Network Design and Computer Management 120HP

EXAMENSARBETE

Creating network design proposals based on specific requirements

Jenny Larsson

Halmstad 2013

Network project

Creating network design proposals based on specific requirements

Network Design and Computer Management

2013

Author: Jenny Larsson

Supervisor: Malin Bornhager

Examiner: Nicolina Månsson

School of Information Science, Computer and Electrical Engineering
Halmstad University
PO Box 823, SE-301 18 HALMSTAD, Sweden

Univeristy Diploma Thesis
Report
School of Information Science, Computer and Electrical Engineering
Halmstad University

Preface

Making this project has been a journey filled with knowledge and experiences. It has been a great way to summarize the semester, and I wish to thank Malin Bornhager, Olga Torstensson and Nicolina Månson for all the work they've done in preparing me for the future.

Abstract

To have a well functioning and tailored network based on priorities and requirements is an important part of most modern companies. Network technicians that design these networks have very important tasks because many people rely on the solutions they chose to help them achieve many of their daily tasks.

This study focused on what you should think about when designing a network for a customer. Two simulated companies were created and modeled from real-world references. From their priorities and requirements a network proposal was created, suiting each company.

The companies were presented, along with an interview where the questions were used to gain the information necessary to reveal the clients needs. The answers were used as underlying motivation to what products and solutions were used to create the network proposals.

Different approaches on what is the most suitable for each company are discussed and hopefully these can be of use when designing networks in the future.

Contents

1 Introduction

A fully functional network is a key component in a modern company today. Different companies, from the smallest local one to the multinational group of companies, use different network solutions to make their daily businesses go around.
Web-pages, email, ip-telephony and wireless communications for remote users are essential tools required for more and more companies.

To create stable networks, on which the companies can rely on, professional network consultants are often hired. The network consultants' job is to design and implement a network infrastructure that is well suited to their client. The consultants always need to have in mind what the company stands for and know their technical requirements, but also know what budget he can use for creating solutions.

This project is built on the importance of a computer network for the modern company. I have been a consultant for two simulated companies, Plastic Fantastic and Cashflow. These two companies need help with setting up an entire new computer network. My job is to create the most suiting proposal to each company, based on their needs and requirements.

1.1 Project background

The reason for choosing to work with this subject is because I believe that it will complement my education in a good way. To have a functional computer network is extremely important and I wish to be able to answer the question about what a well built computer network truly is when asked in the future.
I have done several laborations throughout our courses at the university and have seen up close what big difference a well built network truly does for the user.

The purpose with the project is to see to the individual companies needs and based on this create a suiting network proposal for each company. The comparison that this project will result in will clearly state how different decisions are to be taken based on the type of company and their requirements. The right questions needs to be asked for getting answers that will aid you in designing a well built computer network.

After 2 years of network studies I have learned a lot and I will use all the knowledge I've gained as this project proceeds.

The network of Plastic Fantastic has been modeled based on warehouses I have previously worked in. It is to be considered a fairly realistic scenario and the information given in this report could help someone in the manufacturing business to set up a new network.
The network proposal for Cashflow is partly based on previous experiences of baking units, and partly from a case study about Deutsche Postbank. (See attachments) This case study is written in 2009 when the bank was replacing their old equipment and migrating from an ATM (Asynchronous Transfer Mode) network to an MPLS (Multi Protocol Label Switching) network.

At the time of the study, Deutsche Postbank was a much bigger company than what Cashflow is supposed to reassemble, but the network basic design and priorities are still very similar. This means that if Cashflow were to grow as a company and expand with new branches this network design would be able to grow with them and scale well.

The problem description is as followed:

I'm working as a it-consultant and have been in contact with two companies that are making establishments in a new city, and they require professional help with setting up their new computer network.

The project is to design and plan the networks according to the requirements and priorities of the customers, to further on compare the two different solutions and motivate why I believe that these will be the most suitable solutions for each company.

1.2 Objective

The two different companies I have chosen to simulate have different areas of expertise.
The first one is a smaller company that manufactures and sell plastic. A smaller company like this does not have the same requirements as a bigger company since their operation is more local, along with a smaller budget for their computer network.

The second company is a banking unit. This will be the bigger company with several divisions. Security is highly prioritized which also means that they have chosen to put more money into it. This gives me, as a consultant, the opportunity to put more effort into creating an environment that is as highly secure as possible.

Mainly, this project is defined by these three objectives:

- Knowing the clients priorities
- Define network requirements
- Compare network solutions

Based on these questions I will be able to develop suiting proposals for both companies. I will motivate the differences between the different proposals based on the knowledge I have gained from the different companies. Different client's needs and priorities are an important thing to know when you get out in real life and work for real companies, since different companies work in different ways.

2 Theoretical background

To better understand this report, some technical terms needs to be explained. The following chapter will hopefully give you a better insight in the networking world regarding networking designs, security and what WLAN and VOIP truly mean.

2.1 Network designs

A network is defined by having two or more computers connected. If there is more than two, you need a switch or router that connects these computers together.
When you start designing a network you always need to take into consideration a future growth of your network. A good approach is a hierarchical take, where the routers are on top, connected to switches that are further on connected to the end nodes. End nodes are the users of the network that is in the end of the line and has no additional equipment connected. The hierarchical approach will make it fairly simple to add more routers, switches or end nodes if desired.
When starting to look at the devices you wish to incorporate into your network, it’s a good idea to start with capacity. How many users is this network gonna be able to handle? Does the network need to be fast or redundant [1]? The capacity should be built on the answers of these questions. If there are many users on the network, it can be a good idea to divide them into groups based on the work they need to do. If the network needs to be redundant, more switches or routers may need to be purchased, and more connections need to be made.
If you design for a company that has more than one location, you need to consider how the different sites might differ and how to best connect between them. A bigger office might need more devices than a smaller one, to be able to keep the same standard.
The last thing you need to keep in mind while in the design phase is the budget. How much can we afford? The cost of buying used equipment might be beneficial, but does it conquer all the advantages new equipment can have? Cleaning up old settings, updating software and making sure everything works properly can be both tedious and expensive work.

2.2 Security

Security is a crucial part when designing a network. Like in your everyday life, you wouldn't want your personal information or assets getting into the wrong hands. Fortunately, there are many ways to secure a network.

Before getting into the technical part, you need to think about the human factor. Having a talk about security with your employees and explaining to them why the rules and regulations you have set up are so important is a great start. If people can understand the consequences of their actions they are more likely to try to follow your security standards and helping out keeping sensitive data a private matter. It is also important to keep a "need to know" basis; people shouldn't know, or have access to, more than they need.

When we think of it-security today we mostly think of things as firewalls and having strong passwords [2], but your security should always start with the physical part. Keep your devices in a secure space. If you have a company with many employees, it is a good idea to keep routers and switches in a locked room which only one or two people having access too. Another part to think about is redundancy. If one device goes down or a fire should start in your server room, it is always a good idea to have backups at a different location. Firstly, you need to make sure that these backups are up to date. If they do not have accurate information, they can not be properly used if a breakdown should occur. These backup devices should preferably already be connected into the network so the downtime will be at a minimal and prevent financial drawbacks for the company. The backup devices also need to be sufficient enough to support the network for a longer time since a major breakdown can be hard and time consuming to repair.

The next step is to think about how the computers are connected. If a person is using an end node, how far into the network can he go? Once again, the "need to know" basis should be implied. This can be implied with different security levels being set up by the administrator. An administrator should have access to the entire network, while an end user should only access his own workstation and nothing else.

VPN, Virtual Private Networks [3], is a secure way to connect from remote sites. It is a private tunnel that is set up between two devices so they can interact in a more secure way. It is not a physical tunnel, more a secure connection that encrypts the information being transferred so it is harder to intercept for anyone not having the encryption key. A good example of this is when a member of your staff wish to work from home. The staff member sets up a VPN tunnel that goes from his home computer and connects to the company network.

AAA, Authentication, Authorization and Accounting [4], is a model for access control. Authentication is who has access. To be authenticated you need some sort of username and password. This can be all from a normal username and password that you type in on your computer, to a finger print scanner that has a memory of you fingerprint and will grant you access when you press your finger on it. Authorization is what you have access too. Once you have entered the system you might only be allowed to perform certain tasks. If you have a higher security level you might be able to access all information while on a lower security level only a few things might be available for you. Accounting is logging of all you do. There can be logs on when you were authenticated, how many attempts you tried before getting access, what you authorized when you were logged on and for how long you stayed on. Logging like this is extremely important to have if a crime is committed. You can then see who accessed what and when; almost like a security tape.

2.3 WLAN and VOIP

2.3.1 WLAN

WLAN is the wireless option of a Local Area Network (LAN). This is an option that is becoming more and more popular since people like to move around with their devices and want to have internet access wherever they go.

A Wireless LAN is built using an Access Point – AP [5], that is somehow connected to the wired network. This AP uses radio waves [6] to broadcast a signal that can be picked up by any equipment that has a wireless network card, for example a laptop. To be able to identify the AP, your network administrator will set up an SSID [7]. An SSID is equal to a name of the AP, except for the fact that any AP can have multiple SSID's that all have their unique password. This can be useful if you wish to set up a guest network for example.

When you want to connect your laptop to an AP, you perform a search on computer to view available networks. The most likely scenario is that you will get a list with several different SSID's, and then you chose the one you wish to connect to. If this is a secure network, you will be asked to enter a password to gain access to the AP of your choice. If you are not required to enter a password when you want to access an AP, you need to consider the fact that if you don't have to enter a password – no one else will either. Any AP that is set up in a secure way will have a strong password that only the people who should access it will know of. Most devices will be able to remember the SSID and password of the AP that leads to your WLAN, so once you have entered the correct information you do not need to go thru this procedure again. The fact that you can easily connect to your network, and stay connected while moving around, is a clear advantage compared to wired solutions.

Although we are getting used to having internet access wherever we are, the range of an AP is something that needs to be considered. The signal from the radio waves will decrease the further away you get. You will have a stronger signal the closer you are to the AP and the less obstacles that stand in your way. Walls can, for example, strongly decrease your signal strength.

2.3.2 VOIP

Voice over IP – VOIP [8] is simply a way to make phone calls over the Internet. Skype [9], a program that allows you to make video calls over the internet for free, is a very good example of VOIP. The advantages of software that allows you to make calls over the internet are many. The first advantage is the ability to add a camera to your device and make video calls. Multiple people can join in on the conversation and a video conference between all of you can be set up. This is a great way to show and tell at the same time, instead of trying to explain how something looks or work.

The second advantage is that you do not need a phone line to make calls. Most of these software's are also free, so instead of paying for an expensive landline, or providing employees with their own cell phone, you can easily keep in contact as long as you both have internet access.
QoS, Quality of Service [10] is a way to measure quality in data traffic between two devices. Implementing QoS helps making sure that the quality of your call is consistent and tries to prevent any failure in your call.

3 The Clients

3.1 Plastic Fantastic

Plastic Fantastic, PF for short, is an expanding company on the market. Their area of expertise is to produce and redistribute plastic. They are a smaller company with only 75 employees, but since they are expanding they have decided that they are in need for a new computer network that can help them with their future growth.

PF has two locations, one where the manufacturing and storage take place, along with a newly built office for administration personnel. 50 people are working with the manufacturing of the plastic, and 25 people works at the administration office. Due to the company being such a small enterprise and doesn't hold too much valuable information, the security is not a crucial factor. All files that are sensitive, such as personnel information and company secrets are handled by an external source.

