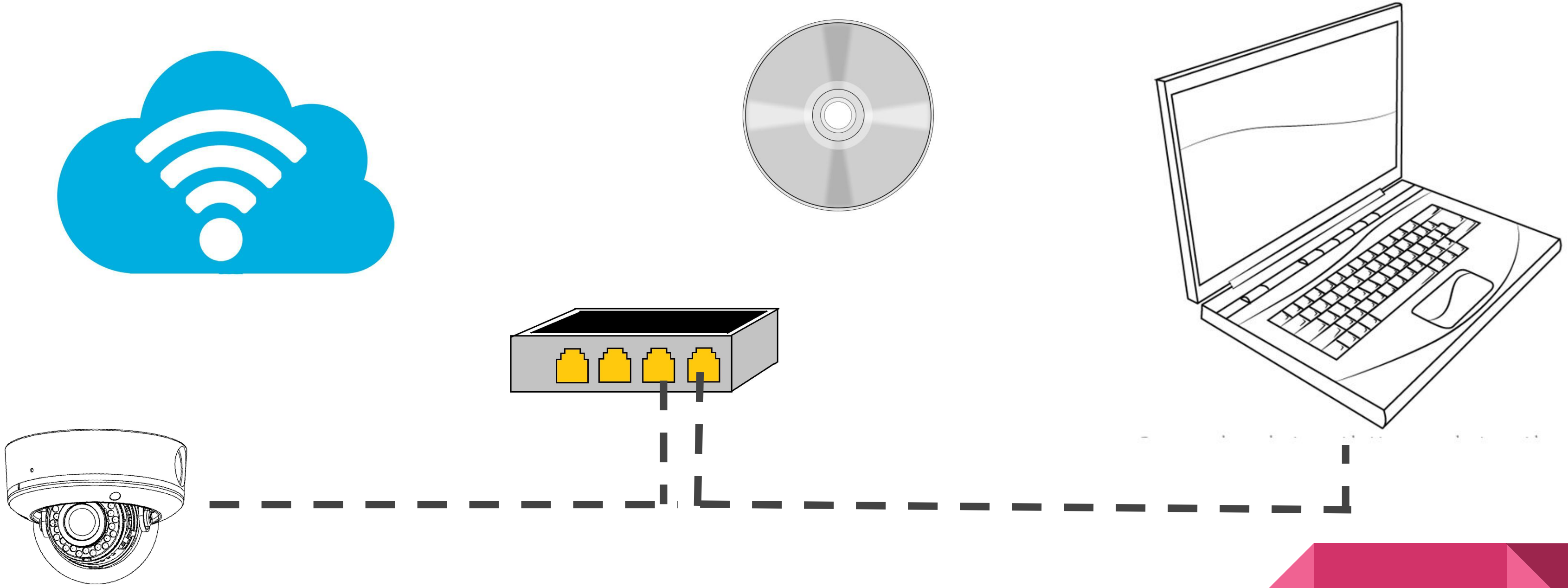
192.168.1.13

192.168.1.12

Chapter 1: What is IP Video Surveillance?



Chapter 1: What is IP Video Surveillance?



Chapter 1: What is IP Video Surveillance?

Question time:

Q1: What is the difference between a managed and unmanaged switch?

One difference between managed and unmanaged switches is complexity. A managed switch is more complex and requires more skills, but it offers better network control and configuration.

Chapter 1: What is IP Video Surveillance?

Question time:

Q2:

What is a PoE camera?

Power over Ethernet (POE) is a technology that lets network cables carry electrical power.

Chapter 2: Introduction to Computer Networks

Data Communication

Components:

1. Message
2. Sender
3. Receiver
4. Transmission medium
5. Protocol

Chapter 2: Introduction to Computer Networks

Data Representation:

Information today comes in different forms such as text, numbers, images, audio, and video.

Chapter 2: Introduction to Computer Networks

Data packets:

Packets are the basic units of communication over a TCP/IP network. Devices on a TCP/IP network divide data into small pieces, allowing the network to accommodate various bandwidths, to allow for multiple routes to a destination, and to retransmit the pieces of data which are interrupted or lost. Each piece is a packet, a term interchangeable with datagram.

Chapter 2: Introduction to Computer Networks

What is a bit in computer?

A **bit** (short for binary digit) is the smallest unit of data in a **computer**. A **bit** has a single binary value, either 0 or 1.

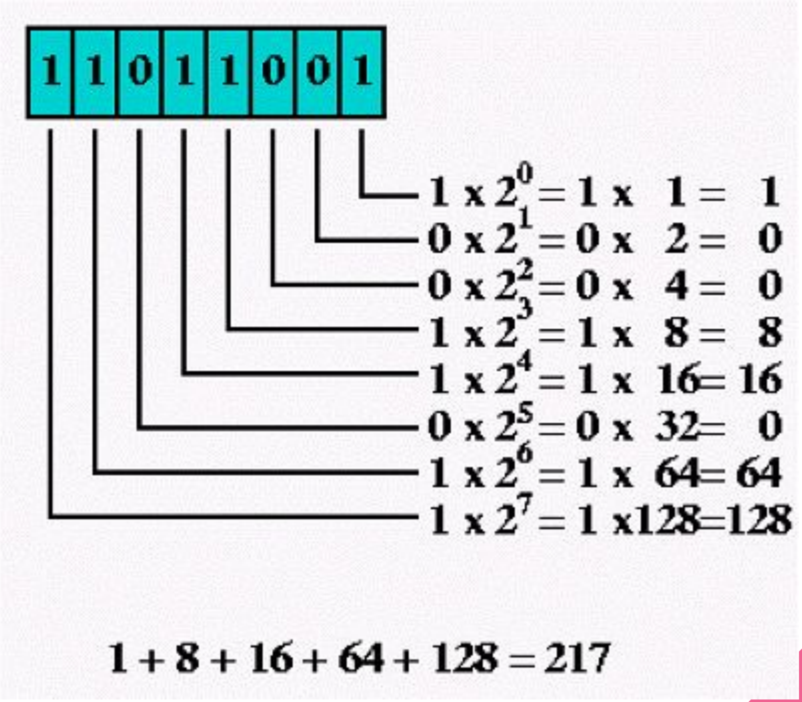
Chapter 2: Introduction to Computer Networks

Binary:

In mathematics and digital electronics, a binary number is a number expressed in the base-2 numeral system or binary numeral system, which uses only two symbols: typically "0" and "1". The base-2 numeral system is a positional notation with a radix of 2.

Chapter 2: Introduction to Computer Networks

Binary to decimal:



1	1	0	1	1	0	0	1

$1 \times 2^{0} = 1 \times 1 = 1$

$0 \times 2^{1} = 0 \times 2 = 0$

$0 \times 2^{2} = 0 \times 4 = 0$

$1 \times 2^{3} = 1 \times 8 = 8$

$1 \times 2^{4} = 1 \times 16 = 16$

$0 \times 2^{5} = 0 \times 32 = 0$

$1 \times 2^{6} = 1 \times 64 = 64$

$1 \times 2^{7} = 1 \times 128 = 128$

$1 + 8 + 16 + 64 + 128 = 217$

Exercise 1: Binary to decimal conversion

Binary to decimal convertor.

