**Network design and security analysis**

1. **Various measures taken in network design**

1. **action taken in the design of the network and rationality**

In this network demonstration, all the layout facilities used include switches, routers, personal desktop computers, wireless access points, wireless devices (smartphones and laptops), servers (data servers, web servers, DHCP servers), and twisted pair cables. It is worth noting that in building ROSS demonstrated two departments (senior managers and administrator), and in building TULIP demonstrated one department (research/development staff). A pair of twisted-pair cables are used to connect the two buildings. The purpose is that when one of them fails, the other can be used as a backup cable for emergency use. Therefore, the normal operation of the company will not be disturbed.

In the entire network architecture of a department, the switch plays an important role and a very large role, because it realizes the communication between all devices in the local area network. Similarly, in each department, the switch also connects the communication between the various devices in the department. A switch is connected to 5 desktop computers, three servers, and a wireless access point.

Regarding different wireless access points, they have their own different SSIDs and communication channels. The purpose is to distinguish between different wireless access points and avoid interference between signals. For example, the SSID of the wireless access points of senior managers is' r1', the channel is 6. The SSID of the administrator department is r2, and the channel is 7

1. **the devices selected and contingency for future expansion**

In the DHCP server, the wireless device is set to automatically allocate IP addresses starting from 192.168.1.128. Up to 129 wireless devices can be allocated to meet the needs of the company. Why start from 128? Considering the expansion of fixed IP in the future, some space is reserved some space is reserved.

1. **layout of floor dimension on network architecture**

Since the area of each floor is relatively large, in order to ensure the quality of network signal transmission and maximize the use of network resources, the switch must be located between each office and the open plan area.

1. **Method to avoid twisted-pair cable exceeding its maximum allowable length**

In network transmission, electronic signals will be affected by resistance and capacitance when they are transmitted in twisted-pair cables, resulting in attenuation and distortion of network signals. When the signal attenuation or distortion reaches a certain level, it will affect the effective and stable transmission of the signal. Extending the signal propagation distance, breaking the 100-meter limit, the shortcomings are also very clear, that is, the network signal will decrease. The type of twisted pair cable should be the newer Cat-8 twisted pair cabling which minimizes signal attenuation

**2.Security analysis and countermeasures of network design**

**1.Security countermeasures and network design flaws**

Network security level assessment

|  |
| --- |
| Security flaws |
| No Network Security System |
| Switch exposed out of sight |
| Too much range of WIFI signal cover |

Figure1

There are three discovered network settings security flaws described in figure 1

**2.Network security detection**

First, for enterprises, the most effective way to prevent network attacks is to monitor all traffic in the LAN in real-time. Although the previous solution has a relatively complete layout and also has NAT, as long as the internal network communicates with the IPS router,

It is possible for hackers to infer the real IP address through layer-by-layer network IP mapping, so the safety factor is low.

Next, although the optical fibre connection distance is very long, up to several kilometre, for the average enterprise, its input cost and layout are not ideal. Obviously, in order to solve the length limitation of the twisted pair, it is the best choice to add the transfer of the switch continuation signal to improve the previous network design. In order to prevent the device from being deemed damaged, a full range of monitoring must be added to the two buildings. Of course, the repeater plays an important role in enhancing signal transmission.

In addition, the range of sending and receiving signals of the wireless access points of each department is set to 110, which is exactly in the centre of the floor. This not only ensures that the company's internal personnel can use the network normally but also prevents some access points from being hacked.