Since most of the people working at the administration office are salesmen it is important for them to have a redundant network, so clients can always get in contact with them and that the salesmen can help them fill out orders on the computer. Everyone working at this office has their own desktop computer that has an additional wireless network card so they can connect in multiple ways.

Another part of working with the administration is also maintaining the company's website, where they have several pictures and movies about their products. For this, PF has their own web server.

To avoid expensive cabling when creating a redundant network, the administration office would also like to have a wireless connection.

PF has a budget at approximately 150 000 SEK, for their new network.

3.2 Cashflow

The company named Cashflow is a big banking firm. It runs at 20 different sites and has about 1000 employees distributed. The main office employs 100 people and is the largest of the sites. 17 of the sites employ 50 people while the two smaller sites hold 25 employees each. The main office will further on be called CF 100. The medium sized offices will be referred to as CF 50, and we will assume in the report that all of the offices look the same. CF 25 is the two smaller offices, located abroad. Both of these offices look alike.

Although the company is multinational, it's only the two smaller sites that are located abroad from the main site. Their locations are in neighboring countries where the bank also has numeral clients.

The bank holds centralized login servers for all of the banks staff members at the main site. The servers also hold all the crucial data of the clients that the bank has. Full backups are taken twice a week and differential backups are taken twice a day in between. The backups are not stored locally.

The manager at the bank was very clear when he stated the needs of the network infrastructure of the company - the redundancy to the servers is a crucial component for the employees. If the link to the server goes down it can prevent the staff from doing their job, which in the end will result in a bad image and large costs for the company.

In addition to the servers being reachable at all times, it will also have to be very secure environment, since the servers store all of the banks most valued data; their clients accounts and records. If the data in some way is threatened, they would prefer the servers being cut off from communication, rather than breached by an attack. The damage of a simple communication block would still be small in comparison with the scandal that can occur if someone was able to withdraw sensible data from the banks servers.
The bank is only interested in getting the best possible solution and is ready to spend big money to get it. Of course they do not wish to waste money, so all decisions need to be clearly motivated.

4 Implementation

To aid me in choosing the most appropriate equipment I need a clear definition from the companies about their operation and requirements. To be able to create the most suiting proposal the following questions were formulated;

- What type of company is it?

Different companies will have different obstacles; a grocery store does not work in the same way as an airport does.

- How many offices do they have?

More offices will require more equipment.

- How many employees do they have?

More employees are equal to a higher security risk. It is also a higher cost if they all will be connected to the network regarding equipment.

- What do they require regarding security and redundancy?

Security and redundancy can both be expensive, but sometimes it's worth it.

- Connections from home or from the field? Virtual Private Networks – VPN?

People working from home or from the field stand for a higher security risk and this needs to be considered when designing the network.

- Will centralized logins be required?
  Authentication, Authorization, Accounting - AAA?

To gain control over who access what inside the network.

- What budget do they have?

Different solutions will have different price tags.

- Are wireless connections required?

If people are moving around a lot and portable computers are used, wireless connections are to prefer.

- Is Voice over IP telephony - VOIP required?

VOIP is a good option if the company makes a lot of calls.

- How do the premises look like?

Physical location is a critical question when designing a network since you can't assume that the location or locations will look and work in a certain way.

Each company will receive a small report that contains the following information;

- The first side with the questions they were given and their answers. This is what the proposal is built on and I need to be able to refer back to these answers any time during the process.
- The proposal in words, where I have explained why I believe that this is the best solution for the company.
- A shopping list, where all the devices the company is advised to buy are stated, along with where to buy them from and how much the individual and total cost will be.
- Information regarding any protocols or configurations that the company is to consider.
- A map over the premises.
- The physical topology; the map with all the new devices drawn on to it.
- A logical topology showing how the devices will be connected.

4.1 Plastic Fantastic Report

4.1.1 PF Questions/Answers

PF is a smaller Plastic manufacturing company. I have been in contact with their CEO and he gave me the following information.

- What type of company is it?

-It's a small company that manufacture and sell plastic.

- How many offices do you have?

- One office and one warehouse, both located in the same city

- How many employees do you have?

- 75 employees. 50 working at the warehouse, 25 at the administration office.

- What do you require regarding security and redundancy?

- Security is not a big concern, however redundancy is. Keeping the network up at all times is a crucial component.

- Connections from home or from the field? VPN?

- Connections from remote locations should be allowed. VPN preferred.

- Will centralized logins be required? AAA?

- No

- What budget do you have?

- 150 000 SEK

- Are wireless connections required?

-Wireless internet connections are to be preferred.

- Is VOIP required?
  - No

4.1.2 PF Proposal

The first thing that was decided was how many devices of different kinds that should be purchased. In the warehouse (Appendix A, Figure 4.1.1) it seemed to be sufficient with only a wireless router at the office. A wireless router was chosen since a router would support VPN, for secure connections between the companies' two locations, and at the same time there would be no need to worry about extensive cabling at the warehouse with a wireless option. Wireless is also great for a company that is in an expanding phase, since a wireless range can cover a large distance and the signal can easily be enhanced to cover a larger area with access points or repeaters.

The administration office (Appendix A, Figure 4.1.2) will firstly hold the server that the company uses for their website. A wireless router will be purchased to this office as well, since the office has both desktop and laptop computers. The wireless router will be located in such a place that it will cover the whole office without loosing signal. If the office area should become larger with time the solution with access points or repeaters would work well even in this environment. To keep the network redundant, an ordinary router will also be purchased that can work as a backup if the primary connection would fail. To be able to reach all the desktop computers a switch with 48 ports is purchased. The cable to connect all this, further explained in section 3.1.4, is a category 6, low smoke zero halogen - LSZH, unshielded twisted pair - UTP, installation cable. Since the cable come in a packet that contains a 305 m long cable I would get 2 of these to be able to cover the whole office. 2 crossover cables will also purchased for the connection between the server and both routers. To keep the network devices secure a storage locker will be purchased. A locker like this will prevent anyone who doesn't have access to the devices to tamper with them. Only the network administrator should have access to this locker. Along with the locker, 2 external fans should be installed to keep the devices cool and prevent them from overheating.

4.1.3 PF Shopping list

Following content should be purchased from attached websites to get the estimated price.

1. Cisco Catalyst 2960 Switch – 4 599 kr [11]
2. Cisco 881W Integrated services wireless router – 5 192 kr x2 [12]
3. Cisco 887V Integrated Service Router – 5 554 kr [13]
4. IBM System x3550 Server – 13 884 kr [14]
5. 19 ” TOTEN Rack cabinet – 1 649 kr [15]
6. 2 Fans for rack cabinet – 349 kr [16]
7. White Cable rolls, 305 m – 1 340 kr x2 [17]
8. Crossover cables – 19 kr x2 [18]

Total cost will be: 39 137 kr

4.1.4 PF Protocols and configurations

Appendix A, figures 4.1.3 & 4.1.4 provides an image of how it could look if all the appliances in section 4.1.3 are purchased and applied, and Appendix A, figure 4.1.5 gives a good view on how the network will work if this proposal is applied.

The cloud in Appendix A, figure 4.1.5 represents that VPN is supported and can be installed between the office at the warehouse and the administration office.

All the computers have both a regular and a wireless network card. If anything happens to the wired network the wireless will kick in. This covers everything from faulty cables to device failure.

4.2 Cashflow Report

4.2.1 CF Questions/Answers

Cashflow is a large banking firm. I have received following information from the company's CEO.

- What type of company is it?

-It's a large banking firm.

- How many offices do you have?

- 1 main office, referred to CF 100, 17 medium sized offices, named CF 50 and 2 smaller offices, CF 25, located abroad.

- How many employees do you have?

- 1000, where 100 of these are working at the main office, 850 distributed among the medium sized offices and 50 working abroad.

- What do you require regarding security and redundancy?

- Both redundancy and security are highly prioritized and should play a crucial role in the building of the network.

- Connections from home or from the field? VPN?

- Connections from remote offices require VPN.

- Will centralized logins be required? AAA?

- Centralized logins will be required and AAA should be applied to make the system as secure as possible.

- What budget do you have?

- Infinite

- Are wireless connections required?

- No.

- Is VOIP required?
  - VOIP should be able to function properly in all the offices.

4.2.2 CF Proposal

The first thing that was done was to make sure that all the offices would be able to connect with each other. This is a crucial component in order for the company to work properly. All the routers that are being purchased support VPN and AAA, so the offices can communicate in a safe way. VOIP is also supported, so the people at the smaller offices in a quick and easy way can connect with the personnel working at the main office.

4.2.2.1 CF 100

The CF100 office, shown in Appendix B, figure 4.2.1 & 4.2.2, is located in a building with two floors. The tech room with servers, routers and distribution switches are located on the first floor, Appendix B, figure 4.2.1, along with the access switches for the first floor. On the second floor there's a smaller cabinet containing the access switches for the second floor.

The office will use 2 powerful ASR1006 routers with 20 Gbps processors. These routers will be purchased with the VPN bundle. In addition to this, a firewall license will be purchased to allow the routers to add features otherwise provided by a firewall device. Routers like this save the company energy and money by implementing services for several devices into one single physical device. This will lower the power consumption, rack space required and cooling needed. Each of the routers has their own ISP connection, to keep the network redundant.

All the switches that will be purchased for this office are layer 3 switches, because of their support of Cisco Express Forwarding – CEF.
The distribution switches that will be used are 2 Nexus 2248TP switches.
They will be purchased because of the need for redundancy between the routers and data centre and to divide all the data that needs to be processed for maintaining the high speed throughout the network. Each switch support 40 Gbps routed traffic, so even if one switch should go down the other one can still support all the traffic on both routers. If CEF is enabled it will be able to switch up to 176 Gbps.

The access layer switch sets are identical for the two floors. They consist of one Catalyst WS-C3560X-48P-L and one Catalyst WS-C3560X-24P-L. These were chosen because of their support for Power over Ethernet - PoE and Quality of Service – QoS, and are both adequate for VoIP. The reason for choosing layer 3 switches instead of layer 2 is simply because of the CEF feature that will help make the host - server connection faster.

The cabinet on the bottom floor will be a Toten 19" locker with 42U rack that will leave much space for more servers or devices if needed in the future. The cabinet is lockable from all sides, adding additional security. The rack on the second floor will be a Toten wall mounted 6U Rack with a lockable door. Extra ventilation will be purchased to keep the devices cool.

The cabling between the distribution switches to the database and web server will be a 10 Gbps link while all other cables support up to 1 Gbps. Straight Cat.6 patch cables will be used everywhere except for the connection between the switches, which will have crossover cables,

4.2.2.2 CF 50

The medium sized offices, shown in Appendix B, figure 4.2.3, have no data centre and therefore require much less bandwidth then the main office. Still the office needs to obtain a lot of information every day since nothing is locally stored. This means that the company still must make sure that the network is well prepared for peak hours when all employees are using the network at the same time. The suggestion made for routing is an ASR 1002 router. It only has half the routing capacity of the bigger ASR 1006, which is stationed in the main office, but still operates at a very high routing capacity of 10 Gbps. Since these smaller offices need to be online during work hours, two identical routers should be purchased for redundancy. Each router should have its own connection to the ISP.

Since there’s no data-centre to protect, the distribution layer is not needed in this site which means that the access switches are connected directly to the routers. The same Catalyst switches that were chosen as access switches in CF100 are chosen here as well, having the same model makes configuration easier and also creates an opportunity for the company to stock reserve parts for these models.

