

**NANYANG  
TECHNOLOGICAL  
UNIVERSITY**  

---

**SINGAPORE**

**EE6223**

**Computer Control Networks**

**Assignment I**

**Team Name: May no rat bite our cable**

WANG MAOSEN, G2001567E (Most Contributor)

YANG RUIQI, G2002916G

WANG CHONGYU, G2002576G

ZHANG FENG, G2001866C

TIAN ZICHEN, G2002883L

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Assumptions</b>	<b>3</b>
<b>3</b>	<b>Solution</b>	<b>3</b>
3.1	Remote Work and Design . . . . .	4
3.2	24/7 Availability . . . . .	4
3.3	Security of Network . . . . .	5
3.4	Surveillance System . . . . .	5
3.5	Manufacturing Facility Network . . . . .	7
<b>4</b>	<b>Model Selection of Network Components</b>	<b>9</b>
4.1	Switch . . . . .	9
4.2	Cable . . . . .	12
4.3	Wireless AP Router . . . . .	14
4.4	VPN Service . . . . .	15
4.5	Surveillance System . . . . .	16
4.6	Server . . . . .	19
<b>5</b>	<b>Overall Topological Diagram</b>	<b>20</b>

# 1 Introduction

This report describes a corporate network that satisfies the following five features:

1. **Robust and 24/7 availability.** The redundancy for switches and servers, auto-backup and shielding enclosure are designed. Details in subsection 3.2.
2. **Security.** VPN access and VLAN groups are designed to address this. A VPN server authenticates all access to intranet data; the entire network is divided into four VLAN groups: 1) Surveillance group; 2) facility group; 3) off-site conference group; 4) remote working group. For non-critical internet access, dedicated wireless and wired are also designed, isolated from secured networks. Details in subsection 3.3.
3. **Remote work.** VPN technology is used to achieve remote access to the corporation's intranet. The VLAN group is designed for a real-time conference. Details in subsection 3.1.
4. **Intelligent manufacturing.** Equipment and sensors in wireless manufacturing facilities should be managed and controlled via a secure and reliable network. They should cater to future development. Therefore, IPv6 address and reliable networking are considered in our design. Details in subsection 3.5.
5. **Surveillance system.** Indoor and outdoor surveillance systems are designed. The H.265 compressing and SSD hard disk are used for long-term storage of surveillance video. Details in subsection 3.4.

The assignment is organized as follows: Section 2 gives assumptions like the company's physical size, the staff number, and the link rate demand. Section 3 describes the main issues to be solved in this network and provides a thorough scheme to address each issue. Section 4 gives the model selection of each network component. Section 5 gives the overall network topology diagram.

**We recommend readers take a quick look at Section 5 first to make life easier.** All diagrams are drawn in vector graph format, so can zoom-in for a clearer view.

## 2 Assumptions

**Rat:** Hopefully no rat bite our cable, although cables are armoured in our design.

**Budget:** The budget for the network should be within US\$ 3.5 billion.

**Physical Size:** For foundry and plant, we refer to the size of foundry (located at 60 Woodlands Industrial Park D St 2, Singapore 738406). For administration and research building, we refer to the size of CISCO SG centre (located at 8 Cross St, Singapore 048424). Details listed in Table 1.

**Table 1: Physical Size Assumption of Buildings**

Building	Physical Size	Floors	Staff
Administration Building	80m × 80m × 11m (262ft × 262ft × 36ft)	2	160
Research and Development Centre	80m × 80m × 11m (262ft × 262ft × 36ft)	2	200
Next Generation Wireless Production Plant	194m × 118m × 21m (633ft × 386ft × 68ft)	2	80
Next Generation Wireless Foundry	194m × 118m × 21m (633ft × 386ft × 68ft)	1	60
Utilities Building	NA	NA	30

**Manufacturing Facility Number & Link Rate:** Assume each manufacturing facility is of size  $10m \times 15m$ , then the plant and foundry each can contain 143 facilities.

**Staff Capability:** Staff number in each building, as shown in Table 1.

## 3 Solution

The demand of the network are divided into five topics: 1) Remote work and design; 2) 24/7 availability; 3) Security; 4) Surveillance System; 5) Manufacturing facility network (IOT). In this section, each topic is responded with a subsection.

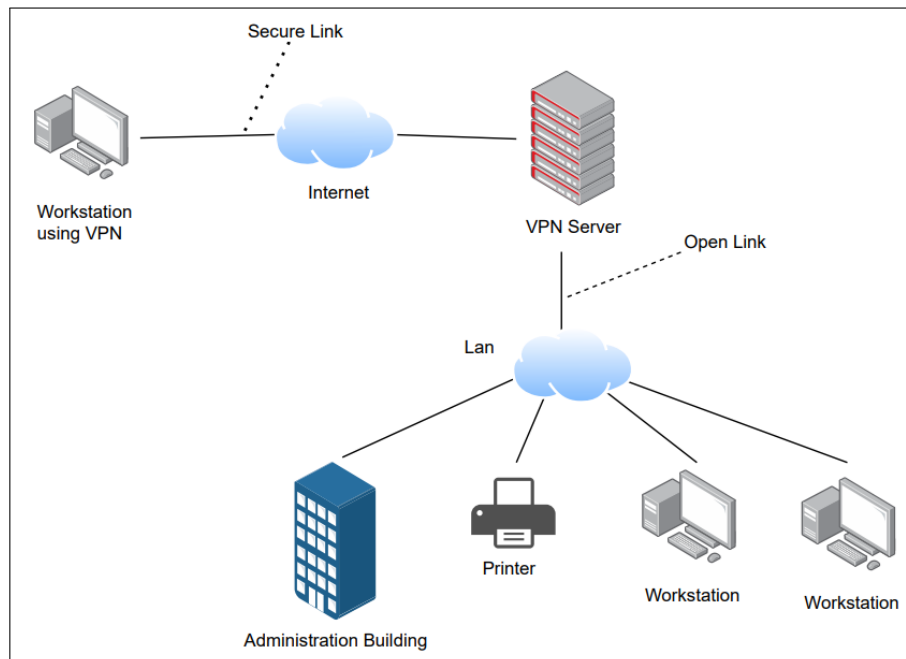


Figure 1: VPN working process

### 3.1 Remote Work and Design

Remote work is realized by using **VPN** technology. The VPN working process is shown in Figure 1. By installing a VPN server in the intranet, remote access is realized. When employees need to design or work remotely, they connect to the local Internet in the field and connect to the VPN server through the local Internet. Then, they can enter the corporate intranet through the VPN server. In order to ensure data security, the communication data between the VPN server and the client is encrypted. With data encryption, it can be considered that data is safely transmitted on a dedicated data link, just like a dedicated network is specially set up. The essence of VPN work is to use encryption technology to encapsulate a data communication tunnel on the public network.

### 3.2 24/7 Availability

We designed the **redundancy** devices, **auto backup** and **shielding enclosure** for all vital network components.