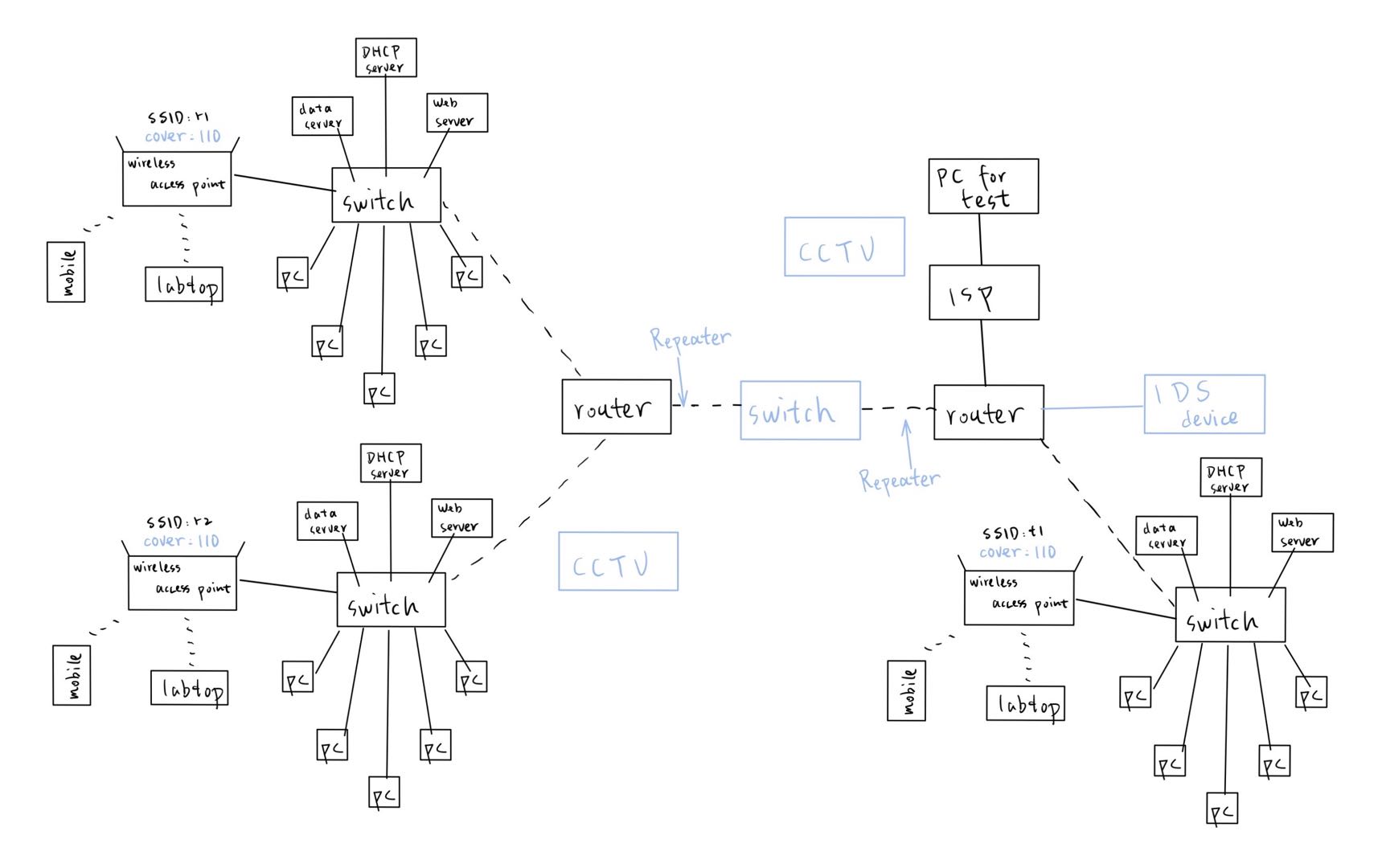
Risks detected. What needs attention is to prevent employees from leaking the password of the wireless access point, and to prevent hackers from defrauding the network password through social engineering to carry out network attacks.

**3.Analysis and summary of the reason for the change**

In the demonstration, the biggest threat to network security is the lack of a ‘security guard’ who can work 24 hours a day. Data is a company's greatest asset, and data leakage is undoubtedly the most fatal to the interests of the company and customers. For example, the fact that Facebook leaked users made it compensated 533 million, and it also allowed countless users' personal information to be used. It shows how important data is in the enterprise. In order to maximize the protection of data, a professional intrusion detection system is indispensable. It can monitor the company's internal network traffic in real-time for 24 hours. If there is an abnormal alarm, the company can make it the first time. Defensive measures to achieve the purpose of emergency data protection.

The second major network security threat is the switch between the two buildings. As mentioned above, the maximum length of the twisted pair cable is about 100 meters. Beyond this range, the weakening of electronic signals will excessively affect the quality of network transmission. With the switch in the middle, combined with the use of RP Repeater, the problem of insufficient maximum length of the twisted pair can be solved, but the switch needs to be exposed between the two buildings, and anyone has the opportunity to intercept the switch to achieve the purpose of intrusion. Therefore, the work of the switch needs to be carried out under a safe field of vision.

In addition, there is another security flaw, that is, the signal coverage of each wireless access point is set too wide, which will cause the signal to be exposed to a wider range in public areas. The method of hacking through the wireless access point is a common trick used by hackers. They have common methods to brute force the password, so in order to solve this problem, the wireless signal must be set to a range that can be used in only one department and WPA2 is added. Password and change the password regularly to increase the difficulty of cracking.

figure2