4.2.2.3 CF 25

The offices located abroad are displayed in Appendix B, figure 4.2.4. With such a small office, the need for two routers for redundancy stands against the already extremely high performance of the device, buying one extra router for redundancy does not seem as the logical choice when the office barely use any of the performance of only one router. The company could buy a smaller model router with less performance and buy two of these instead but in order for them to buy a smaller router they would have to go to another series of models. Switching to another model has several disadvantages; the networking staff has to learn the new model and it will be harder for them to implement it, it would work and have different configurations than the other routers in the network and it would take a lot of time to work with it, and as we all know – time is money. If the network were to increase it is also an advantage of having devices that works the same.

The advice is to only purchase one router and then make sure that there is a service contract set up with technical experts in the near area that will have 24-hour service if a problem should arise since a network downtime can cause the company to lose clients and their trustworthiness.

The switch to be purchased is the same used in CF 50, a Catalyst WS-C3560X-48P-L. A cabinet, TOTEN 19”, along with 2 extra fans will be obtained to keep the systems safe and cool. Straight Cat.6 patch cables will be used to connect the devices with each other.

4.2.3 CF Shopping list

4.2.3.1 CF100

Following content should be purchased from attached websites to get the estimated price. Appendix B, figures 4.2.5 & 4.2.6 will further on show how these things are planned to be implemented into the office environment.

1. ASR1006 Router, 20 Gbps, VPN Bundle – 319 657 kr x2 [19]
2. Firewall licenses – 35 127 kr x2 [20]
3. Nexus 2248TP Switch – 32 599 kr x2 [21]
4. Catalyst WS-C3560X-48P-L Switch - 25 489 kr x2 [22]
5. Catalyst WS-C3560X-24P-L Switch - 14 086 kr x2 [23]
6. TOTEN 19" Floor cabinet 42U 600X1000 - 7 499 kr [24]
7. 19” TOTEN Rack cabinet – 1 649 kr [25]
8. Fans for rack cabinet – 349 kr x2 [26]
9. Patch cable STP Cat6 PIMF, 1000 Mbps. 5m - 63 kr x102 [27]
10. Patch cable STP Cat 6 10m -129 kr x10 [28]
11. Patch cable S/FTP Cat 7 PIMF, 10 Gbps. 1m – 39 kr x8 [29]
12. Patch cable STP Cat6 PIMF, 1000 Mbps. 1m – 23 kr x4 [30]
13. Crossover Patch cable UTP Cat6 1m – 15 kr x6 [31]
14. Crossover Patch cable UTP Cat6 5m – 39 kr x6 [32]
15. Cat6 LSZG, UTP, 305m packs, Order no. 06-8219 – 1 340 kr x15 [33]

Total cost for CF100 will be: 892 306 kr

4.2.3.2 CF 50 x 17

Following content should be purchased from attached websites to get the estimated price. Appendix B, figure 4.2.7 will further on show how these things are planned to be implemented into the office environment.

1. ASR1002 Router, 5Gbps, VPN bundle – 181 107 kr x2 [34]
2. Firewall licenses – 36 221 kr x2 [35]
3. Catalyst WS-C3560X-48P-L Switch - 25 489 kr x2 [36]
4. Catalyst WS-C3560X-24P-L Switch - 14 086 kr x2 [37]
5. 19” TOTEN Rack cabinet – 1 649 kr [38]
6. 2 Fans for rack cabinet – 349 kr [39]
7. Patch cable STP Cat6 PIMF, 1000 Mbps. 1m – 23 kr x4 [40]
8. Patch cable STP Cat6 PIMF, 1000 Mbps. 5m - 63 kr x50 [41]
9. Patch cable STP Cat6 PIMF, 1000 Mbps. 10m – 103 kr x4 [42]
10. Patch cable S/FTP Cat 7 PIMF, 10 Gbps. 0,5 m – 28 kr x4 [43]
11. Cat6 LSZG, UTP, 305m packs, Order no. 06-8219 – 1340 kr x5 [44]

Total cost for one CF 50 office will be: 526 207 kr

Total cost for all 17 CF 50 offices will be: 8 946 590 kr

4.2.3.3 CF 25 x2

Following content should be purchased from attached websites to get the estimated price. Appendix B, figure 4.2.8 will further on show how these things are planned to be implemented into the office environment.

1. ASR1002 Router, 5Gbps, VPN bundle – 181 107 kr [45]
2. Firewall license – 36 221 kr [46]
3. Catalyst WS-C3560X-48P-L Switch - 25 489 kr [47]
4. 19” TOTEN Rack cabinet – 1 649 kr [48]
5. 2 Fans for rack cabinet – 349 kr [49]
6. Patch cable STP Cat6 PIMF, 1000 Mbps, 1m - 23 kr x 4 [50]
7. Patch cable STP Cat6 PIMF, 1000 Mbps, 5m - 63 kr x 27 [51]
8. Patch cable STP Cat6 PIMF, 1000 Mbps, 10 m - 103 kr x 4 [52]
9. Patch cable S/FTP Cat 7 PIMF, 10 Gbps, 0,5 m - 28 kr [53]
10. Cat6 LSZG, UTP, 305m packs, Order no. 06-8219 – 1 340 kr x 3[54]

Total cost for one CF 25 office will be: 251 068 kr

Total cost for both CF 25 offices will be: 502 136 kr

Total cost for all offices will be: 10 341 032 kr

4.2.4 CF Protocols and configurations

Appendix B, figures 4.2.9, 4.2.10, 4.2.11 & 4.2.12, are representations of how the network will be connected. Figure 4.2.9 displays that the network also has an external link, which can be a security threat, but since AAA is supported it is suggested that it’s implemented to make the network more secure. Another security feature that is supported is VPN. VPN tunnels should be set up between the companies different locations so that information between different sites is transferred in a secure environment.

To get the redundancy working well without reducing network capacity, GLBP [55]Gateway load balancing protocol) will be used on all routers in the network and also on the distribution switches in the CF100 network. This makes sure that not only the redundancy is in place, but the devices are actually working together to maintain a higher throughput.

The ip addresses of the network will all be statically assigned since the hosts are all stationary and will not be moved, added or deleted unless a technician is involved. This is to maintain the high security standard, to make the network easier to document and if a problem arises and you have an ip address to track it will be very simple to isolate the problem. All access ports on the switches in the network will be set to work only with the single mac address of the host connected to it. Setting the switch ports to access mode is also recommended since it prevents rouge network equipment to interfere with the network. All unused ports will be shutdown.

IP telephony is supported, and can easily be implemented by external consultants.

5 Analysis

5.1 Analysis of PF report

The big concern with PF was the budget. PF is a smaller company and had to have a network that would be fully functional, but also in the right price range. 150 000 kr is not much if you intend to get all new devices, but I chose to discard the option with used devices since this is a company that is growing and getting all new equipment seemed to be a more long lasting solution.
In the end the budget never proved to be much of a problem since the bandwidth requirements didn’t exceed 100 Mbps which allowed us to choose a smaller router model that was substantially cheaper than the other options with higher processing capacity.

Since this is a company that both manufacture and sell, the connection with the outside world is crucial for the company to go around. The importance of being able to reach customers, and for customers to reach them, made redundancy play a big part in their new network. This caused me to go for the two router solution with both routers having their own connection to the ISP for full redundancy.

The advantages with the 880 series routers were many. IDS (Intrusion Detection System), a content filter to help protect the network, support for IPSec (IP Secure), STP (Spanning Tree Protocol), QoS (Quality of Service) and IPv6 (IP version 6).

In the warehouse I choose to stay with the same wireless router model as used in the office environment. The simplicity of working with similar devices contributed to making this decision along with the security perspective where the warehouse and office would be directly connected and this model support multiple security features and offers a secure connection.

5.2 Analysis of CF report

CF was the bigger company that had multiple locations and security as its main concerns. The company had no budget, which allowed me to create a very advanced and secure network.

Both security and redundancy were two main issues that needed to be addressed. Bandwidth and throughput are also key components, since this is a big banking unit and things need to working and they need to work fast in order for the employees to be able to do their job properly.

Since the company stated that they would like VOIP to be implemented all the devices in the network will support both VOIP and QoS. VPN was also one of the things the company needed to have, so all devices need to have IPSec to set up secure GRE (Generic Routing Encapsulation) tunnels.

Backups are a crucial component to consider when dealing with networks. It is the only way you can make sure that your information doesn't get lost and saving your backups at a remote location is always a good option. CF has an external place where their backups are stored. Full backups are taken twice a week and differential backups are taken twice a day in between. A suggestion for the company is to allow the web server at the remote location to take over the DNS connection if the network should go down. This way the customers can still get hold of their account information while the ordinary network is being fixed.

Since the network is partly modeled on Deutsche Postbanks network the routers chosen are mainly the same as they use in the study; routers from the ASR1000 series. ASR 1004 Routers are not used, as in the study, simply because Cashflows medium and small sized branches do not need such large routers. Instead, the ASR1002 router is used in the same way as Deutsche Postbank uses their ASR1002 routers with their smaller branches. For redundancy reasons, all routers have their own connection to the ISP.

In the study of Deutsche Postbank they mention that the bank uses Cisco configuration engine. This creates an opportunity to push all future software and configurations out centrally through this solution making management processes much faster. This would be a very good investment to make for Cashflow if the company expands further.

6 Conclusion

This thesis has been about the design phase of a network. I have worked with two very different companies and therefore received two very different solutions.

The smaller company called Plastic Fantastic, PF, had a limited budget and a smaller office building which required careful planning with regards to size, location and prize on the devices. I believe the solution I came up with would work well for this company. However, other small companies can have other limitations and everything needs to be carefully reviewed before starting to purchase equipment. It is always a struggle with limitations, but a good way to start is to get as much information about the company as you can, and also pay a visit to the perimeters to see what limitation and opportunities that exist. Seeing something with your own eyes is worth way more than just getting a blueprint or map over the place.
One thing that has not been considered in this thesis is the purchase of used equipment. For a company with a strict budget, this might be a useful thing to take into consideration. The downside of used equipment, such as previous configurations and no guarantee from the seller, made me not consider it in this case. The fact that the budget was enough to buy efficient equipment anyways was also a contributing argument.

The bigger company named Cash Flow, CF, had security as its biggest priority. Since there was no budget this gave me an opportunity to search for the top notch security features existing on the market today. The struggle was to find devices that would support all the security features, and also make sure the network was redundant enough. In the end, the cost for having these security features became quite extensive, although security in itself cannot have a price when sensitive data is handled. If a security breach was to occur, or redundancy would fail, this would cost this bank much more than just money.

The goal with this thesis was to show that different priorities can give different solutions. There are a lot of things to take into consideration when planning a network and it’s not done over night, but taking the time and money to plan a network accordingly will most likely result in something that is sustainable, cost efficient and has a low down time and in the long run, it’s worth it.