Computer Network Types

- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

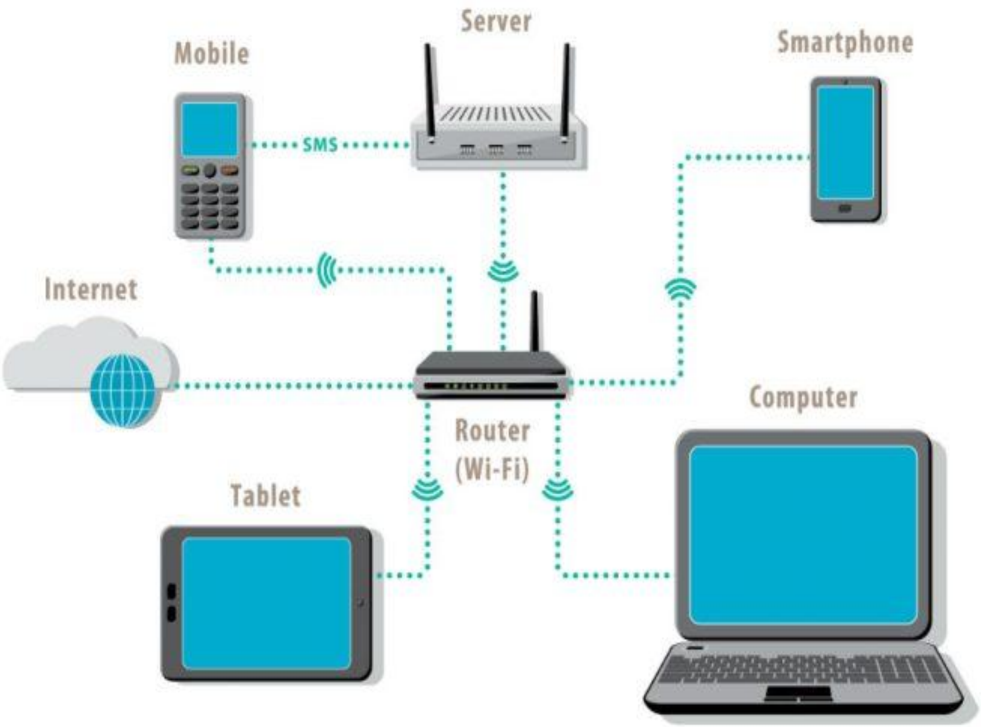
Computer Network Types

- **What is a LAN(Local Area Network)**

  Local Area Network is a group of computers connected to each other in a small area such as building, office.

Computer Network Types

- **LAN**



Computer Network Types

How to find a local area network TCP/IP setting?

How do I find the local IP address of my laptop or desktop?

1. From the desktop, navigate through; Start > Run> type "cmd.exe". A command prompt window will appear.
2. At the prompt, type "ipconfig /all". All IP information for all network adapters in use by Windows will be displayed.

Computer Network Types

How to find a local area network TCP/IP setting?

How do I find my local IP address on Android?

1. Go to “Settings” and tap on “About device” option at the very bottom.
2. Here tap on “Status” and you'll find the local IP address listed under the “IP address” section.

Computer Network Types

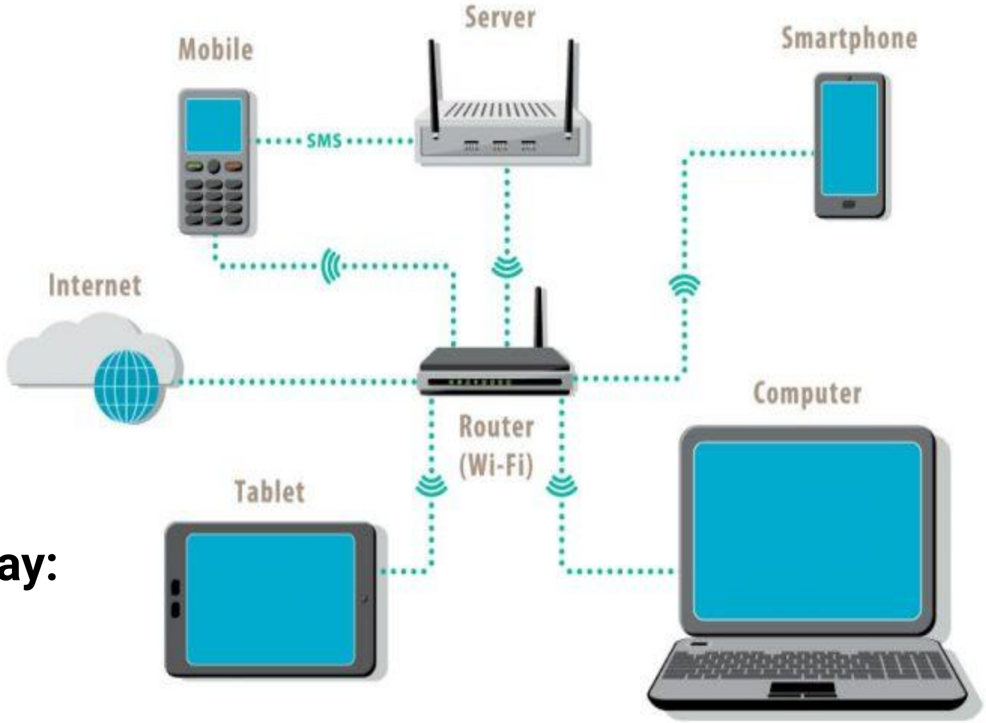
How to find a local area network TCP/IP setting?

How to Find the IP Address of Your iPhone.

1. Press to select Settings from your SpringBoard.
2. Press to select Wi-Fi from the Settings menu.
3. Press to select your network if it isn't already selected. Then next to your network name press the blue circle with the i in it.
4. You will now be displayed your iPhone's IP Address!

Computer Network Types

- LAN

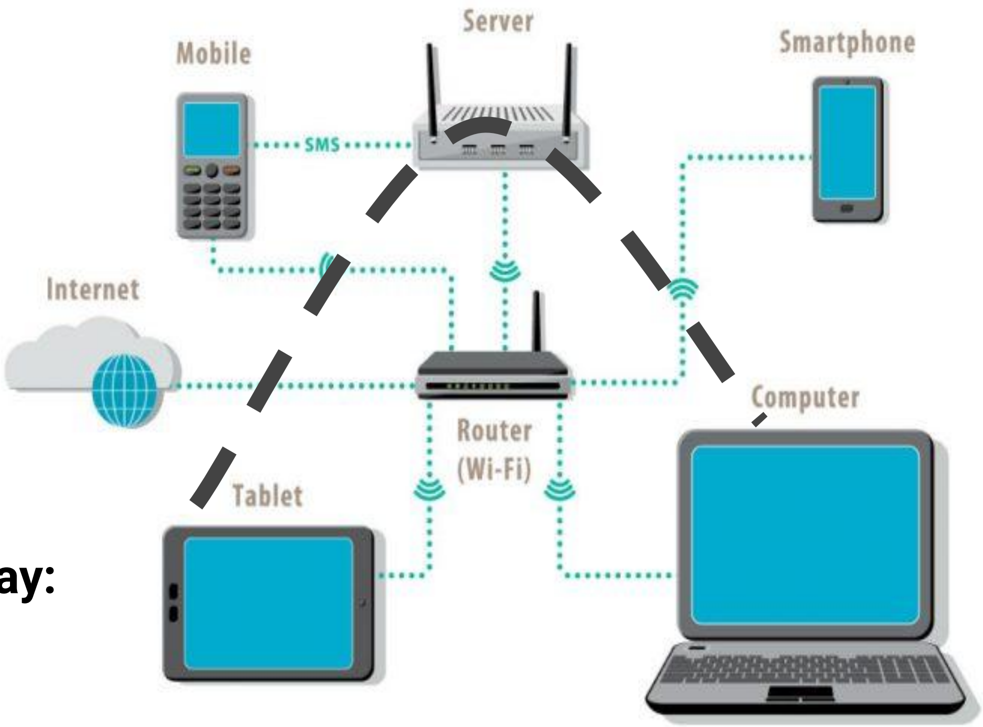


IPv4 address:
192.168.1.14
Subnet Mask:
255.255.255.0
Default Gateway:
192.168.1.254

IPv4 address:
192.168.1.13
Subnet Mask:
255.255.255.0
Default Gateway:
192.168.1.254

Computer Network Types

- LAN



Mobile:
IPv4 address:
192.168.1.14
Subnet Mask:
255.255.255.0
Default Gateway:
192.168.1.254

Laptop:
IPv4 address:
192.168.1.13
Subnet Mask:
255.255.255.0
Default Gateway:
192.168.1.254