For **switches**, all the switches are accompanied with a redundancy switch, and

the redundancy switch should be placed in a different physical location. Figure 4 shows the overview of the core network, two core switches are deployed. Figure 5 shows the network for plant and foundry, the work group switches are accompanied with a POE switch, all of them will be placed into a secured shield to avoid fire/water/lightening etc. The details of switches are described in subsection 4.1.

For **servers**, the important intranet database has a backup on a remote cloud server. Diagram of server farm are shown in Figure 9, the encrypted servers are designed to be auto-back up time to time. The selection of servers are described in subsection 4.6

All the switches and servers are put **indoor and shielded**. All backbone cables should be **armoured in a insulating jacket** to avoid lightening and rat bite.

### 3.3 Security of Network

The security of the network is realized by implementing **VPN** and **VLAN** technologies.

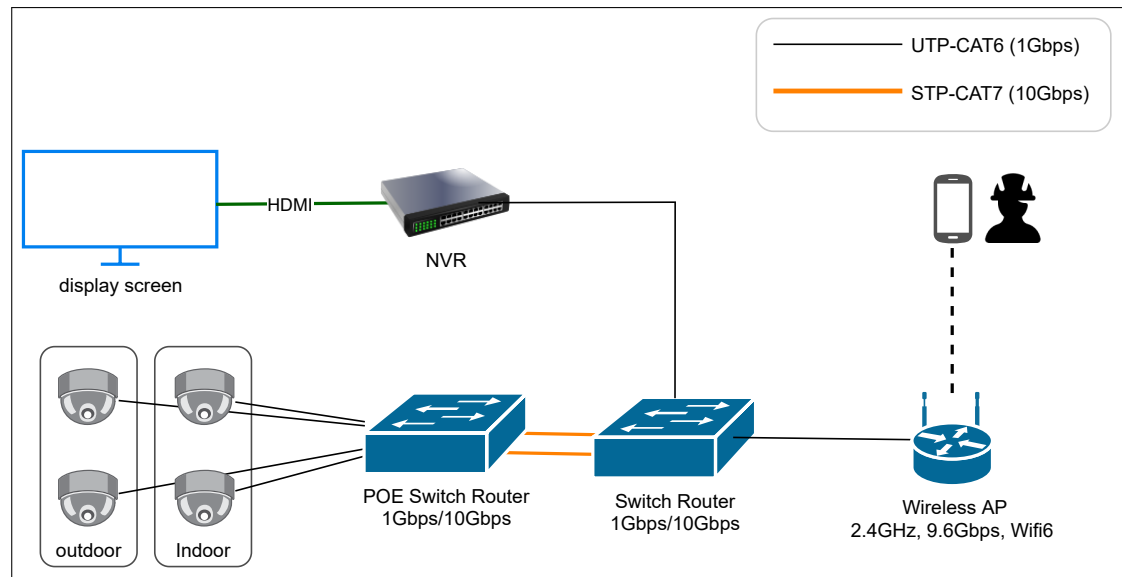
VPN uses traditional equipment to encrypt or decrypt the sent or received IP packets, and establish a ciphertext communication channel between the two ends of the communication on the IP communication network. The communication between two VPN devices can be done on a public network or the Internet, but it can achieve high security like communication within a private network.

VLAN is a two-layer isolation technology, the principle of which is to divide multiple VLANs on the switch. Users in the same VLAN can access each other, but data packets of one VLAN will not be sent to another VLAN on the switch. Therefore, the users of each VLAN are independent of each other on the network, thereby ensuring that the information of the VLAN will not be eavesdropped by the people of other VLANs, and improving the security of the network.

### 3.4 Surveillance System

In order to ensure the security of the monitoring system, a separate VLAN is set up for the monitoring system. Figure 2 shows the topology of surveillance system. The camera is powered by a PoE switch. The PoE switch supplies power to the PoE IPC through a network cable, which can avoid additional wiring. NVR is used to

centrally manage all cameras. Install cameras of different angles to form no blind spot monitoring. The monitoring system can set recording plans, video blocking, motion detection, playback, and export recording. The automatic switching of infrared day and night modes can ensure all-weather and all-day monitoring. The mobile phone APP can be used for remote monitoring anytime and anywhere. The surveillance camera reaches IP67 industrial grade dustproof and waterproof, and can still work normally in harsh environments.



**Figure 2: The surveillance system**

### NVR:

The number of access channels is a decisive factor in NVR selection. In fact, the number of NVR channels is calculated based on the number of cameras in the surveillance network.

One of the core functions of NVR in the surveillance network is to store videos. The storage time of videos is related to the total capacity of the hard disk. The number of disks is a key consideration in NVR selection. It is necessary to consider the number of IPCs, the number of storage days, and the bit rate of the IPCs to perform a comprehensive calculation to obtain the number of hard disks needed. It is estimated according to the 8M code rate (Using H.265 encoding method, so it is calculated according to 4M). And the capacity required at different times is shown as follows:

Based on the above calculations, if there are 24 H.265 IPCs need to be stored

**Table 2: Estimation of Storage**

Number of IPC	1 day	2 weeks	1 month
1	42GB	589GB	1260GB
8	336GB	4712GB	10080GB
24	1008GB	14136GB	30240GB

for one month, at least an 8-bay NVR is needed. The mainstream IPC encoding methods are H.264 and H.265. NVR can decode H.265 IPC only if it supports H.265 encoding. The H.265 coded IPC has a higher compression rate. In order to save storage space, choose H.265 coded IPC. Therefore, we need to choose a NVR which supports H.265.

Monitoring system should provide:

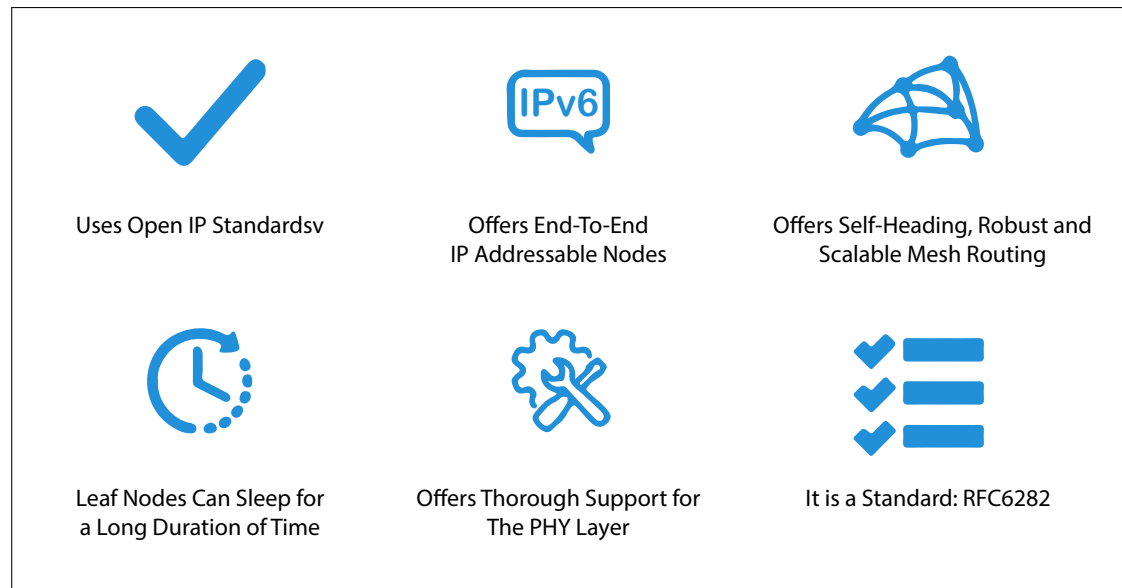
1. Isolated VLAN.
2. No blind point and automatic switching of infrared day and night modes.
3. Dustproof and waterproof.
4. Support WEB remote preview/playback, support mobile APP remote preview and video.
5. IPC and NVR support H.265 encoding.
6. The number of disks provided by NVR and the supported hard disk can store one month's surveillance video.
7. Support multiple intelligent detection functions such as motion detection, occlusion detection, video interruption detection, etc.

### 3.5 Manufacturing Facility Network

The designing of manufacturing facility is introduced in this part. To meet the future development and considering the machines and sensors in the plant are low power, and the requirement for data transmission speed in manufacturing facility is not high, IPv6 Routing Protocol over the Low-Power Wireless Personal Area Network/IPv6 over IEEE 802.15.4 (6LoWPAN) is used for convenient communication in wireless network. With the development of Internet of Things (IoT),



numerous devices is required to connect to the Internet. At present, the existing address space of IPv4 is almost exhausted. In order to enable manufacturing equipment to meet the needs of future development, IPv6 address is chosen in our design. 6LoWPAN not only supports self-healing, robust and scalable mesh routing, but also uses AES-128 link layer security defining in IEEE 802.15.4, which can ensure the security of network. Other advantages of implementing 6LoWPAN are summarized in Figure 3.



**Figure 3: Advantages of 6LoWPAN**

There are four commonly used IoT access technologies, including Bluetooth, Wifi, 6LoWPAN, and Zigbee. Bluetooth is a low-power IoT technology. The main applications of this technology are Bluetooth headsets, Bluetooth mice, and Bluetooth keyboards. Bluetooth connections need to be paired, and usually the number of connections supported is less than ten. Therefore, Bluetooth is not a good choice for IoT in a plant with a large scale. WIFI is currently the wireless networking technology with the highest utilization rate. It is characterized by high transmission speed, but low security and low anti-interference. At present, many companies use WIFI to design smart homes, which is a simple and easy way to implement. But the disadvantage is that the number of supported nodes is small, and when it develops to a certain extent, it will inevitably cause obstacles. Zigbee is an IoT self-organizing network protocol launched by the Zigbee Alliance in 2001. It is a commercial agreement and requires the authorization of the Zigbee Alliance to use it. It is a self-organizing network structure, supports a large number of nodes, low power consumption. In many wireless projects, such as smart street lights,

industrial automation, etc. this technology has been widely used. But Internet is TCP/IP based Internet. Any other protocol needs to be converted to TCP/IP, which causes the implementation of the Zigbee gateway to be customized. And only the Zigbee gateway may have an IP address, and the zigbee node does not have an IP address. 6LoWPAN is an IPv6-based wireless ad hoc network protocol standard launched in 2006. The National Grid Corporation of the United States has formulated 6LoWPAN as the National Grid Standard Specification. 6LoWPAN has been widely used in some developed countries in Europe and America. Google and Samsung have adopted 6LoWPAN's UDP as a standard to design new smart home applications.

**Table 3: Comparison of wireless networking solutions**

Contents	6LoWPAN	Zigbee	Wifi	Bluetooth
Networking method	Automatic networking	Automatic networking	WIFI pairing	Bluetooth pairing
Security	High	High	Low	High
Number of Nodes	>200	>200	<20	<10
TCP/IP Property	IPv6	-	IPv4/v6	IPv4/v6
Power Consumption	low	Low	High	low
protocol Property	Public Protocol	Private Protocol	Public Protocol	Public Protocol

Because most public Internet is based on the IPv4 protocol, and 6LoWPAN is based on IPv6 protocol. Therefore, in order for the device to be able to access the Internet, protocol conversion is required. This function is implemented by the router. The 6LoWPAN router integrates the NAPT-PT protocol. This protocol will establish a NAT table and convert IPv6 addresses to IPv4 addresses to access Internet servers. When the Internet server returns data, it queries the NAT table, and if there is a record, it returns the data to the node recorded in the NAT table. The designed manufacturing facility topology network is shown in Figure 6 (presented in the last page).

## 4 Model Selection of Network Components

### 4.1 Switch

There are totally three kinds of switches: 1) **The core switch** connected directly to ISP, with 10GE/10GE down/up-Link rate. 2) **The work group switches** between the core switch and the work stations, with 1GE/10GE down/up-link rate. 3) **The server switches** supports the access to servers, with 10GE/10GE down/up-link rate.

**Table 4: The Core Switch**

Property	Description
Model	Cisco MS425-32
Number	2
Price	US\$15,892 * 2 = US\$31,658
Ports	32 × 10GE SFP+ port 2 × 40GE QSFP+ uplinks
Switching Capability	Up to 800Gbps switching capacity 160Gbps of flexible stacking Layer3 Warm spare redundancy (VRRP) OSPF Routing MAC forwarding entries, up to 512K DHCP Server, DHCP Relay 802.1X Authentication DHCP Snooping STP Enhancements IPv4 and IPv6 ACL
Cloud Management	Remote troubleshooting tools Manage ports from a GUI-based dashboard Per-port and per-client usage statistics Secure, user-scheduled firmware updates

**The core switch** is the root switch. Its detailed configuration and model is shown in Table 4. In our network design, two core switches are needed, 1 of which will become the redundancy switch, as shown in Figure 4. The switches have 10 Gbps down link and 10 Gbps up link. It uses 100Gbps Single Mode Fibre to connect with the ISP, and uses the STP-CAT7 cable to connect with the work-group switches and the server switches. To meet above conditions, we selected **CISCO MS425-32** as the core switch. It have 32×10GE down link ports, and 2×40GE up link ports. Besides, it offers good DHCP, addressing spacing and routing support, and supports both IPv4&IPv6 well for future network. The most important thing is that it have user-friendly GUI for staff to access, and programmable system, which is suitable for our customer: a network facility company which should has the ability to configure the network via GUI according to their demands.