7 References

1. http://www.windowsnetworking.com/articles-tutorials/netgeneral/Importance-Network-Redundancy.html
   Retrieved Dec 14 2013

2. http://www.microsoft.com/security/online-privacy/passwords-create.aspx
   Retrieved Dec 14 2013

3. IT Essentials, PC Hardware and Software Companion Guide, 4th Edition, Cisco Press, page 334, ISBN-10:158713263 ,ISNB-13:9781587132636

4. http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfaaa.html
   Retrieved Sep 25 2013

5. Certified Wireless Network Administrator, official study guide, Planet 3 Wireless, Inc., page 72, ISBN: 0-9716057-2-6

6. Certified Wireless Network Administrator, official study guide, Planet 3 Wireless, Inc., page 18, ISBN: 0-9716057-2-6

7. Certified Wireless Network Administrator, official study guide, Planet 3 Wireless, Inc., page 169, ISBN: 0-9716057-2-6

8. Voice over IP Fundamentals,2nd Edition Jonathan Davidson, James Peters, Manoj Bhatia, Satish Kalidindi, Sudipto Mukherjee, Cisco Press, ISBN-10: 1-58705-257-1, ISBN-13: 978-1-58705-257-6

9. http://www.skype.com/en/
   Retrieved Dec 14 2013

10. http://www.cisco.com/en/US/products/ps6558/products_ios_technology_home.html
    Retrieved Sep 25 2013

11. http://www.dustin.se/product/5010191579/cisco-catalyst-2960-48tt-s-switch-48-10-100/#intcmp=searchProvider_dacsa
    Retrieved Nov 26 2012

12. http://declan.se/products/Natverk-kommunikation/Router-tradlost/Cisco/Cisco-881W-Integrated-Services-Router-Tradlos-ro?searchtrack=Unknown&prodid=11248
    Retrieved Dec 8 2012

13. http://declan.se/products/Natverk-kommunikation/Router/Cisco/Cisco-887V-Integrated-Services-Router-Router-I?prodid=20981&info=2#.UMTKRGfGKaR
    Retrieved Dec 9 2012

14. http://www.misco.se/Product/Product.aspx?P_ItemId=5586485&hbx_CMP=AFC-05&cm_mmc_o=4blgBCjCVybgw2BF5zyblBECjCzkkCjC5yblXzLf
Retrieved Dec 3 2012

15. http://www.dustin.se/product/5010206992/toten-19-vaggskap-6u-600x600-glasdorr-svart/#intcmp=searchProvider_dacsa
Retrieved 3 Dec 2012

16. http://www.dustin.se/product/5010107222/flaktpaket-med-2-flaktar-for-600x600mm-skap/#intcmp=searchProvider_dacsa
Retrieved Dec 3 2012

17. http://direktronik.se/prod/prod.asp?ProdId=56
Retrieved Dec 8 2012

18. http://www.cableworld.se/naetverkskabel-och-tillbehoer/crossover-patchkabel/crossover-patchkabel-utp-cat5e-1-meter.asp
Retrieved Dec 9 2012

19. http://www.senetic.se/product/ASR1006-20G-VPN/K9
Retrieved Dec 9 2012

20. http://www.senetic.se/product/FLASR1-FW-RTU=
Retrieved Dec 9 2012

21. http://www.senetic.se/product/N2K-C2248TP-1GE
Retrieved Dec 9 2012

22. http://www.senetic.se/product/WS-C3560X-48P-L
Retrieved Dec 9 2012

23. http://www.senetic.se/product/WS-C3560X-24P-L
Retrieved Dec 9 2012

24. http://www.dustin.se/product/5010198167/toten-19-golvskap-42u-600x1000-perforerad-dorr-svart/#intcmp=searchProvider_dacsa
Retrieved Dec 9 2012

25. http://www.dustin.se/product/5010206992/toten-19-vaggskap-6u-600x600-glasdorr-svart/#intcmp=searchProvider_dacsa
Retrieved 3 Dec 2012

26. http://www.dustin.se/product/5010107222/flaktpaket-med-2-flaktar-for-600x600mm-skap/#intcmp=searchProvider_dacsa
Retrieved Dec 3 2012

27. http://www.cableworld.se/naetverkskabel-och-tillbehoer/naetverkskabel-cat6/patchkabel-stp-cat6-pimf-5-meter.asp
    Retrieved Dec 9 2012

28. http://www.cableworld.se/naetverkskabel-och-tillbehoer/naetverkskabel-cat6/patchkabel-stp-cat6-pimf-10-meter.asp
    Retrieved Dec 9 2012

29. http://www.cableworld.se/naetverkskabel-och-tillbehoer/naetverkskabel-cat7/patchkabel-sftp-cat7-pimf-(ljusgraa)-1-meter.asp
    Retrieved Dec 9 2012

30. http://www.cableworld.se/naetverkskabel-och-tillbehoer/naetverkskabel-cat7/patchkabel-sftp-cat7-pimf-(ljusgraa)-1-meter.asp
    Retrieved Dec 9 2012

31. http://www.cableworld.se/naetverkskabel-och-tillbehoer/crossover-patchkabel/crossover-patchkabel-utp-cat6-1-meter.asp
    Retrieved Dec 9 2012

32. http://www.cableworld.se/naetverkskabel-och-tillbehoer/crossover-patchkabel/crossover-patchkabel-utp-cat6-5-meter.asp
    Retrieved Dec 9 2012

33. http://direktronik.se/prod/prod.asp?ProdId=56
    Retrieved Dec 9 2012

34. http://www.senetic.se/product/ASR1002-5G-VPN/K9
    Retrieved Dec 9 2012

35. http://www.senetic.se/product/FLASR1-FW-RTU=
    Retrieved Dec 9 2012

36. http://www.senetic.se/product/WS-C3560X-48P-L
    Retrieved Dec 9 2012

37. http://www.senetic.se/product/WS-C3560X-24P-L
    Retrieved Dec 9 2012

38. http://www.dustin.se/product/5010206992/toten-19-vaggskap-6u-600x600-glasdorr-svart/#intcmp=searchProvider_dacsa
    Retrieved 3 Dec 2012

39. http://www.dustin.se/product/5010107222/flaktpaket-med-2-flaktar-for-600x600mm-skap/#intcmp=searchProvider_dacsa
    Retrieved Dec 3 2012

40. http://www.cableworld.se/naetverkskabel-och-tillbehoer/naetverkskabel-cat6/patchkabel-stp-cat6-pimf-1-meter.asp
Retrieved Dec 9 2012

41. http://www.cableworld.se/naetverkskabel-och-tillbehoer/naetverkskabel-cat6/patchkabel-stp-cat6-pimf-5-meter.asp
Retrieved Dec 9 2012

42. http://www.cableworld.se/naetverkskabel-och-tillbehoer/naetverkskabel-cat6/patchkabel-stp-cat6-pimf-10-meter.asp
Retrieved Dec 9 2012

43. http://www.cableworld.se/naetverkskabel-och-tillbehoer/naetverkskabel-cat7/patchkabel-sftp-cat7-pimf-(ljusgraa)-0,5-meter.asp
Retrieved Dec 9 2012

44. http://direktronik.se/prod/prod.asp?ProdId=56
Retrieved Dec 9 2012

45. http://www.senetic.se/product/ASR1002-5G-VPN/K9
Retrieved Dec 9 2012

46. http://www.senetic.se/product/FLASR1-FW-RTU=
Retrieved Dec 9 2012

47. http://www.senetic.se/product/WS-C3560X-48P-L
Retrieved Dec 9 2012

48. http://www.dustin.se/product/5010206992/toten-19-vaggskap-6u-600x600-glasdorr-svart/#intcmp=searchProvider_dacsa
Retrieved 3 Dec 2012

49. http://www.dustin.se/product/5010107222/flaktpaket-med-2-flaktar-for-600x600mm-skap/#intcmp=searchProvider_dacsa
Retrieved Dec 3 2012

50. http://www.cableworld.se/naetverkskabel-och-tillbehoer/naetverkskabel-cat6/patchkabel-stp-cat6-pimf-1-meter.asp
Retrieved Dec 3 2012

51. http://www.cableworld.se/naetverkskabel-och-tillbehoer/naetverkskabel-cat6/patchkabel-stp-cat6-pimf-5-meter.asp
Retrieved Dec 3 2012

52. http://www.cableworld.se/naetverkskabel-och-tillbehoer/naetverkskabel-cat6/patchkabel-stp-cat6-pimf-10-meter.asp
Retrieved Dec 3 2012

53. http://www.cableworld.se/naetverkskabel-och-tillbehoer/naetverkskabel-cat7/patchkabel-sftp-cat7-pimf-(ljusgraa)-0,5-meter.asp
Retrieved Dec 3 2012

54. http://direktronik.se/prod/prod.asp?ProdId=56
Retrieved Dec 3 2012

55. http://www.routereflector.com/en/2013/09/glbp/
Retrieved Dec 14 2013

8 Attachments

Customer Case Study Customer Case Study
Leading German Bank Raises Bar on Secure, Reliable Service

Deutsche Postbank deploys Cisco MPLS core network to deliver secure, reliable, scalable service for
global customers.

EXECUTIVE SUMMARY
Customer Name: Deutsche Postbank
Industry: Financial Services
Location: Bonn, Germany
Number of Employees: 21,000
BUSINESS CHALLENGE
.
Migrate from ATM to MPLS
.
Maintain high security level
.
Support future technology roadmap
NETWORK SOLUTION
.
Cisco ASR1000 Aggregation Services Router
BUSINESS RESULTS
.
Secure, flexible infrastructure
.
Reduced energy consumption
.
Lowered TCO by 40percent
.
Exceeded security compliance standards

Business Challenge

With 14 million domestic customers, 21,000 employees, and total

assets of €242 billion, Deutsche Postbank Group is one of Germany's major financial services providers. Its focus is on retail business with private customers; however, Postbank is also active in the corporate banking sector. In its "Transaction Banking" division, it performs back-office services for other financial services providers. The bank offers deposits, loans and mortgages, asset management, insurance, and commercial finance, including factoring and leasing services, through more than 1100 branches; it also offers some services through post office locations. Postbank is considered to have the largest customer potential of any bank in Germany.

Postbank's business relationship with Cisco has been long and successful. For over 16 years, the bank had run its core backbone on Cisco® 7500 routers on ATM technology. Now, to provide the technological base in the network backbone that the bank needed to successfully position itself as Germany’s largest retail bank, and to meet strict compliance requirements, Deutsche Postbank made the decision to migrate from ATM to the more flexible Multiprotocol Label Switching (MPLS) technology. The bank turned to Cisco for a solution that would meet its needs for the future. Because Postbank also performs transaction services for other banks, it needed to split the network into logical parts while maintaining the highest security level. The bank also needed to implement a quality of service (QoS) policy to support its technology roadmap, for example, voice over IP (VOIP). Finally, Deutsche Postbank was looking for enhanced network performance and scalability in order to stay flexible and be able to move quickly in the marketplace.

Customer Case Study

Network Solution

Postbank’s existing backbone lacked flexibility, did not allow for multiple, simultaneously secure sessions, and did not offer the ability to accommodate future QoS needs for VoIP. In addition, multiple virtual circuits made traffic engineering and operations cumbersome on an ATM-based network and too complex.

To achieve the reliability, performance, and security that Postbank needed, the bank adopted an MPLS core network utilizing the Cisco ASR1000 Aggregation Services Router Series. As part of the Cisco Borderless Network vision, the Cisco ASR 1000 transforms and extends the enterprise WAN edge, offering business-critical resiliency with intelligent services flexibility to allow enterprise businesses to accelerate their growth potential. The Cisco ASR 1000 also provides scalable, secure multiservice aggregation at the headquarters and high-end branch and managed customer premises equipment (CPE) services in remote offices. Postbank installed four ASR1006 routers with 20Gbps engine, VPN, and firewall licenses at its two data centers. The bank also installed four ASR1004 with 10 Gbps engine, and 25 ASR1002 with 10 Gbps engine, all with VPN (IPSec) and firewall licenses throughout the 15 main branches. This configuration makes up Postbank’s core backbone. “We are convinced by the Cisco architectural solutions, and based on our experience, we put our trust in the excellent product quality of Cisco products,” says Michael Heinze, Postbank senior architect.