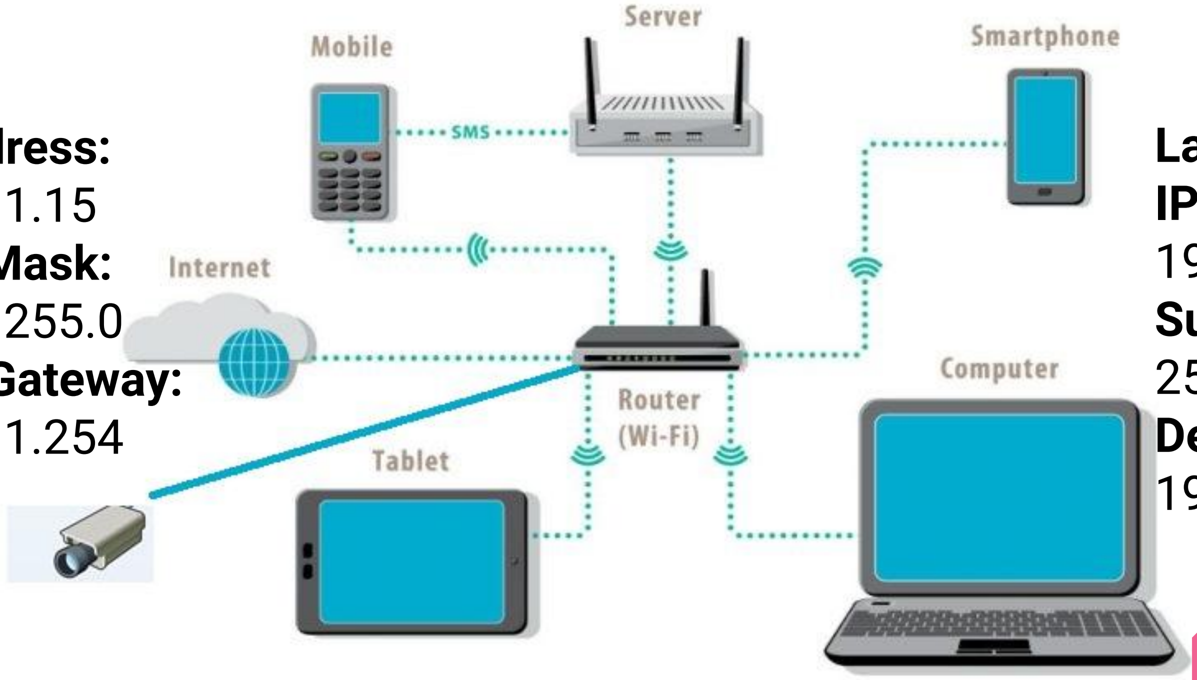
Chapter 2: Introduction to Computer Networks

- **LAN - Ping Test**

  When a situation such as this one occurs it’s encouraged that you first conduct a ping test.
  Pinging is usually the first line of defense when troubleshooting internet connections.

Chapter 2: Introduction to Computer Networks

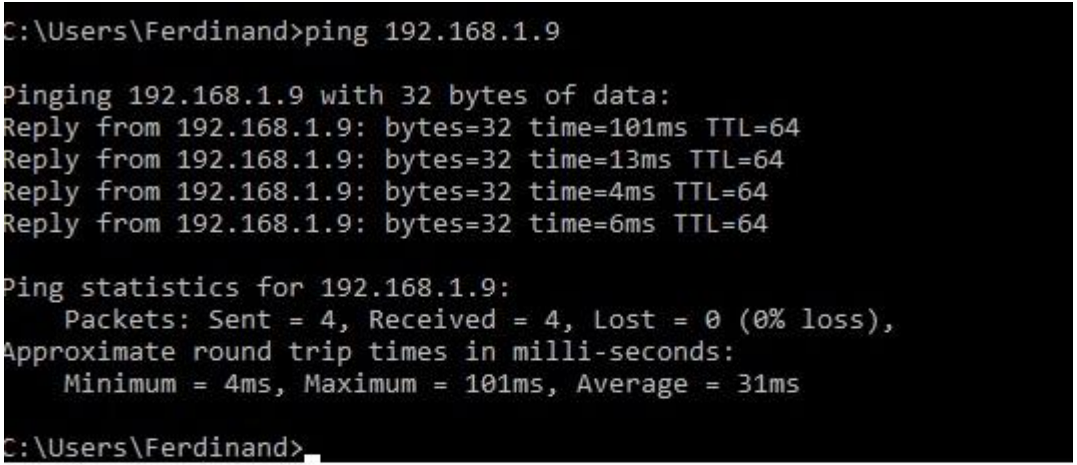
Camera:
IPv4 address:
192.168.1.15
Subnet Mask:
255.255.255.0
Default Gateway:
192.168.1.254



Laptop:
IPv4 address:
192.168.1.13
Subnet Mask:
255.255.255.0
Default Gateway:
192.168.1.254

Chapter 2: Introduction to Computer Networks

Ping test result:

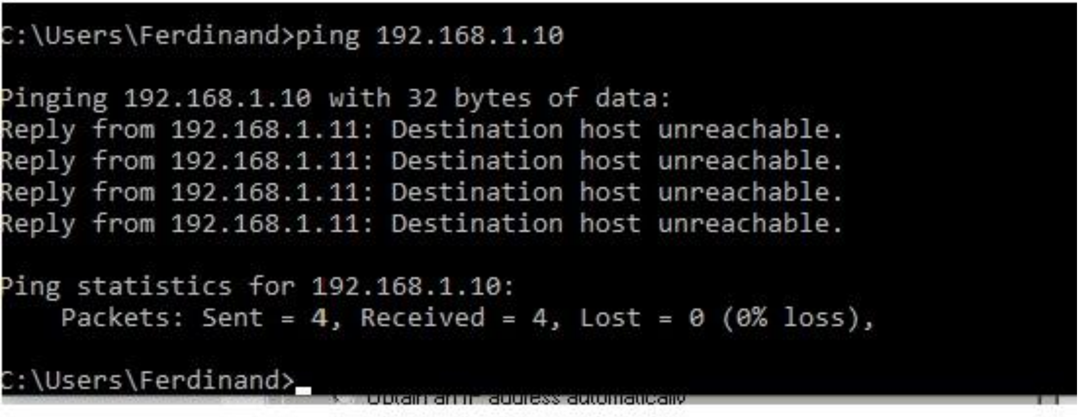


```
C:\Users\Ferdinand>ping 192.168.1.9

Pinging 192.168.1.9 with 32 bytes of data:
Reply from 192.168.1.9: bytes=32 time=101ms TTL=64
Reply from 192.168.1.9: bytes=32 time=13ms TTL=64
Reply from 192.168.1.9: bytes=32 time=4ms TTL=64
Reply from 192.168.1.9: bytes=32 time=6ms TTL=64

Ping statistics for 192.168.1.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 101ms, Average = 31ms

C:\Users\Ferdinand>
```

SUCCESSFUL

Chapter 2: Introduction to Computer Networks

Ping test result:

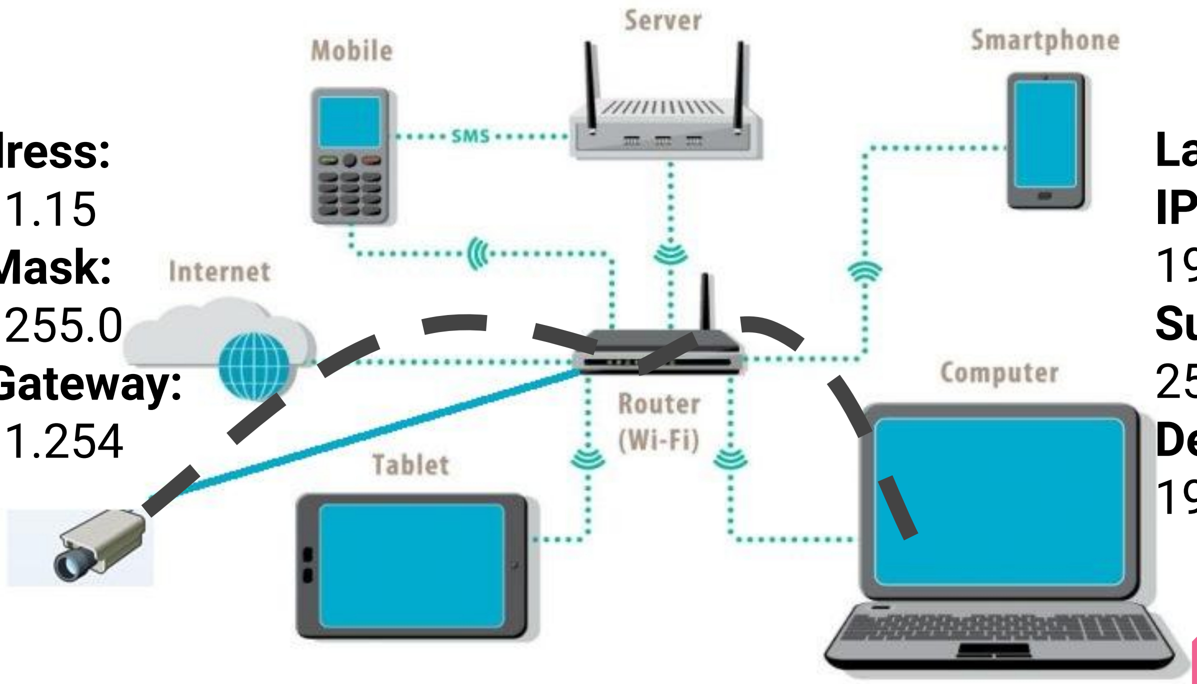


```
C:\Users\Ferdinand>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.11: Destination host unreachable.
Reply from 192.168.1.11: Destination host unreachable.
Reply from 192.168.1.11: Destination host unreachable.
Reply from 192.168.1.11: Destination host unreachable.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Ferdinand>_
```