**The work group switch** is the children switch for each department. We put three of them, one at administration building, one at Research and Design Centre, one at plants and foundry buildings, as shown in Figure 4. The work group

**Table 5: The Workgroup Switch**

Property	Description
Model	Cisco MS350-24X
Number	3
Price	US\$5,393 * 3 = US\$ 16,179
Ports	8 × MGig port 16 × 1Gbps port 4 × 10Gbps SFP+ uplinks
Switching Capability	Stack up to 8 units 160Gbps of physical stacking Layer3 Warm spare redundancy (VRRP) OSPF Routing MAC forwarding entries, up to 512K DHCP Server, DHCP Relay 802.1X Authentication DHCP Snooping STP Enhancements IPv4 and IPv6 ACL
Cloud Management	Remote troubleshooting tools Manage ports from a GUI-based dashboard Per-port and per-client usage statistics Secure, user-scheduled firmware updates

switches should have 1GE/10GE down/up link, and companies with a redundancy POE switch which supports the cameras. It will connected with the core switch with STP-CAT7 cables, and connect with the computers in the office with UTP-CAT6 cables. We select the **CISCO MS350-24X** switch, its details are shown in Table 5. It is in the same family with the core switch, thus can provide good compatibility. It owns 16 × 1GE down link ports, and 4 × 10 Gbps up link ports. As a switch with programmable GUI, its price is also reasonable. Last but important, its integrated GUI platform offers good VLAN division service, which is suitable for our need: multiple VLAN configuration.

**The server switch** is the children switch connected with server farms. For server farms, the switch should provide high throughput and high link rate. Besides, for intranet security, it should provide good VLAN support and VPN programmable ability. To meet this, we choose the **CISCO NEXUS 2332TQ 10GE** as the server switches. It has 16 × 10GE down link ports, and 4 × 40GE up link ports.

**Table 6: The Server Switch**

Property	Description
Model	Cisco Nexus 2332TQ 10GE Fabric Extender
Number	4
Price	US\$11,931 * 4 = US\$47724
Ports	16 × 10GE SFP+ ports 4 × 40GE QSFP+ uplinks RJ-45 connectors
Performance	FCoE support up to 30m with Category 6a and 7 cables Up to 160 Gbps of switching capacity in each direction (320 Gbps full duplex) Hardware forwarding at 960 Gbps or 1440 mpps 32-MB buffer
Dimensions	1.72 * 17.3 * 14.07 inch
Weight	15.00 lbs
Environment	Operating temperature: 32 to 131°F (0 to 55°C) Non-operating temperature: -40 to 158°F (-40 to 70°C) Humidity: 5 to 95 percent (noncondensing) Altitude: 0 to 10,000 ft. (0 to 3,000m)
Features	Layer 2 VLAN trunks IEEE 802.1Q VLAN encapsulation Advanced PortChannel hashing Jumbo frames on all ports (up to 9216 bytes) Pause frames (Priority Flow Control [PFC] and IEEE 802.3x) Private VLANs (promiscuous only on uplinks) Autonegotiation to 1000BASE-T full duplex on host interfaces


It offers plenty of VLAN controlling features, as shown in Table 6. It's connection with the core switch and servers are both using STP-CAT7 cables, as shown in Figure 9.

## 4.2 Cable

There are three types of cables used in our network: 1) UTP-SAT6 with 1Gbps link rate over 100m; 2) STP-SAT7 with 10Gbps link rate over 100m; 3) Backbone Single Mode Fibre with 100Gbps over 25-40km, as shown in Figure 4, each fibre

is annotated with different color.

**Table 7: Model selection of cable**

	Brand	Model Number	Data Transfer Rate	Cable Type	Price	Figure
CAT6	UGREEN	70680	1 Gigabits Per Second	Ethernet	\$15.99(50ft)	
CAT7	UGREEN	11266	10 Gigabits Per Second	Ethernet	\$18.99(50ft)	

For **UTP-SAT6** and **UTP-SAT7**, they should support 1G and 10G data rate. We choose the UGREEN cables, as shown in Table 8. All cables are well armoured to avoid lightening and rat bite.

**Table 8: Single Mode Fibre Model**

Property	Description
Model	QSFP-100G-ER4L-S
Feature	100GBASE QSFP Transceiver 25-40KM reach over SMF Duplex LC
Cable Distance	40km (with host FEC) 30km (without host FEC)
Power Consumption (W)	4.5
Price	$\text{US\$}4974 \times 2 = \text{US\$}9948$
Nominal Wavelength (nm)	1295, 1300, 1304, 1309
Core Size (Microns)	G.652

For **backbone Single Mode Fibre** between core switch and ISP, we choose the **CISCO QSFP-100G-ER4L-S**, as shown in Table 8. It supports *100Gbps* link rate, and can be as long as *40km* long. It is armoured with an insulating shielding to avoid lightening strike.

### 4.3 Wireless AP Router

For the wireless AP router is used in the facility, the elements that are needed for the wireless AP router are speed, capacity, and range. Compared with many other routers, NETGEAR Nighthawk AX12/12-Stream WiFi 6 Router (RAX120) has most benefits. Firstly, the AX WiFi delivers twelve WiFi spatial streams, which include four in the 2.4GHz band, and eight in the 5GHz band. The speed is up to  $1.2 + 4.8$  Gbps with 12-stream connectivity. Secondly, as the most important new feature correlated to 802.11ax, OFDMA supports sending up to eight multi-user MIMO transmissions at a time. Also, the 8-stream MU-MIMO<sup>‡</sup> enables up to four  $2 \times 2$  devices to stream content at the same time. This results in a significantly improved network capacity and benefits the performance of all legacy devices. Thirdly, Eight pre-optimized hidden antennas extend strong and reliable WiFi signals over larger area.

**Table 9: Wireless AP Router**

Property	Description
Model	NETGEAR Nighthawk AX12/12-Stream WiFi 6 Router (RAX120)
Price	\$799.00
Technology	802.11ax Dual-Band WiFi (AX6 2.4GHz AX: 4x4 (Tx/Rx) 1024 QAM 20/40MHz, up to 1.2Gbps 5GHz AX: 8x8 (Tx/Rx) 1024-QAM 20/40/80/160MHz, up to 4.8Gbps Backwards compatible with 802.11a/b/g/n/ac WiFi
Ethernet Ports	Five 10/100/1000 Mbps Gigabit Ethernet ports ports and one 5G/2.5G/1Gbps Multi-Gig port (configurable) 1 WAN and 4 LAN Dual Gigabit Ethernet Port Aggregation 5G/2.5G/1G Multi-Gig Ethernet LAN port
Performance	AX6000 WiFi
Range	Eight concealed antennas pre-optimized for best WiFi performance
Band	Simultaneous dual band 2.4 & 5GHz
Processor	AX optimized powerful 64-bit Quad-core 2.2GHz processor
Speed	1200+4800 Mbps with 12-stream connectivity 2.2GHz processor boosts wireless, wired and WAN-to-LAN performance 1024-QAM provides 25% increased data efficiency and faster speeds than 256-QAM router 8x8 MU-MIMO allows simultaneous streaming to multiple devices Multi-gig 5G/2.5G/1G Ethernet port delivers 5 times the wired speed of typical Gigabit Ethernet port
Capacity	OFDMA provides more WiFi for more devices by allowing efficient data transmission 8-stream MU-MIMO <sup>‡</sup> enables up to four 2x2 devices to stream content at the same time

Figure



### Router

The HP A-MSR30 Series are designed for use by enterprise branch and regional offices. A high-performance processor and modular design, combined with embedded applications for business productivity, enhanced security, and performance acceleration, enable users to meet their networking objectives today, and easily modify applications and services as their businesses evolve. Also, HP A-MSR30 series routers feature a comprehensive portfolio of interface and module options for reliable, scalable LAN and WAN communications, along with unparalleled security and convergence capabilities through embedded and integrated encryption and voice processing.