“By migrating our backbone from ATM to MPLS technology including QOS Service with Cisco’s ASR 1000 Series router we have reduced complexity and operational expenses and provided a flexible base to build our future on.”

— Manfred Paulus, Infrastructure Planning Team Lead, Postbank Systems AG

Business Results

With the transition from ATM technology to MPLS technology utilizing Cisco’s ASR1000 Series routers, Postbank has gained a more secure, flexible, and agile infrastructure that allows the bank to optimize the retail business as well as set up future business needs. Lifecycle management and roadmap planning are also high priorities for Postbank. By working with Cisco as a strategic partner, the bank developed a future roadmap of the MPLS core network that would give it plenty of capacity for expansion.

Postbank saw big cost savings on energy, as well. One of the most important ways that the Cisco ASR 1000 Series Router helps reduce energy consumption is its ability to consolidate the services of multiple single-function appliances into one device. By reducing rack space, power consumption, and cooling, Postbank.'s energy cost savings allowed it to re-finance more than 40 percent of its hardware investment costs. Heinze says, "To win in today's global financial services industry, it is essential that we have a dynamic, highly secure, and reliable network infrastructure. By partnering with Cisco, our new MPLS network with Cisco ASR 1000 routers gives us the advantage we need to stay ahead of our competitors."

PRODUCT LIST

.
Cisco ASR1000 Aggregation Services Router

Next Steps

Based on Postbank´s core network design, the bank will extend the network to 120 of its A&B Finance Consulting branches using the Cisco ASR1000 and Cisco ISR G2 with a zero touch deployment. The

deployment will be fully automated with the Cisco Configuration Engine, where all future configuration and software updates are pushed out centrally. This capability makes the management processes in the operations department of Postbank much thinner and faster.

Technical Implementation

The following is a sample deployment and configuration guide for an MPLS virtual private network in IP tunnel environments.

http://www.cisco.com/en/US/prod/collateral/routers/ps9343/Deploying_and_Configuring_MPLS_Virtual_Private_Networks_In_IP_Tunnel_Environment.pdf.

For More Information

To find out more about the Cisco Aggregated Services Routers, go to: http://www.cisco.com/go/asr.

Printed in USA C36-647404-00 02/11

9 Appendix

9.1 Appendix A – PF

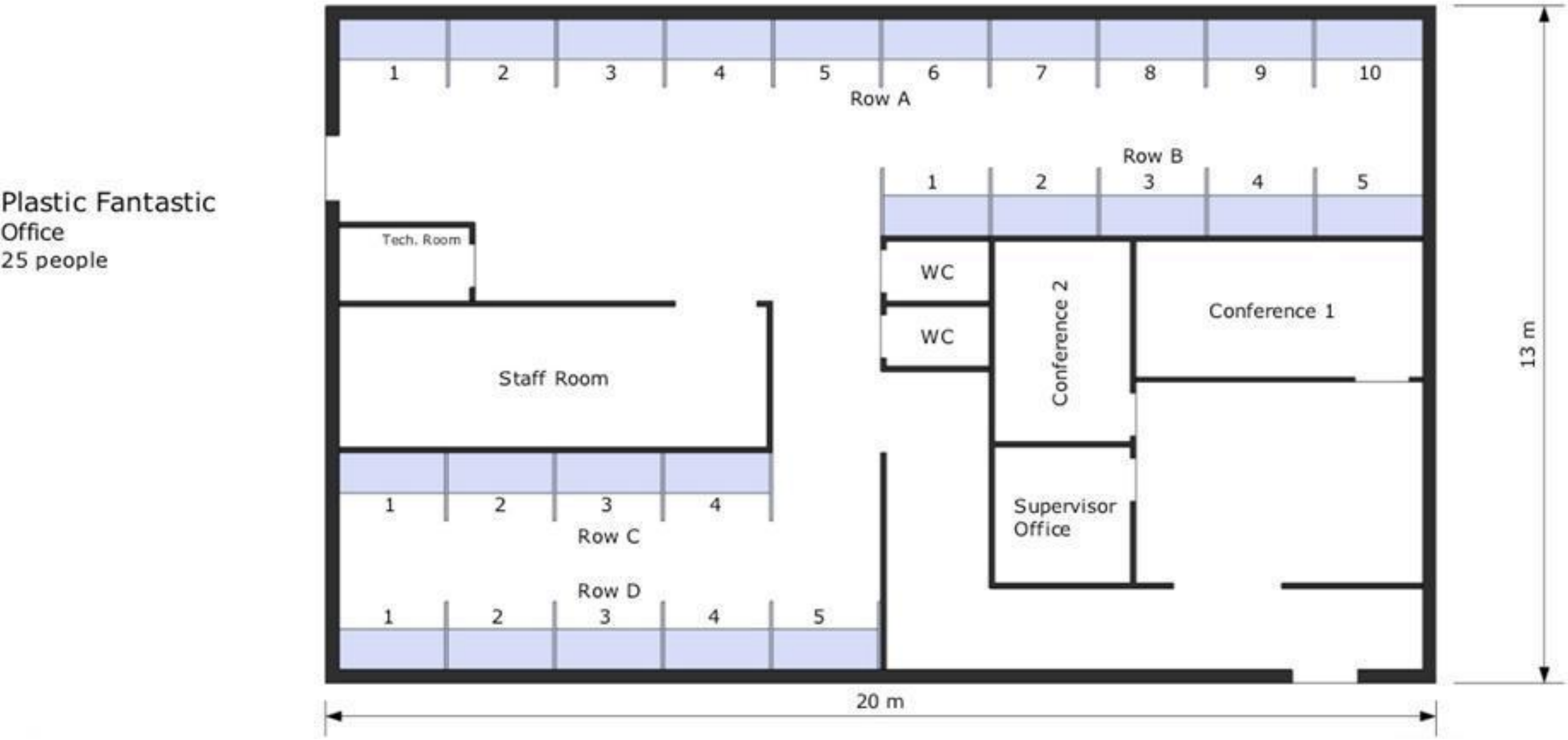
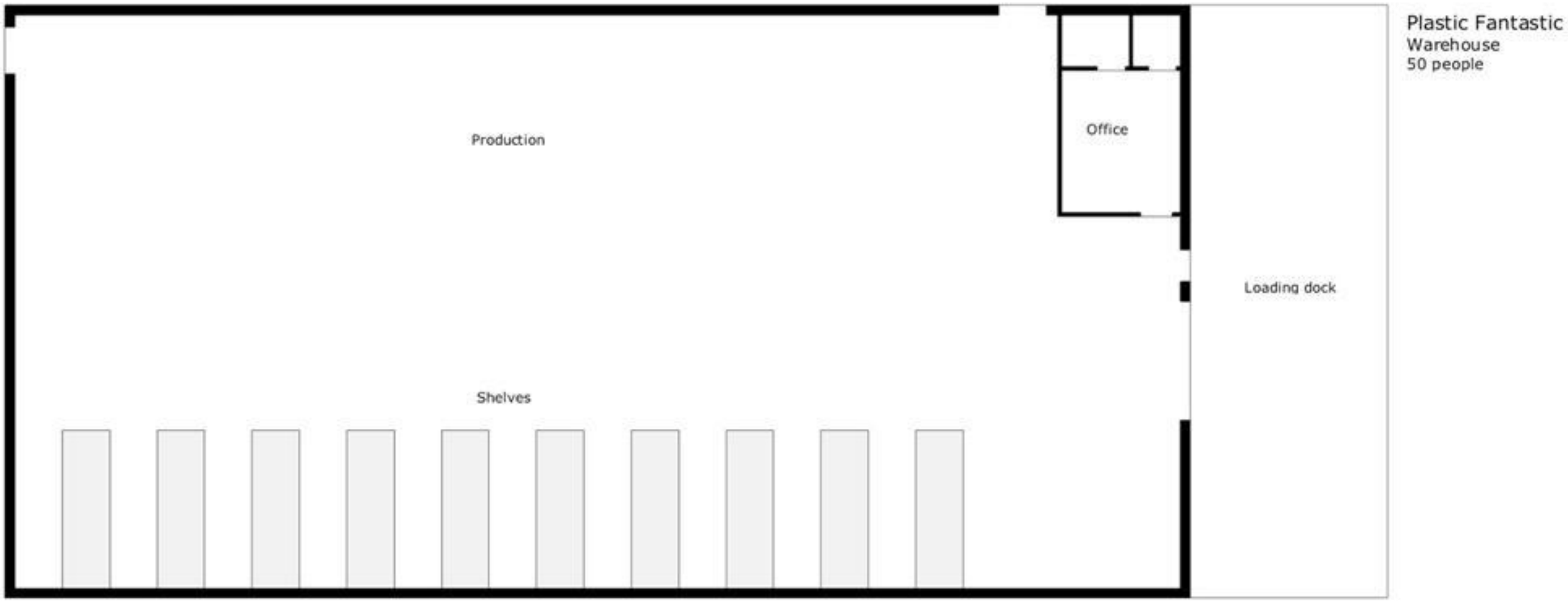