FAILED

Chapter 2: Introduction to Computer Networks

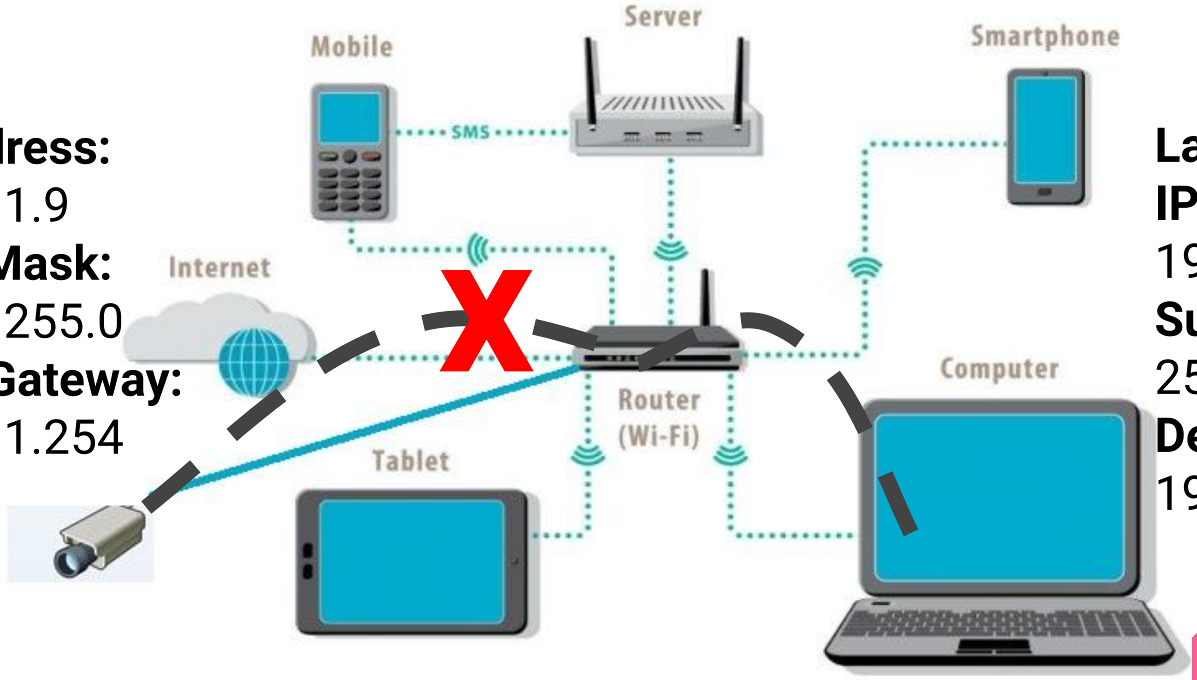
Camera:
IPv4 address:
192.168.1.15
Subnet Mask:
255.255.255.0
Default Gateway:
192.168.1.254



Laptop:
IPv4 address:
192.168.1.13
Subnet Mask:
255.255.255.0
Default Gateway:
192.168.1.254

Chapter 2: Introduction to Computer Networks

Camera:
IPv4 address:
192.168.1.9
Subnet Mask:
255.255.255.0
Default Gateway:
192.168.1.254



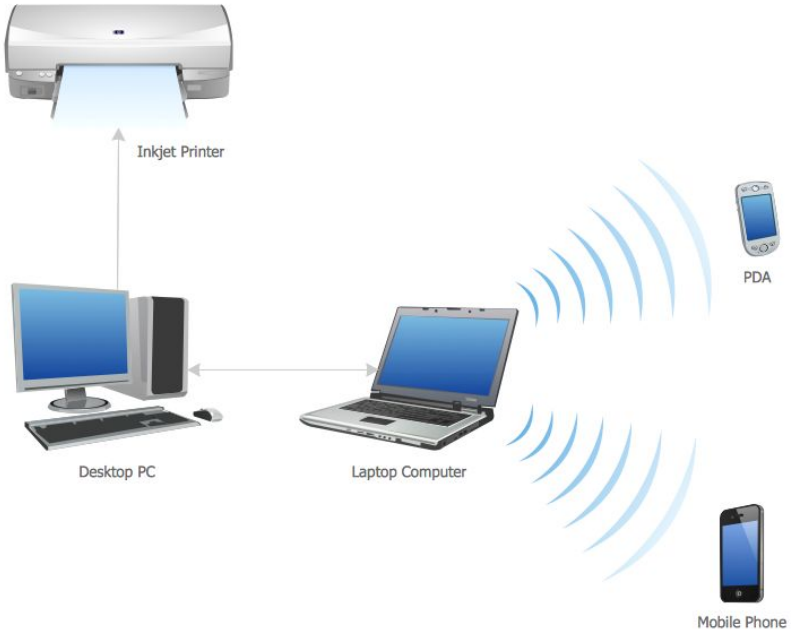
Laptop:
IPv4 address:
192.168.1.13
Subnet Mask:
255.255.255.0
Default Gateway:
192.168.1.254

Chapter 2: Introduction to Computer Networks

- **PAN(Personal Area Network):**

  A personal area network is a computer network for interconnecting devices centered on an individual person's workspace. A PAN provides data transmission among devices such as computers, smartphones, tablets and personal digital assistants.

Chapter 2: Introduction to Computer Networks



PAN (Personal Area Network)

Chapter 2: Introduction to Computer Networks

- **MAN(Metropolitan Area Network):**

  A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN).

Chapter 2: Introduction to Computer Networks

- **WAN(Wide Area Network):**

  A **wide-area network** (**WAN**) spans a relatively large geographical area and typically consists of two or more local-area networks (LANs).

Chapter 2: Introduction to Computer Networks

Network topologies and types of networks

- Bus Topology
- Ring Topology
- Star Topology
- Mesh Topology
- Tree Topology

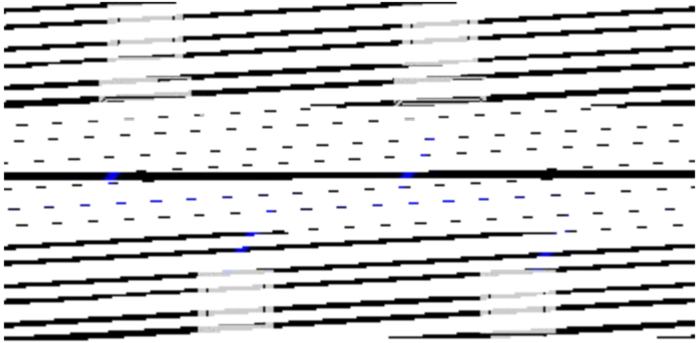
Chapter 2: Introduction to Computer Networks

Bus Topology:

The network setup where each computer and network device is connected to a single cable or backbone. Depending on the type of computer network card, a coaxial cable or an RJ-45 network cable is used to connect them together.

Chapter 2: Introduction to Computer Networks

Bus Topology:



Chapter 2: Introduction to Computer Networks

Bus Topology:

Advantages:

- It works well when you have a small network.
- It's the easiest network topology for connecting computers or peripherals in a linear fashion.
- It requires less cable length than a star topology.

Chapter 2: Introduction to Computer Networks

Bus Topology:

Disadvantages:

- It can be difficult to identify the problems if the whole network goes down.
- It can be hard to troubleshoot individual device issues.
- Bus topology is not great for large networks.

Chapter 2: Introduction to Computer Networks

Bus Topology:

Disadvantages:

- Terminators are required for both ends of the main cable.
- Additional devices slow the network down.
- If a main cable is damaged, the network fails or splits into two.