**Table 10: 6LoWPAN Router**

Property	Description
Model	HP A-MSR 30-20 DC MULTI SERVICE Router JF235A
Expansion Slot Type	MIM
Flash Memory	256 MB
Memory Technology	SDRAM
Network Technology	10/100/1000Base-T
Ports	2 10/100/1000 Ethernet (RJ-45)
Security Features	TACACS+; MAC Authentication; VPN firewall; DES; 3DES; AES; SSHv2; NAT; NAPT; RADIUS; Access Control List
Standard Memory	256 MB
Total Number of Ports	2

Figure



## 4.4 VPN Service



VPN can enable efficient work outside of the factory and make our network more secure. It ensures the encryption of your IP address and protocols. The primary job of a VPN is to hide IP address from ISP. It allows sending and receiving information online without the risk of anyone but employees and factory seeing it. It can also prevent factory from leaving traces, the encryption of cookies is especially important because it prevents third parties from gaining access to confidential information such as data, financial information and other content on websites. Since our routers come with built-in VPN servers, it can be used to build factory VPN server. As Client-to-Server VPN, employees can install and configure a VPN client



on the computer, so they can dial into the company network from their home office via the secure connection. This involves users not being connected to the internet via his own ISP, but establishing a direct connection through factory. This essentially shortens the tunnel phase of the VPN journey. Also, Some methods can be used to improve security. For example, two-factor authentication, to checks everyone who tries to log in, every employee might be prompted to enter a password, after which a code is sent to its mobile device. This makes it difficult for uninvited third parties to access your secure connection.

## 4.5 Surveillance System

**Table 11: Model selection of surveillance cameras**


Property	Description
Model Number	DS-2CD2347G1-L(U)
Max Resolution	2688 × 152
Main Stream	50Hz; 60Hz
Video Compression	Main stream H.265+/H.265/H.264+/H.264;
Video Bit Rate	32 Kbps to 16 Mbps
Power supply	12 VDC ± 25%, 5.5 mm coaxial power plug,PoE (802.3af, class 3)
Startup And Operating Conditions	Conditions:-30 °C to +60 °C (-22 °F to +140 °F), humidity 95% or less (non-condensing)
Price	\$425
Figure	
Model Number	DS-2CD2047G1-L
Max. Resolution	2560 × 1440
Main Stream	50Hz; 60Hz
Video Compression	Main stream: H.265+/H.265/H.264+/H.264;
Video Bit Rate	32 Kbps to 8 Mbps
Power supply	12 VDC ± 20%, PoE: 802.3af
Startup And Operating Conditions	Conditions:-30 °C to +60 °C (-22 °F to +140 °F)
Price	\$462
Figure	

The PoE switch should be compatible with the camera. TL-SG3226PE POE Switch has 24 10/100/1000Base-T RJ45 ports (supporting PoE power supply). For security, it supports IEEE 802.1Q VLAN, IPv6, port security, port monitoring,


port isolation, Web network management, CLI command line, SNMP. It supports IEEE 802.3af PoE standard, which can power the selected surveillance camera.

Although solid state drives (SSD) are more expensive than ordinary drives, with the development of technology, the update of the camera will have higher requirements for writing speed, so we choose SSD to store video for each camera to store video for a month. The parameter of the selected SSD is presented in the table below, which is selected according to the interface.

**Table 12: Model selection of PoE switch**


Property	Description
Brand	TP-Link
Product number	TL-SG3226PE
Gigabit RJ45 port	24
Gigabit SFP port	2
PoE port	24GE
PoE output power	370W
Whole machine power consumption	433W
PoE standard	IEEE 802.3at(PoE+), IEEE 802.3af
Operation conditions	Working temperature: 0°C-40°C Storage temperature: -40°C-70°C Working humidity: 10%-90% RH non-condensing Storage humidity: 5%-90% RH non-condensing
Figure	

**Table 13: Model selection of SSD**

Property	Description
Brand	Sabrent 4TB Rocket NVMe PCIe M.2 2280 Internal SSD High Performance Solid State Drive
Price	\$700
Digital Storage Capacity	4TB
Hardware Interface	PCI Express x4
Read Speed	3400 Megabytes Per Second
Write Speed	3000 Megabytes Per Second
Figure	


NVR is responsible for storing video. The selected NVR should be able to store surveillance video for at least one month. We choose the TL-NVR6432, which supports H.265. encoding, provides 4 SATA interfaces, each of which supports up to 10TB hard disk access. And it supports up to 8 million pixel ultra-high-definition network camera input, WEB remote preview/playback and mobile APP remote preview and recording.

**Table 14: Model selection of NVR**

Property	Description
Brand	TP-Link
Product number	TL-NVR6432
Number of Ways	32
Number of disks	4
Maximum access resolution	800W
Encoding	H.265/H.264
Output resolution	4K and below
Network Interface	1 10/100/1000Mbps adaptive RJ45 port
Operation conditions	Operating temperature:0°C-40°C Working humidity:10%-90%
Figure	

The display screen is placed in the monitoring room to display the real time video. We choose TL-DP1, which supports H.265 encoding method. It supports up to 4 HD IPC access and mobile APP remote viewing, monitoring screen preview at any time.

**Table 15: Model selection of display screen**


Property	Description
Brand	TP-Link
Product number	TL-DP1
Network video input	4 way
Network video access bandwidth	20Mbps
Video compression standard	H.264/H.265
Operation conditions	Operating temperature:0°C-40°C Working humidity:10%-90%
Figure	

## 4.6 Server

For tower we choose P920 which is a Lenovo Super Deep Learning/Top Two-way Full-size Workstation. The dual-processor workstation of ThinkStation P920 uses Intel's latest XeonCPU and design strstructure. For GPU, it use Nvidia's new Quadro RTX GPU with real-time ray tracing and AI enhanced workflow, which realize the real-time control of foundry, while meeting the office use. Also, It can connect a variety of I/O devices and support the top NVIDIA GV100 or RTX8000 professional graphics cards. Two onboard M.2 SSDs and four M.2 SSD array cards are supported, and the M.2 SSD array cards can be read at the same time, thus realizing the perfect compatibility between high-speed independent writing and security of hard disk, which enables future expansion of the sever. It can support RAID0/1/5/10 of M.2 SSD.