Figure 4.1.1


Plastic Fantastic
Warehouse
50 people
Production
Office
Loading dock
Shelves

Figrure 4.1.2

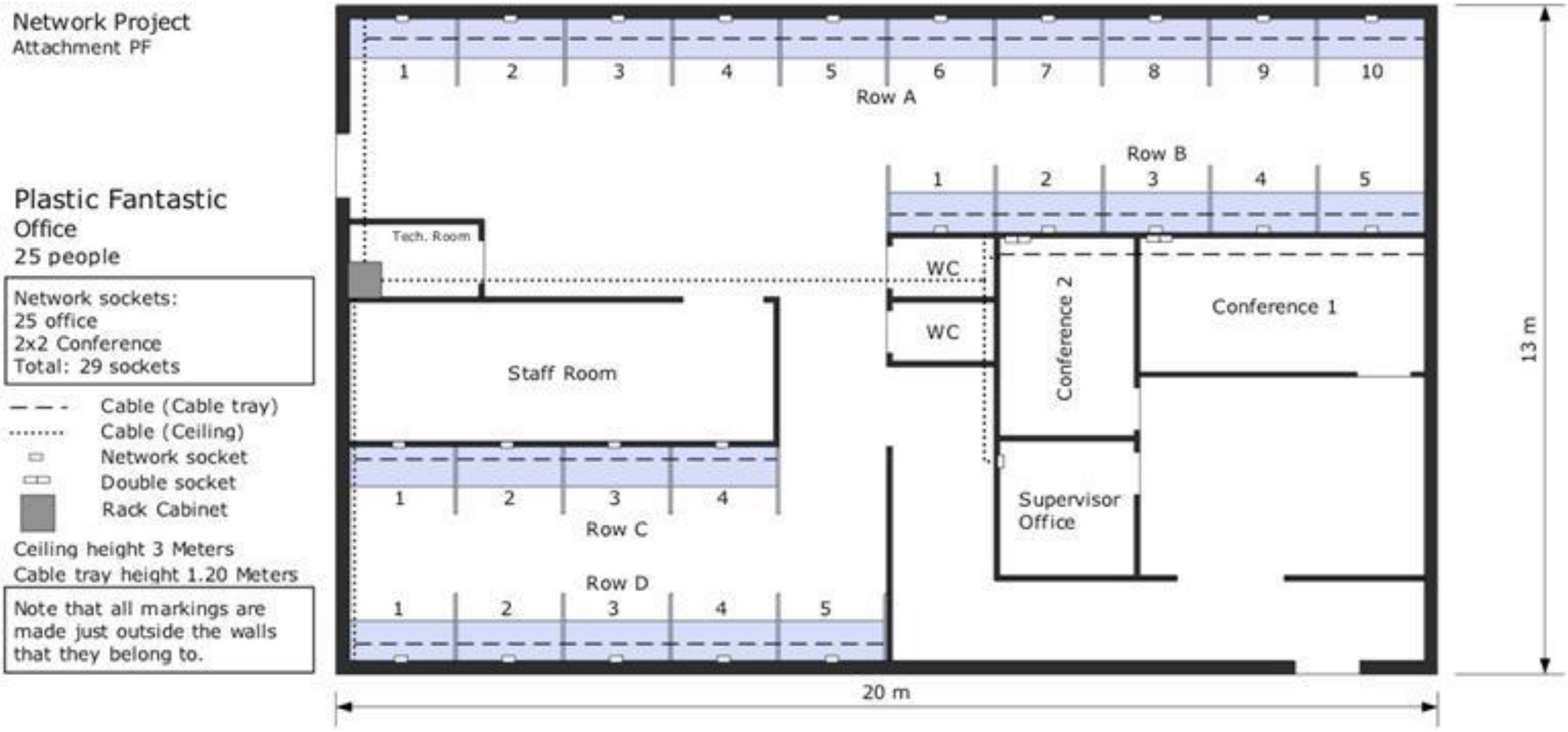

Network Project
Attachment PF
Plastic Fantastic
Office
25 people
Network sockets:
25 office
2x2 Conference
Total: 29 sockets
Cable (Cable tray)
Cable (Ceiling)
Network socket
Double socket
Rack Cabinet
Ceiling height 3 Meters
Cable tray height 1.20 Meters
Note that all markings are made just outside the walls that they belong to.
1
2
3
4
5
6
7
8
9
10
Row A
Row B
1
2
3
4
5
Tech. Room
WC
WC
Conference 2
Conference 1
Staff Room
1
2
3
4
Row C
Row D
1
2
3
4
5
Supervisor Office
13 m
20 m

Figure 4.1.3

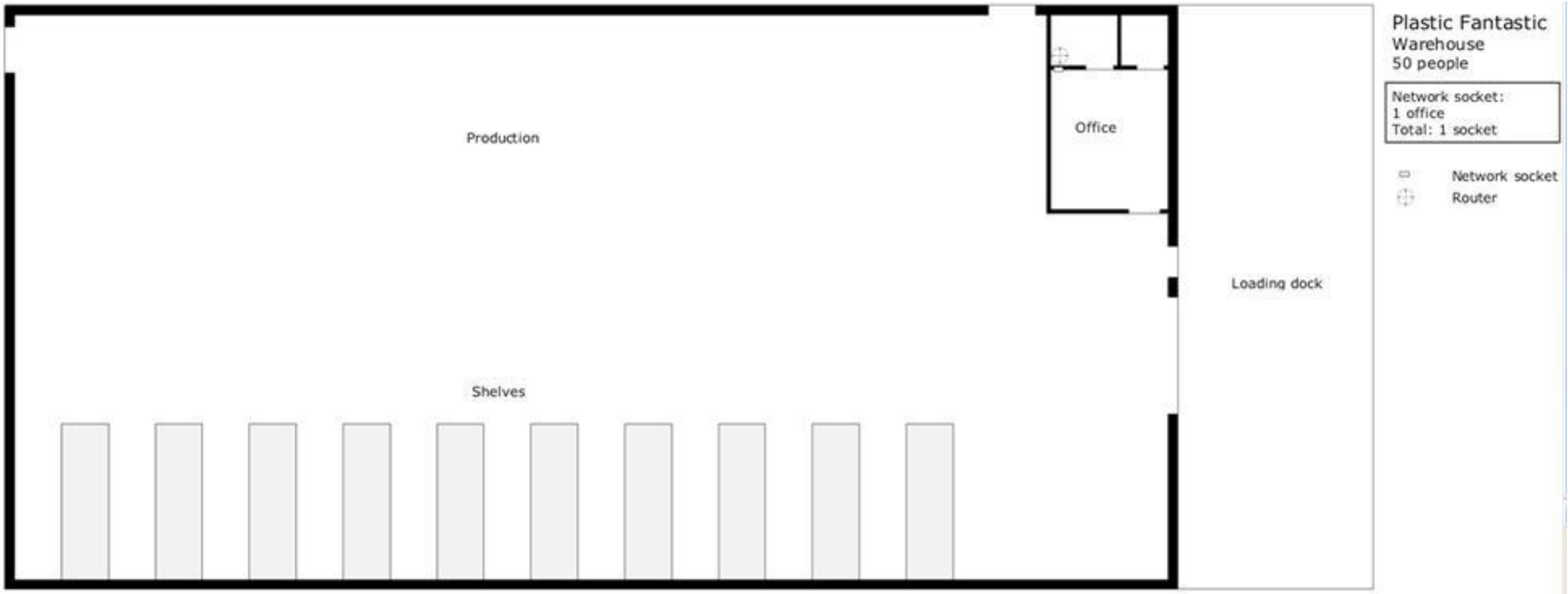

Production
Office
Shelves
Loading dock
Plastic Fantastic
Warehouse
50 people
Network socket:
1 office
Total: 1 socket
Network socket
Router

Figure 4.1.4

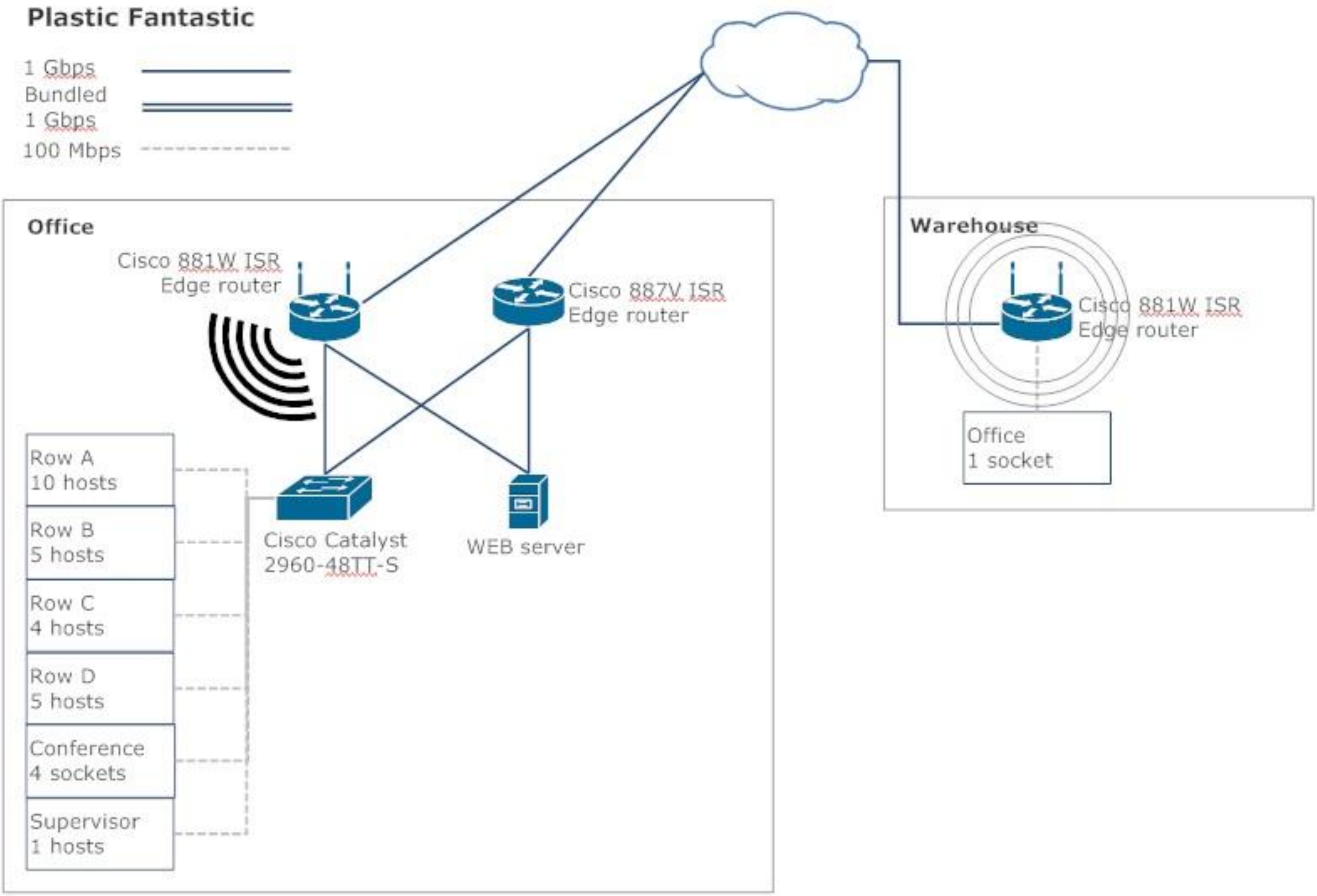
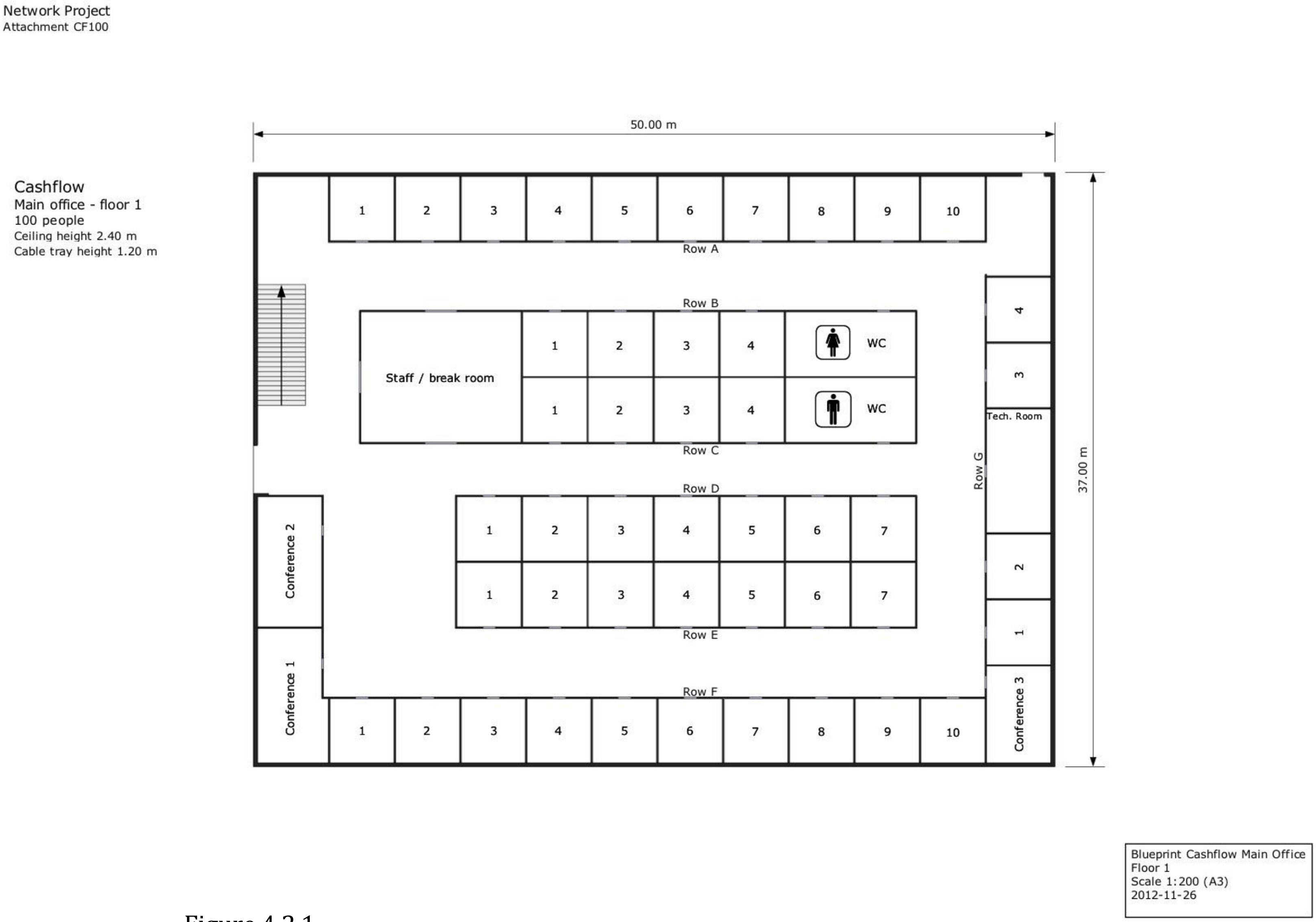