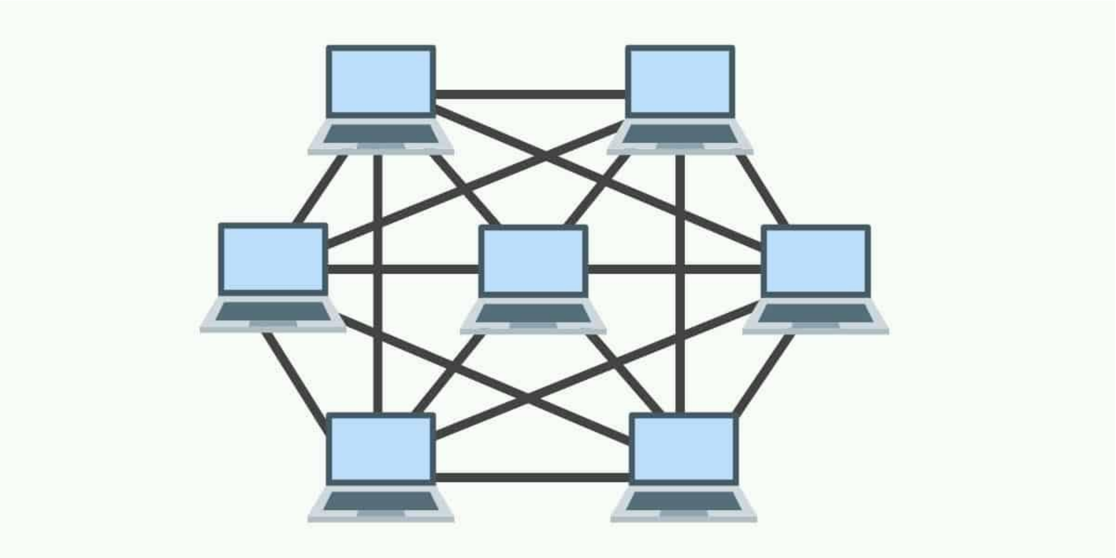
Chapter 2: Introduction to Computer Networks

Mesh Topology:

- A network setup where each computer and network device is interconnected with one another, allowing for most transmissions to be distributed even if one of the connections go down.

Chapter 2: Introduction to Computer Networks

Mesh Topology:



Chapter 2: Introduction to Computer Networks

Mesh Topology:

It is an inexpensive way to implement redundancy in a network. If one of the primary computers or connections in the network fails, the rest of the network continues to operate normally.

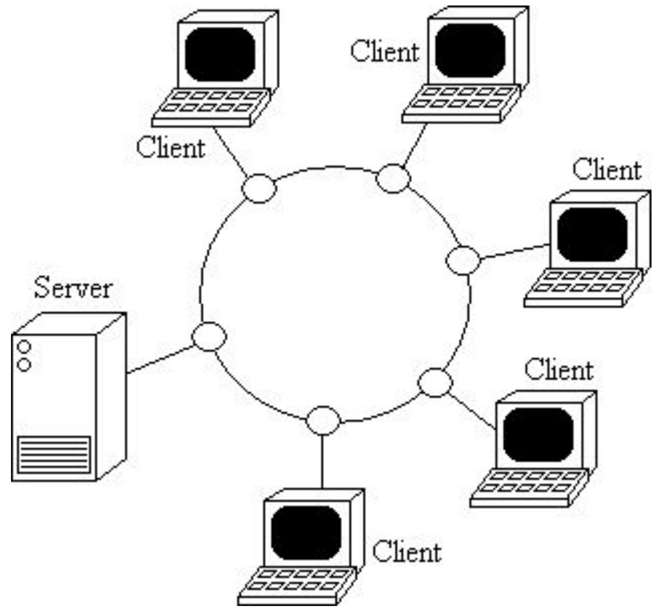
Chapter 2: Introduction to Computer Networks

Ring Topology:

A ring topology is a network configuration in which device connections create a circular data path.

Chapter 2: Introduction to Computer Networks

Ring Topology:



Chapter 2: Introduction to Computer Networks

Advantages of Ring Topology:

- All data flows in one direction, reducing the chance of packet collisions.
- A network server is not needed to control network connectivity between each workstation.
- Data can transfer between workstations at high speeds.
- Additional workstations can be added without impacting performance of the network.

Chapter 2: Introduction to Computer Networks

Disadvantages of Ring Topology:

- All data being transferred over the network must pass through each workstation on the network, which can make it slower than a star topology.
- The entire network will be impacted if one workstation shuts down.
- The hardware needed to connect each workstation to the network is more expensive than Ethernet cards and hubs/switches.

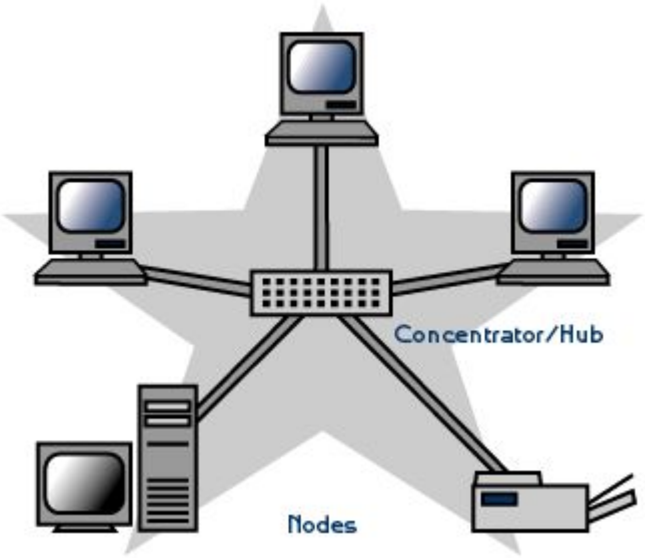
Chapter 2: Introduction to Computer Networks

Star Topology:

Star topology is one of the most common network setups.
The central network device acts as a server and the peripheral devices act as clients.

Chapter 2: Introduction to Computer Networks

Star Topology:



Chapter 2: Introduction to Computer Networks

Advantages star topology:

- Centralized management of the network, through the use of the central computer, hub, or switch.
- Easy to add another computer to the network.
- If one computer on the network fails, the rest of the network continues to function normally.

Chapter 2: Introduction to Computer Networks

Disadvantages star topology:

- May have a higher cost to implement, especially when using a switch or router as the central network device.
- The central network device determines the performance and number of nodes the network can handle.
- If the central computer, hub, or switch fails, the entire network goes down and all computers are disconnected from the network.

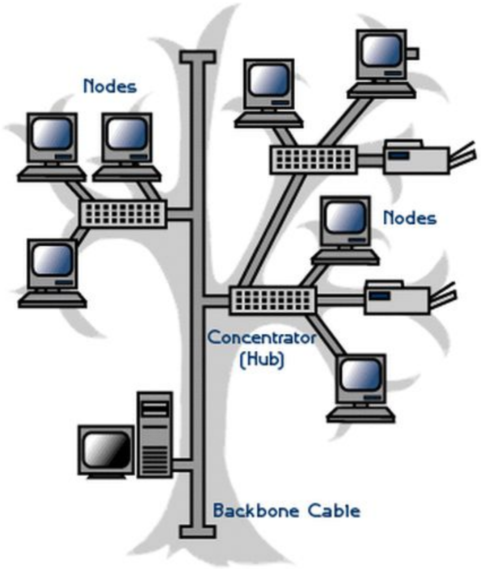
Chapter 2: Introduction to Computer Networks

Tree topology:

A **tree topology** is a special type of structure in which many connected elements are arranged like the branches of a tree. For example, tree topologies are frequently used to organize the computers in a corporate network or the information in a database.

Chapter 2: Introduction to Computer Networks

Tree topology:



Chapter 3: Internet Protocol

The Internet is a global network of billions of computers and other electronic devices.

Chapter 3: Internet Protocol

Routing Traffic Across the Internet:

1. Request must be broken into packets
2. Packets are routed through your local network and possibly through one or more subsequent networks to the Internet backbone.
3. After leaving the backbone the packets are routed through one or more networks until they reach the appropriate server and are reassembled into the complete request.