Meanwhile, the server backs up the data in the cloud drive every week, while the cloud storage is cleaned up every six months.

**Table 16: Model selection of Tower**

Property	Description
Brand	Lenovo
Product number	ThinkStation P920
Chipset	Intel C621
Processor	up to 28 cores, up to 3.6 GHz per CP
U CPU	ECC DDR4 2666MHz/2933MHz
Expansion slots	5 x PCIe x 16 4 x PCIe x 4 1 x PCI
Hard disk interface type	SATA/SSD/SAS
Storage	3.5" SATA HDD 7200 rpm up to 10 TB 2.5" SATA HDD up to 1.2 TB 2.5" SATA SSD up to 2 TB M.2 PCIe SSD up to 2 TB
Power supply	1400 W @ 92%
Operation conditions	Working temperature: 0°C-40°C Working humidity: 10%-90%
Figure	

## 5 Overall Topological Diagram

Figure 4 shows the overall topological network.

Figure 5 shows the network of plant and foundry.

Figure 6 shows the network of manufacturing facility.

Figure 7 shows the Research and Design Centre.

Figure 8 shows the Administration Building.

Figure 9 shows the server farm topological network.

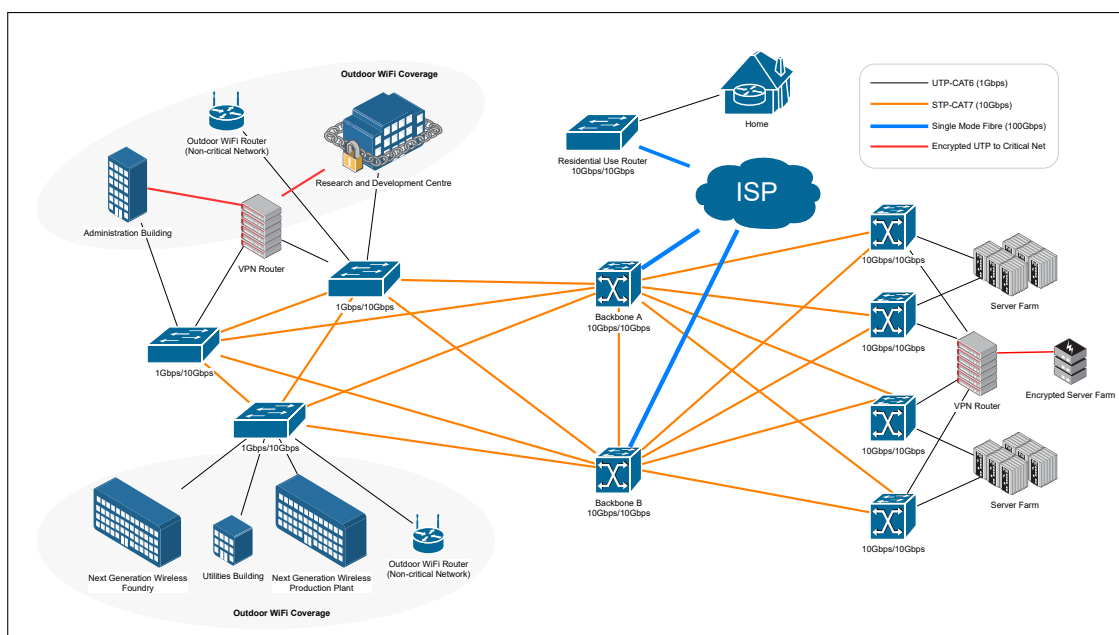


Figure 4: The Overall Topological Network

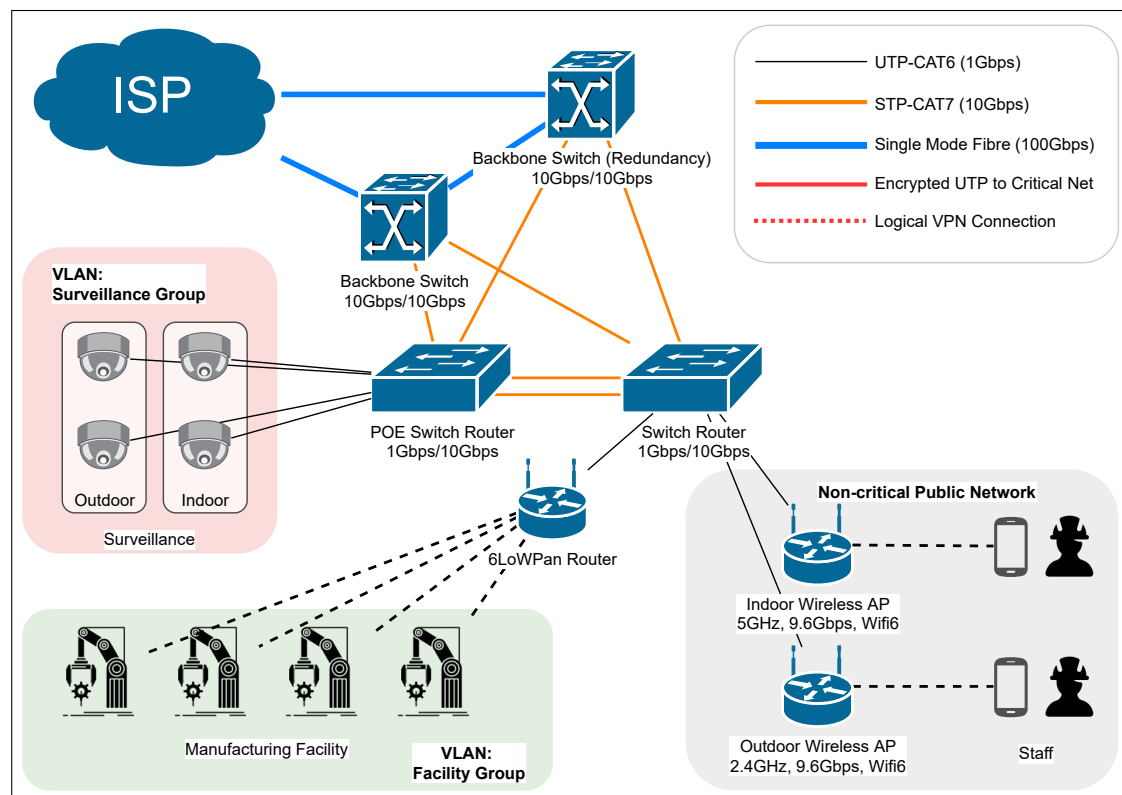


Figure 5: The Plant and Foundry

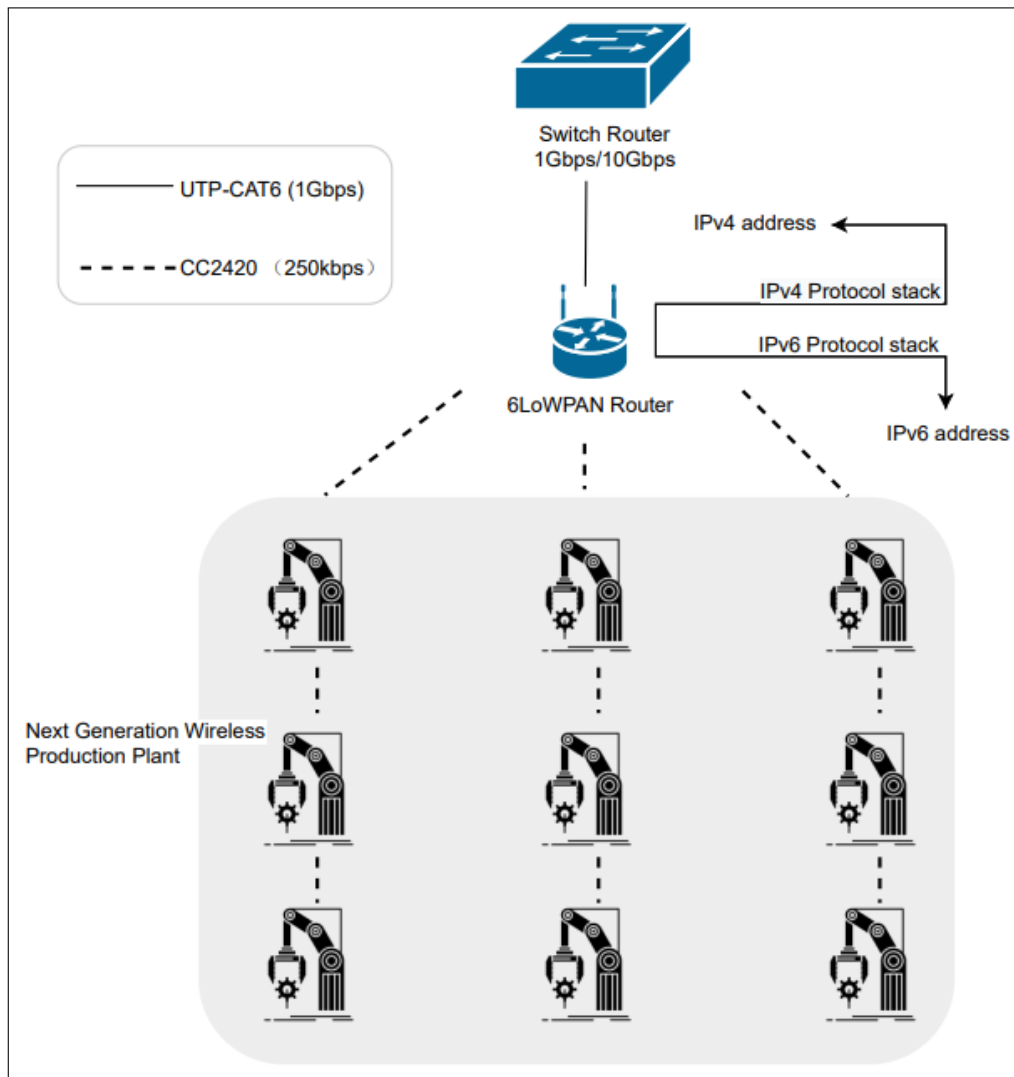


Figure 6: Manufacturing Facility Topology Network



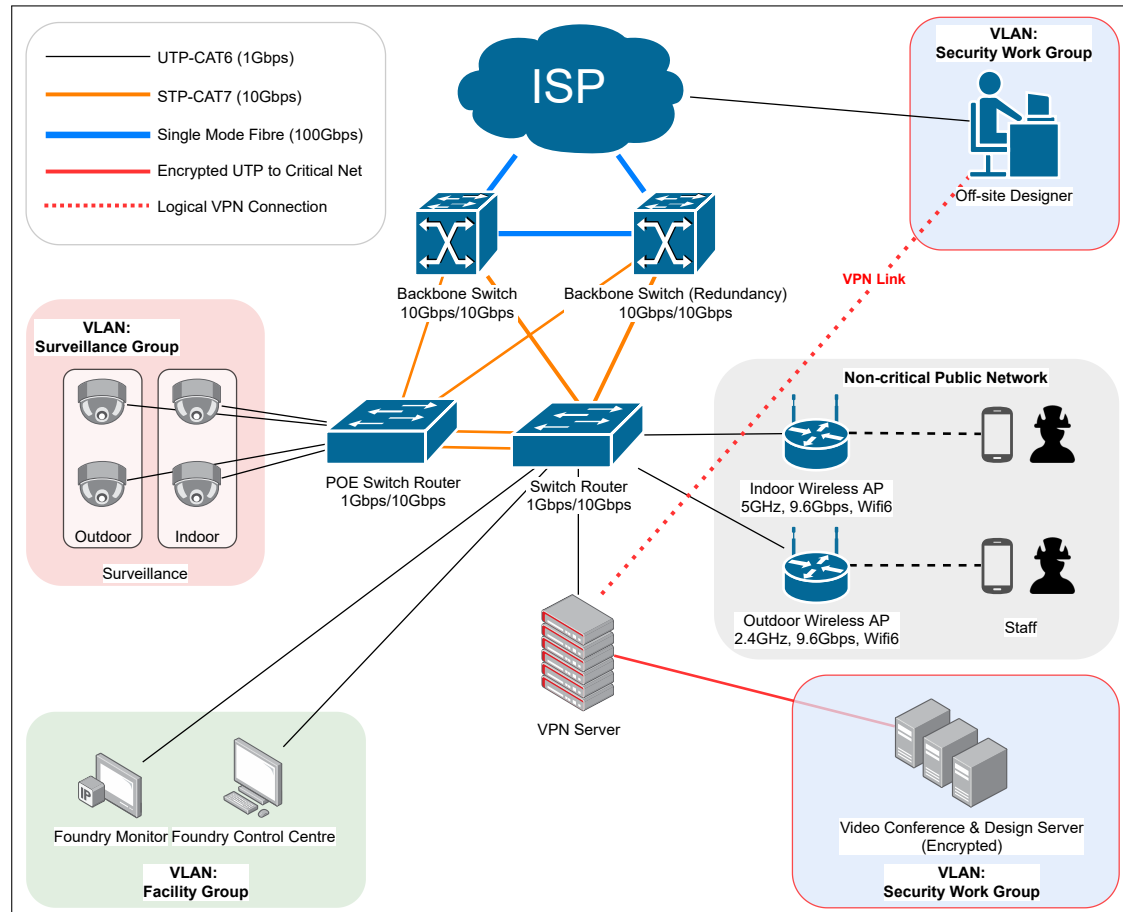


Figure 7: The Research and Design Centre

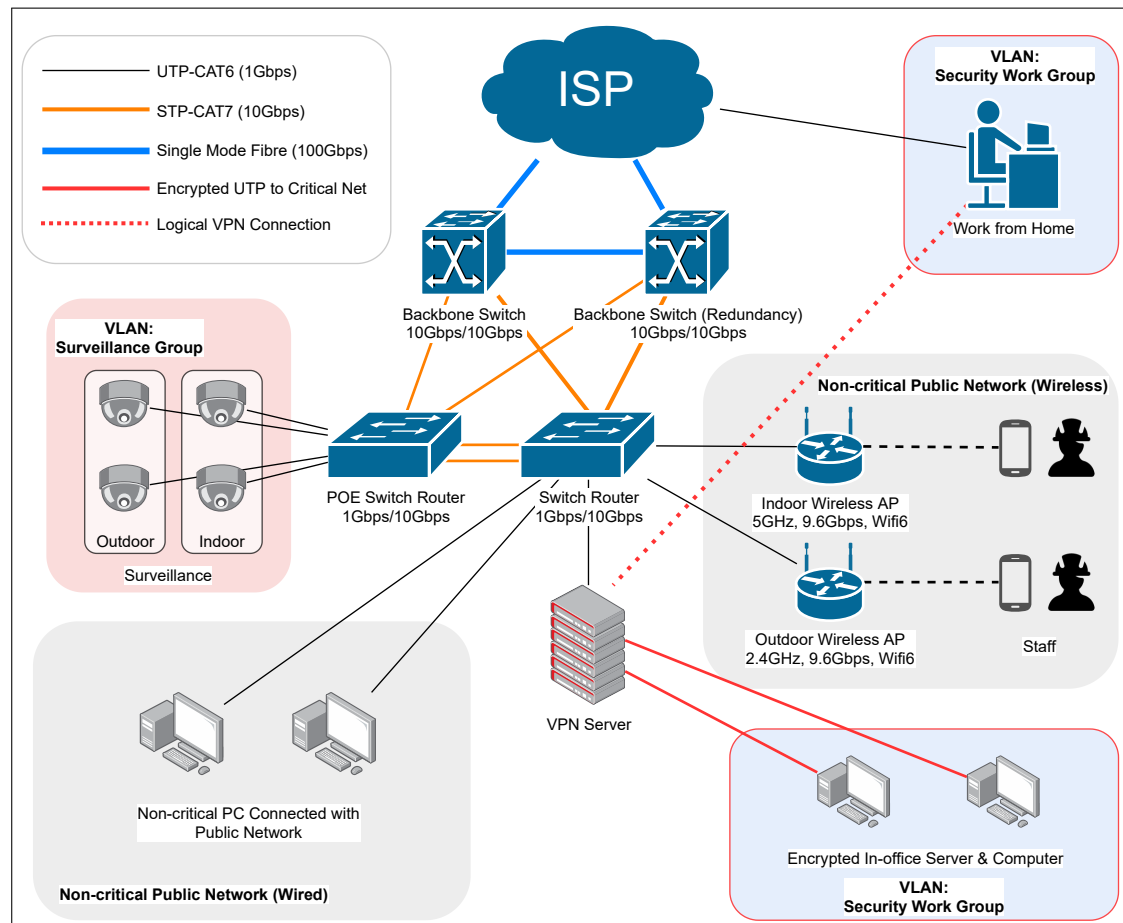


Figure 8: The Administration Building

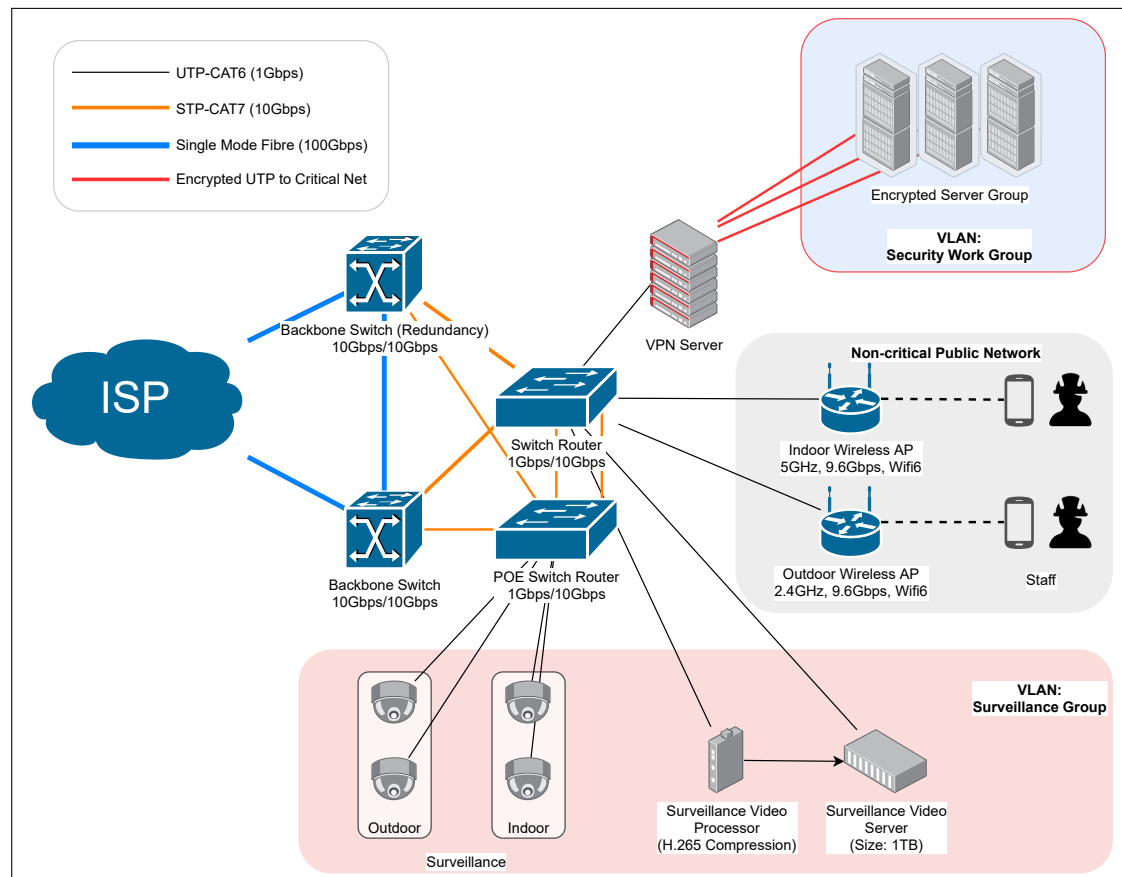


Figure 9: The Server Farm