Plastic Fantastic
1 Gbps
Bundled 1 Gbps
100 Mbps
Office
Cisco 881W ISR Edge router
Cisco 887V ISR Edge router
Row A 10 hosts
Row B 5 hosts
Row C 4 hosts
Row D 5 hosts
Conference 4 sockets
Supervisor 1 hosts
Cisco Catalyst 2960-48TT-S
WEB server
Warehouse
Cisco 881W ISR Edge router
Office 1 socket

Figure 4.1.5

9.2 Appendix B - CF



Network Project
Attachment CF100

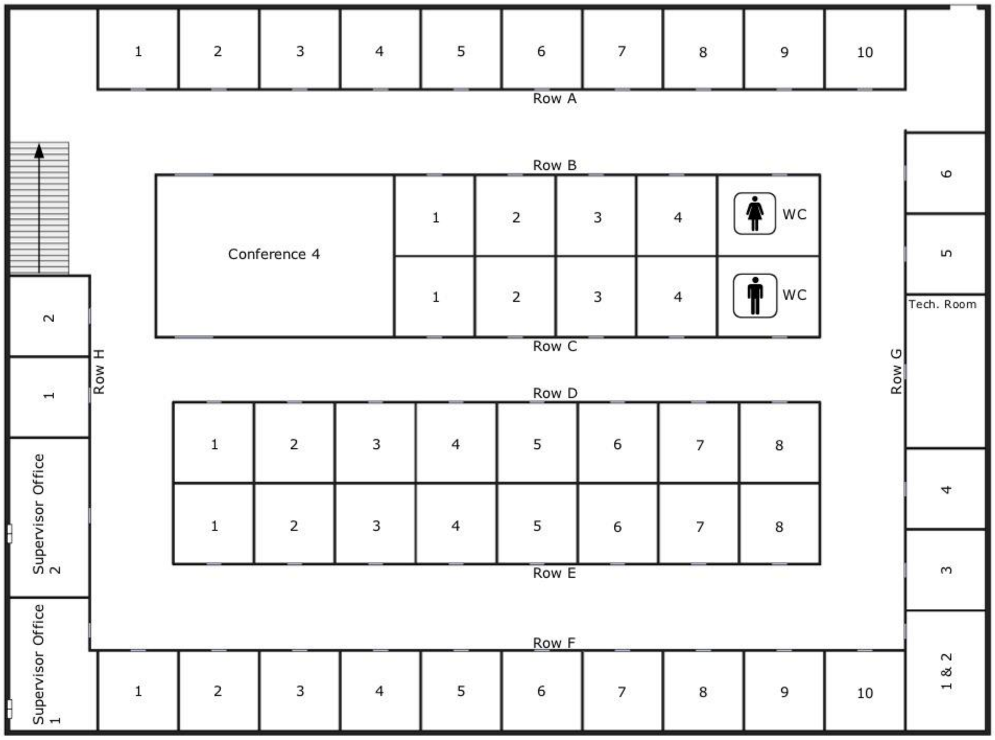
Cashflow
Main office - floor 1
100 people
Ceiling height 2.40 m
Cable tray height 1.20 m

Blueprint Cashflow Main Office
Floor 1
Scale 1:200 (A3)
2012-11-26

Figure 4.2.1

Network Project
Attachment CF100

Cashflow
Main office - floor 2
100 people
Ceiling height 2.40 m
Cable tray height 1.20 m



Blueprint Cashflow Main Office
Floor 2
Scale 1:200 (A3)
2012-11-26

Figure 4.2.2

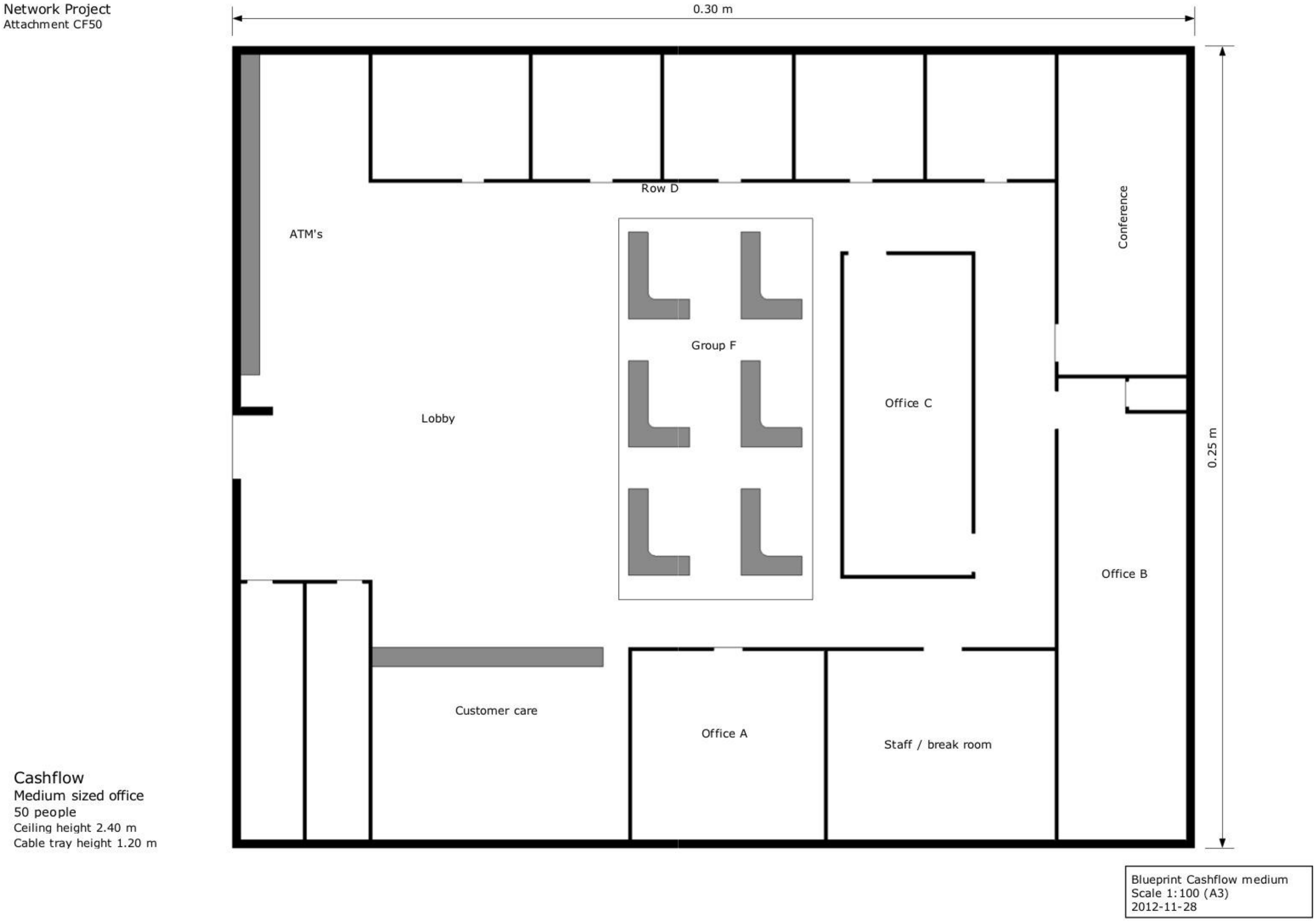

Network Project
Attachment CF50
0.30 m
Row D
ATM's
Conference
Group F
Office C
Lobby
0.25 m
Office B
Customer care
Office A
Staff / break room
Cashflow
Medium sized office
50 people
Ceiling height 2.40 m
Cable tray height 1.20 m
Blueprint Cashflow medium
Scale 1:100 (A3)
2012-11-28