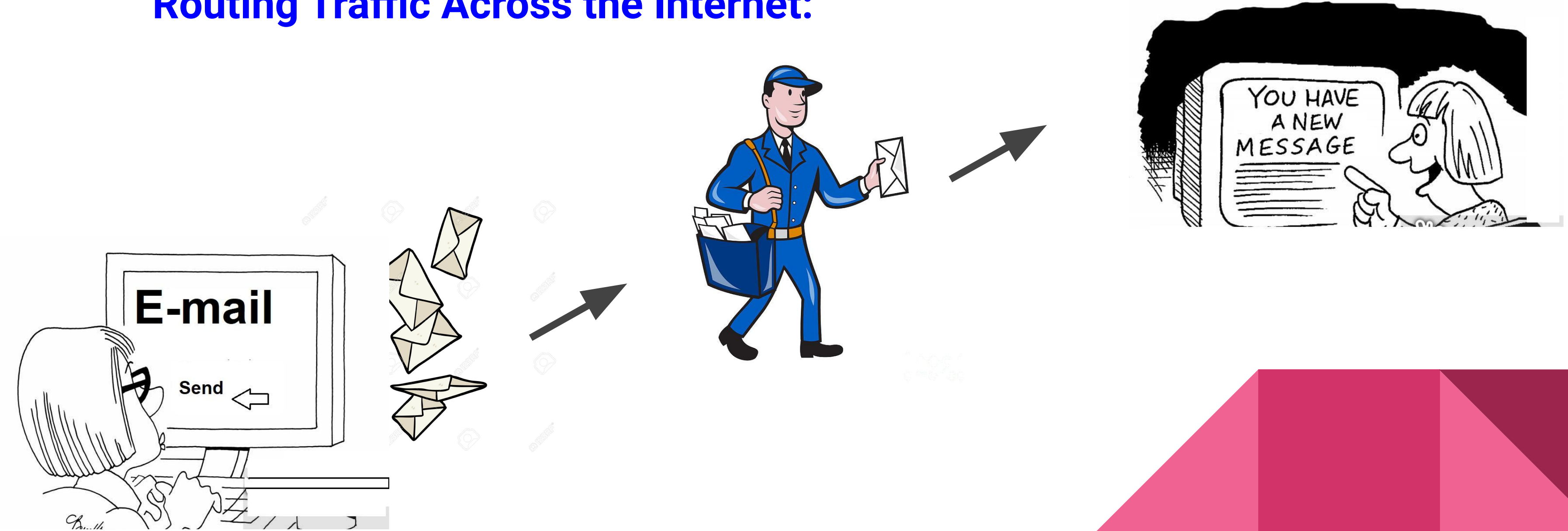
Chapter 3: Internet Protocol

Routing Traffic Across the Internet:

4. Once the destination server receives your request it begins sending you the requested data which winds its way back to you possibly over a different route.

Chapter 3: Internet Protocol

Routing Traffic Across the Internet:



Chapter 3: Internet Protocol

We use social protocols to know how to behave and communicate with other people. What if we don't have any protocol to communicate?

Chapter 3: Internet Protocol

TCP/IP

Just like people, it’s important for computers to have a common way to communicate with each other. Today most computers do this through TCP/IP.

TCP/IP stands for Transmission Control Protocol/Internet Protocol. TCP/IP is a set of standardized rules that allow computers to communicate on a network such as the internet.

Chapter 3: Internet Protocol

TCP/IP

What is the difference between TCP and IP?

IP is the part that obtains the address to which data is sent.
TCP is responsible for data delivery once that IP address has been found.

Chapter 3: Internet Protocol

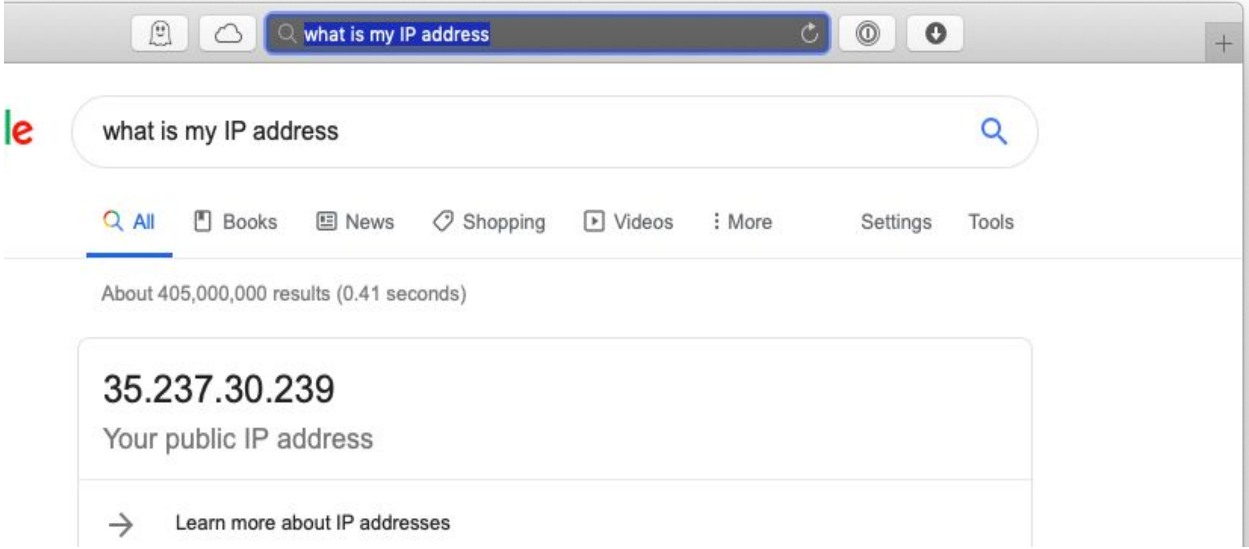
IP address

What is an IP address?

A public IP address is an IP address that your home or business router receives from your ISP(Internet Service Provider).

Chapter 3: Internet Protocol

IP address



About 405,000,000 results (0.41 seconds)

35.237.30.239

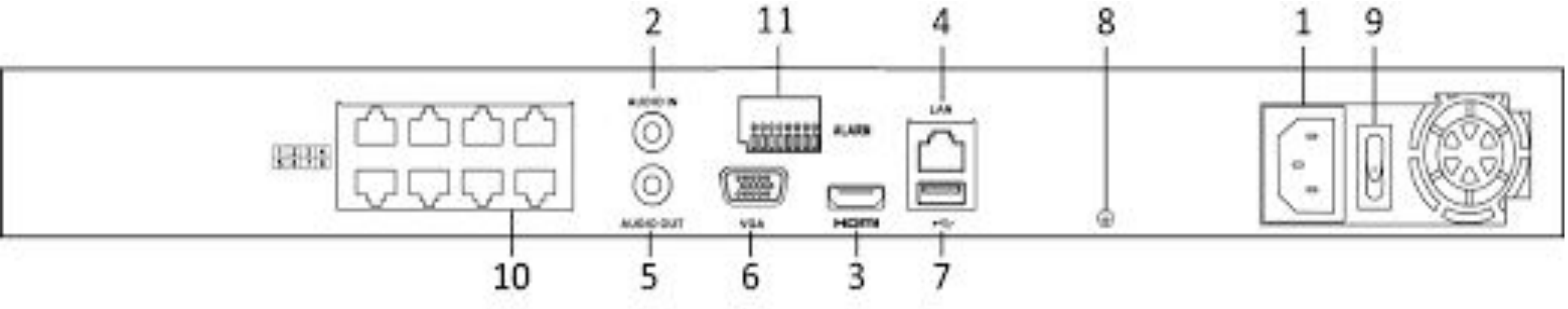
Your public IP address

How to set the TCP setting of your video surveillance system?

How to find the TCP/IP setting in your NVR or DVR?

NVR - (Network Video Recorder)

1 - Power (Mains), 2 - Audio in, 3 - HDMI, 4 - LAN, 5 - Audio out, 6 - VGA



7 - USB port, 8 - Earth, 9 - Power switch, 10 - PoE ports for cameras

Chapter 4: Onvif and private protocols

ONVIF (Open Network Video Interface Forum):

ONVIF is an open industry forum that provides and promotes standardized interfaces for effective interoperability of IP-based physical security products.

PSIA (Physical Security Interoperability Alliance)

The Physical Security Interoperability Alliance (PSIA) is a global consortium of physical security product companies and system integrators focused on promoting interoperability of IP-enabled security devices and systems across the security ecosystem and beyond.

Chapter 4: Onvif and private protocols

RTSP (Real Time Streaming Protocol):

The Real Time Streaming Protocol (RTSP) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.

RTSP provides unprecedented ease of implementation and has been embraced by nearly every mainstream IP-camera manufacturer in the market.

This protocol will allow you to live-stream your camera on social platforms such as youtube, Facebook, etc.

Chapter 4: Onvif and private protocols

RTMP (Real Time Messaging Protocol):

RTMP is mostly depreciated for use as a viewer-facing video streaming protocol. That’s because it’s dependent on the Flash plugin, which has been plagued with security problems for years and is rapidly becoming obsolete.

RTMP is a streaming protocol providing very low latency streams. The drawbacks of RTMP protocol is that it's vulnerable to bandwidth issues and it requires a flash media player.

Chapter 4: Onvif and private protocols

HTTP Live Streaming (HLS):

HTTP Live Streaming (also known as HLS) is an HTTP-based adaptive bitrate streaming communications protocol developed by Apple Inc.

Chapter 4: Onvif and private protocols

Private Protocols:

- Hikvision
- Dahua
- Axis
- Bosch

Chapter 4: Onvif and private protocols

Private Protocols:

How compatible are private protocols?

Can you connect a Hikvision camera to a Dahua NVR?

Yes, you can integrate cameras with different protocols as long as they are compatible with an open protocol. Most security surveillance systems are compatible with ONVIF standards. By using this open protocol ONVIF, cameras of different makes can be integrated as a single solution.

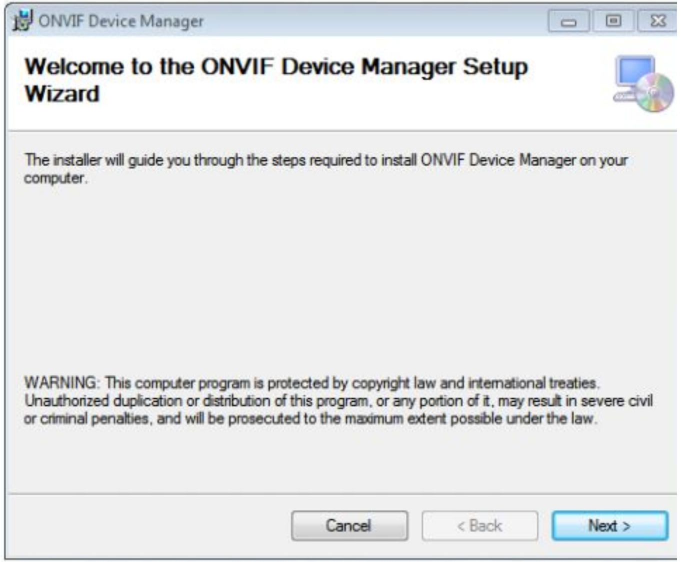
ONVIF

Downloading the ONVIF device manager

Open web browser - download ONVIF device manager -

URL: Download onvifdm.msi setup-file from Synesis (http://synesis.ru/ru/surveillance/downloads) or SourceForge (http://sourceforge.net/projects/onvifdm/) web site.

ONVIF



Welcome to the ONVIF Device Manager Setup Wizard

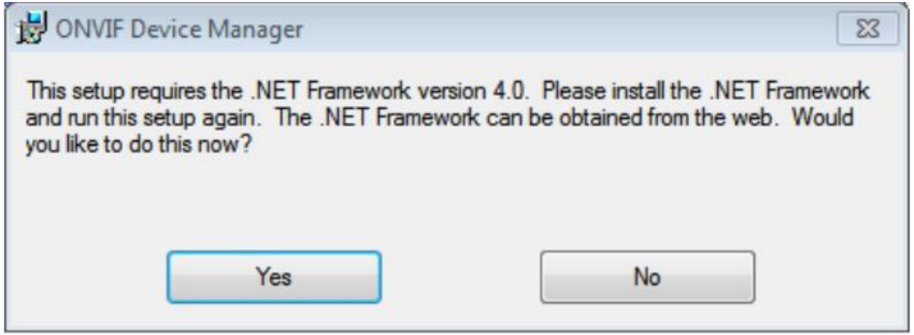
The installer will guide you through the steps required to install ONVIF Device Manager on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

ONVIF Installation

Run onvifdm.msi.

Setup Wizard will check if Microsoft .NET Framework 4 is installed to the computer. If it is absent, the following message is displayed.



This setup requires the .NET Framework version 4.0. Please install the .NET Framework and run this setup again. The .NET Framework can be obtained from the web. Would you like to do this now?

ONVIF Installation

Click Yes. You will be redirected to http://www.microsoft.com/

Download dotNetFx40_Full_setup.exe and install .NET Framework according to the setup instructions.

After Microsoft .NET Framework 4 setup run onvifdm.msi again.

(**NET Framework** is **used to** create and run software applications. . **NET** apps can run on many operating systems, using different implementations of . **NET**. . **NET Framework** is **used for** running)

ONVIF Installation

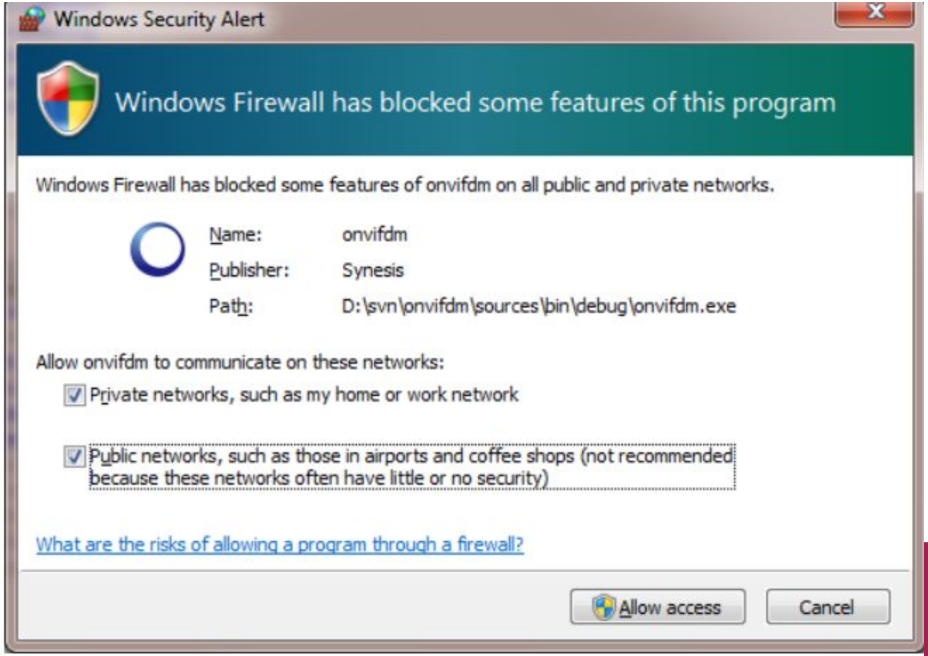
Windows User Account Control may ask for the permission to continue the installation. Click Yes.

To complete ONVIF Device Manager installation process, click Close.

Starting ONVIF

Launch ONVIF Device Manager from the desktop or Start menu.

During the first launch, Windows Firewall may ask for the permission to open access to the network for onvifdm.exe. Click Allow access.



Windows Firewall has blocked some features of this program

Windows Firewall has blocked some features of onvifdm on all public and private networks.

Name: onvifdm

Publisher: Synesis

Path: D:\svn\onvifdm\sources\bin\debug\onvifdm.exe

Allow onvifdm to communicate on these networks:

☑ Private networks, such as my home or work network

☑ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

What are the risks of allowing a program through a firewall?

Starting ONVIF

After ONVIF Device Manager has been launched, your device is automatically detected and displayed at the end of the device list on the left. If the device has not been detected automatically, check the connection and click Refresh.

Hikvision - ONVIF (Enabling ONVIF)

ONVIF protocol has been disabled by default in IP camera firmware versions since v5.5.0.

Step 1: Open a Web browser.

Step 2: Access your camera by using its IP address.

Step 3: Go to CONFIGURATION > NETWORK > ADVANCED SETTINGS > INTEGRATION PROTOCOL.

Hikvision - ONVIF (Enabling ONVIF)

Step 4: Under Security - change RTSP and WEB from digest to digestbasic

(H.265 or H.265 + profile may not work with ONVIF.)

Step 5: Network - Advanced setting - Enable Hikvision CGI - Digest and enable ONVIF.

Step 6: Add ONVIF user - user name and password

Step 7: Open ONVIF device manager and search for the camera in

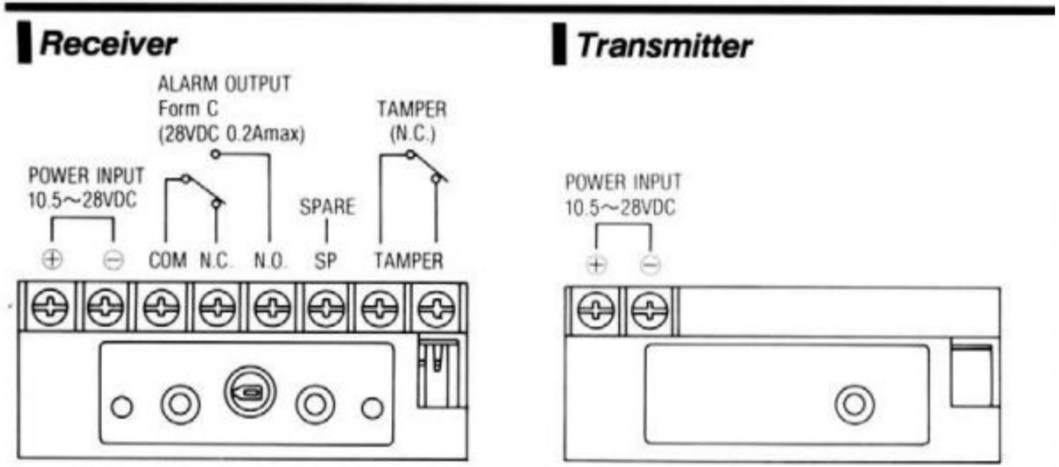
LAN or add the IP address of the camera.

Chapter 5: Alarm Integration

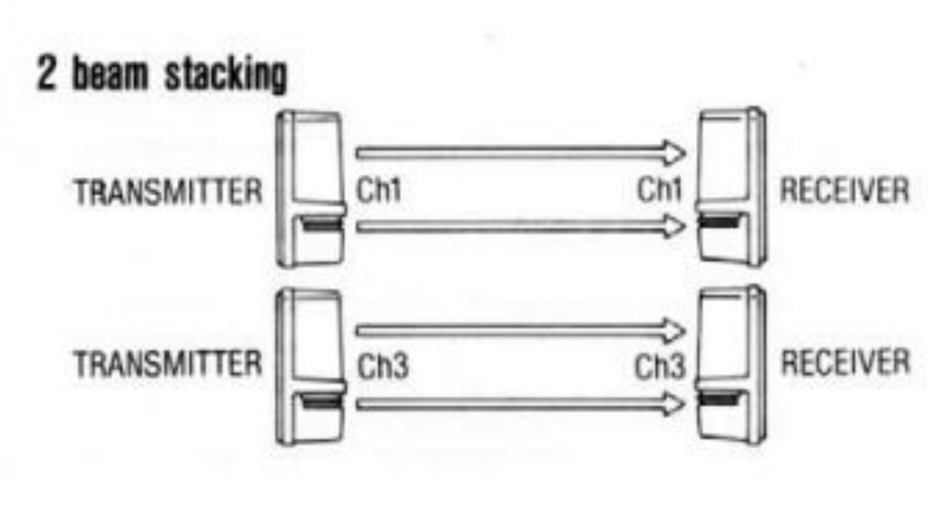
Integrating cameras with an alarm sensor gives us several advantages.

1. Accurate triggers
2. False alarm management
3. Effective utilisation of security surveillance system.

Alarm sensor



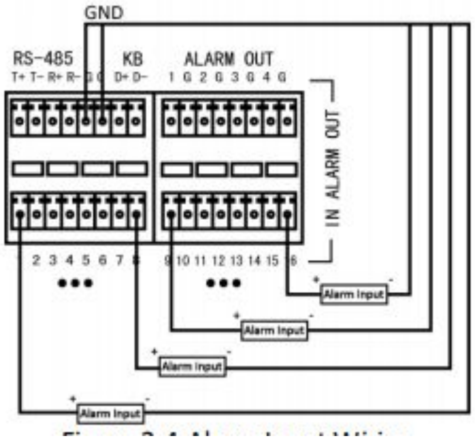
Alarm sensor



Alarm sensor

Alarm Input Wiring

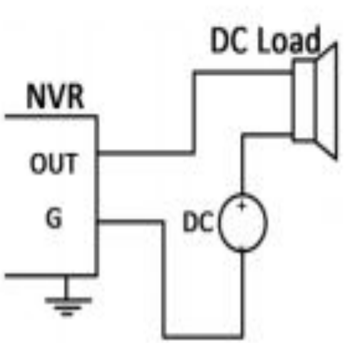
The alarm input is an open/closed relay. To connect the alarm input to the device, use the following diagram.

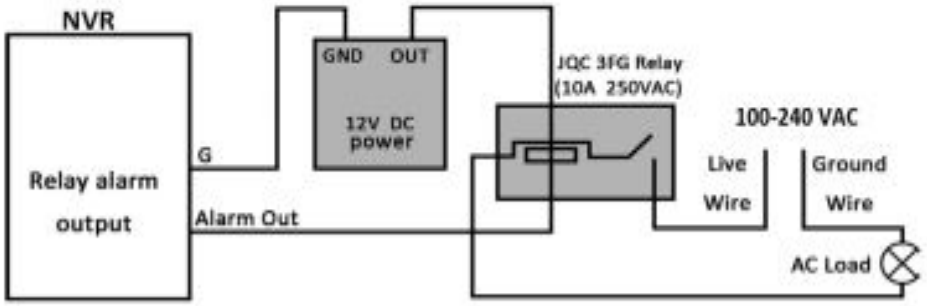


Alarm sensor

Alarm Output Wiring

To connect to an alarm output (AC or DC load), use the following diagram:





Alarm sensor

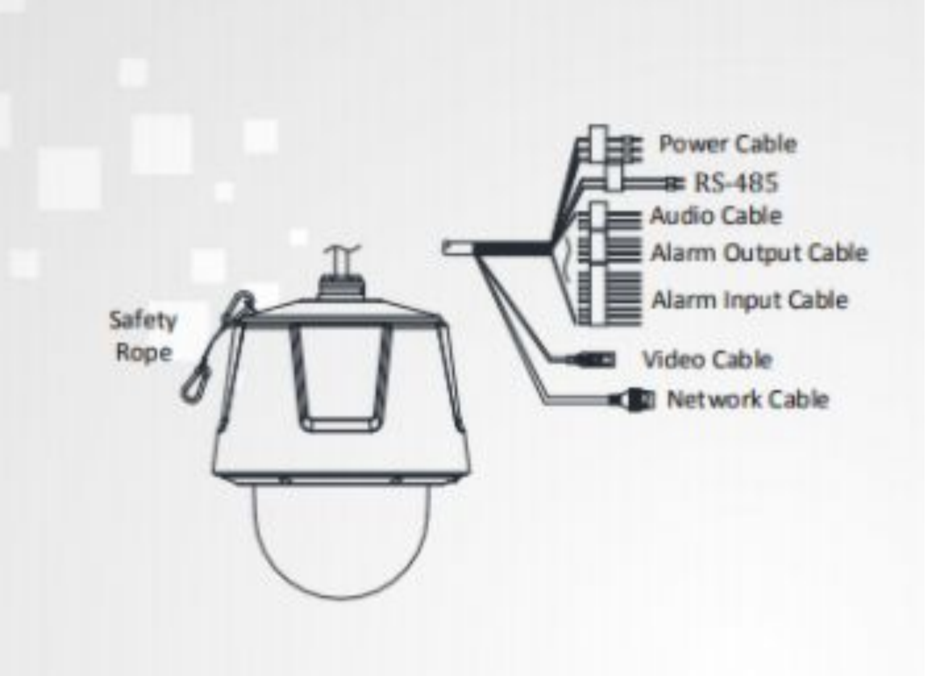
Alarm Output Wiring

For DC load, the jumpers can be used within the limit of 12V/1A safely.

To connect an AC load, jumpers should be left open (you must remove the jumper on the motherboard in the NVR).

Use an external relay for safety (as shown in the figure above). There are 4 jumpers (JP6, JP9, JP10, and JP11) on the motherboard, each corresponding with one alarm output. By default, jumpers are connected. To connect an AC load, jumpers should be removed.

Alarm sensor


Power Cable
RS-485
Audio Cable
Alarm Output Cable
Alarm Input Cable
Video Cable
Network Cable
Safety Rope