Figure 4.2.3

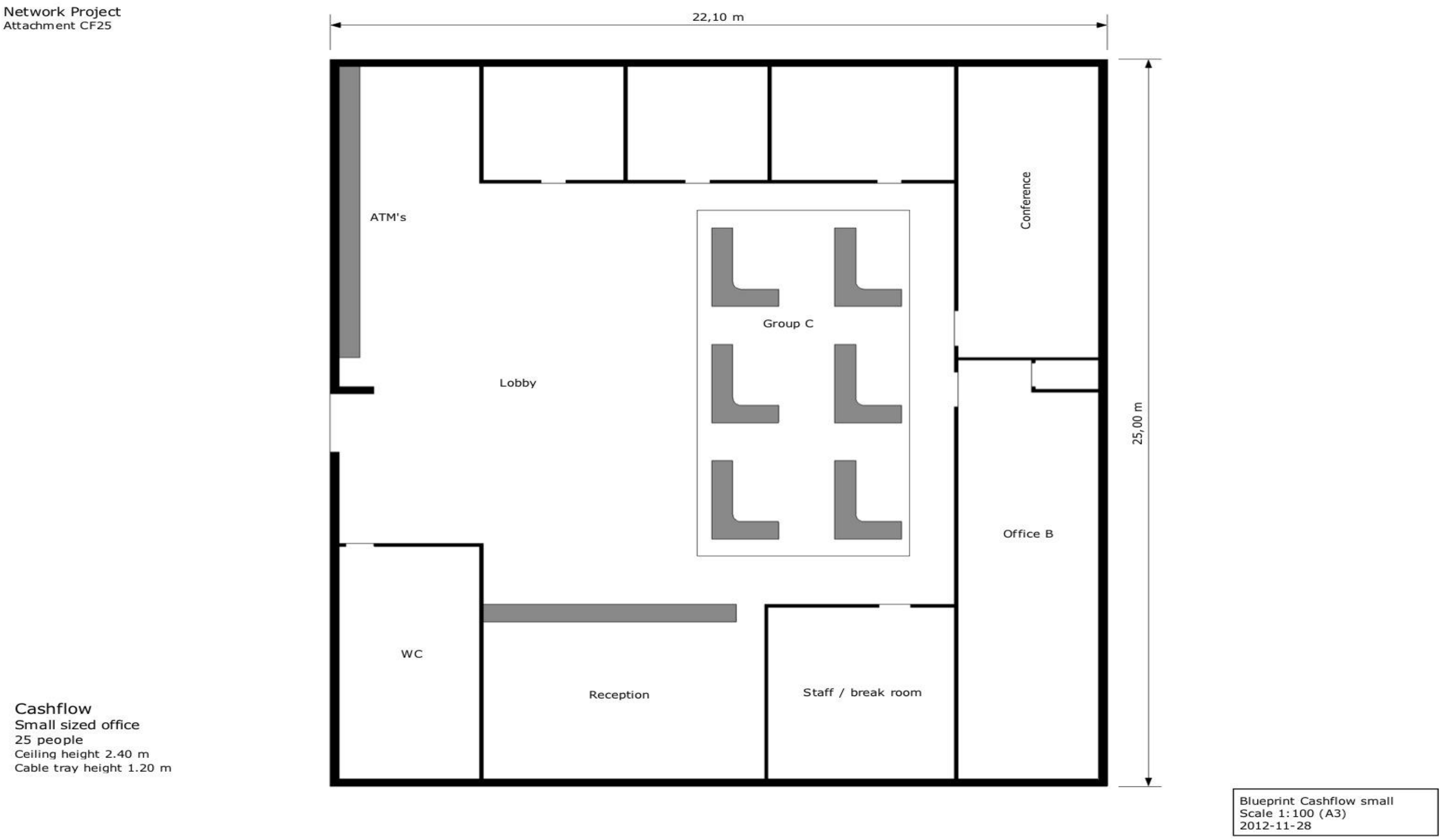

Network Project
Attachment CF25
22,10 m
ATM's
Conference
Group C
Lobby
25,00 m
Office B
WC
Reception
Staff / break room
Cashflow
Small sized office
25 people
Ceiling height 2.40 m
Cable tray height 1.20 m
Blueprint Cashflow small
Scale 1:100 (A3)
2012-11-28

Figure 4.2.4

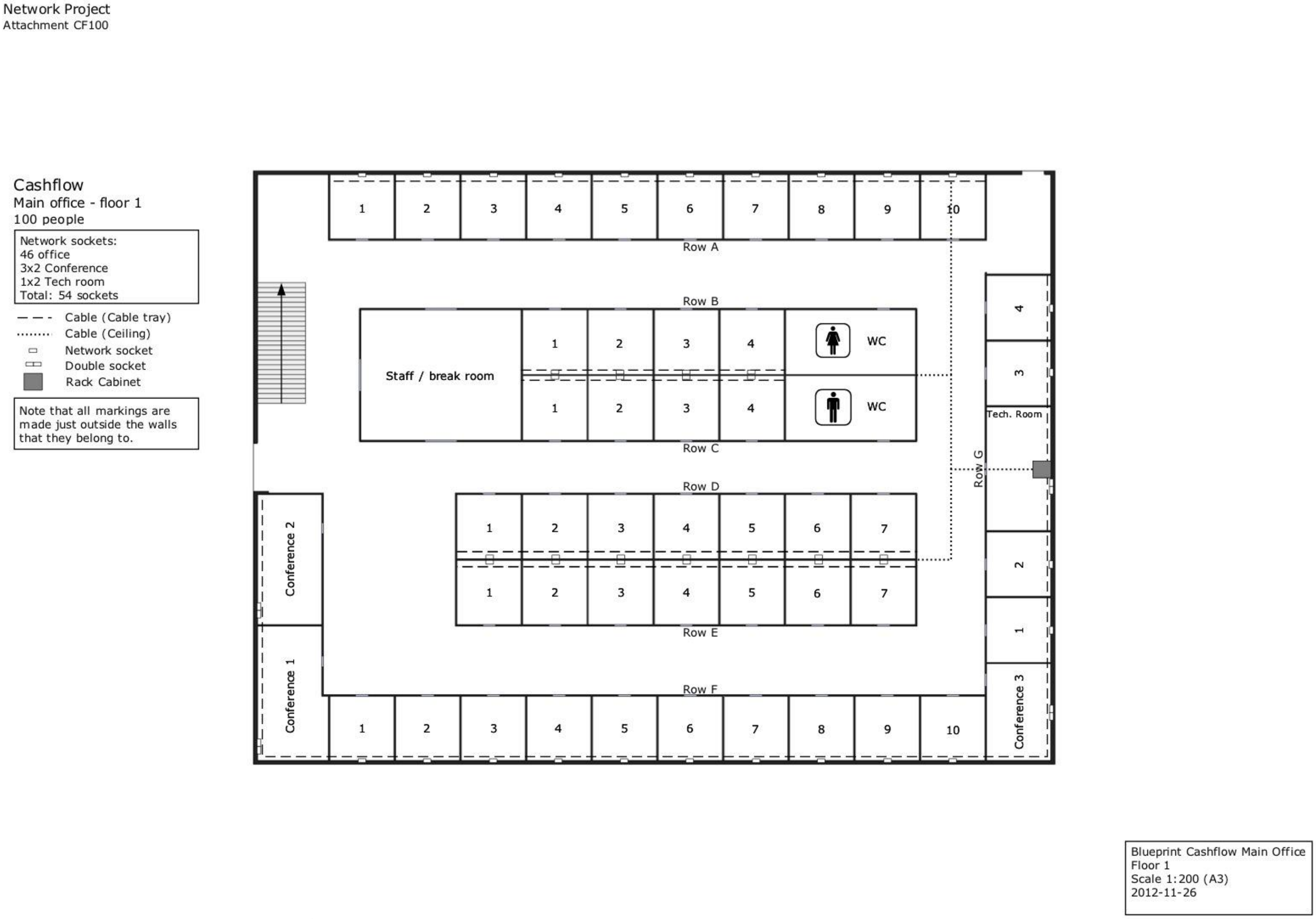

Network Project
Attachment CF100
Cashflow
Main office - floor 1
100 people
Network sockets:
46 office
3x2 Conference
1x2 Tech room
Total: 54 sockets
Cable (Cable tray)
Cable (Ceiling)
Network socket
Double socket
Rack Cabinet
Note that all markings are made just outside the walls that they belong to.
1 2 3 4 5 6 7 8 9 10
Row A
Row B
Staff / break room
1 2 3 4
WC
1 2 3 4
WC
Row C
Row D
1 2 3 4 5 6 7
1 2 3 4 5 6 7
Row E
Row F
1 2 3 4 5 6 7 8 9 10
Conference 2
Conference 1
4
3
Tech. Room
Row G
2
1
Conference 3
Blueprint Cashflow Main Office
Floor 1
Scale 1:200 (A3)
2012-11-26

Figure 4.2.5

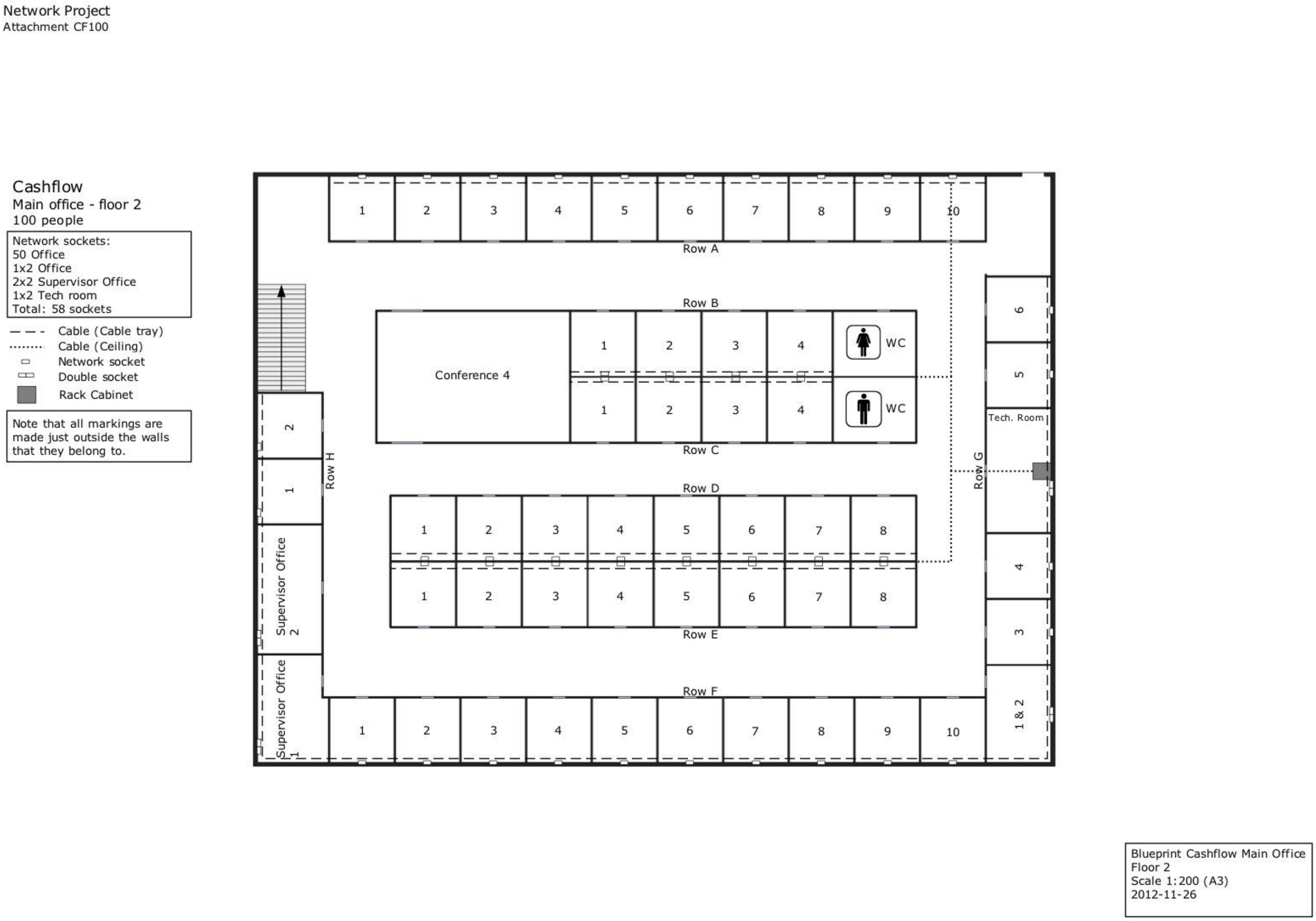

Network Project
Attachment CF100
Cashflow
Main office - floor 2
100 people
Network sockets:
50 Office
1x2 Office
2x2 Supervisor Office
1x2 Tech room
Total: 58 sockets
Cable (Cable tray)
Cable (Ceiling)
Network socket
Double socket
Rack Cabinet
Note that all markings are made just outside the walls that they belong to.
Row A
Row B
Row C
Row D
Row E
Row F
Row G
Row H
Conference 4
WC
WC
Tech. Room
Supervisor Office 2
Supervisor Office 1
1 & 2
Blueprint Cashflow Main Office
Floor 2
Scale 1:200 (A3)
2012-11-26

Figure 4.2.6

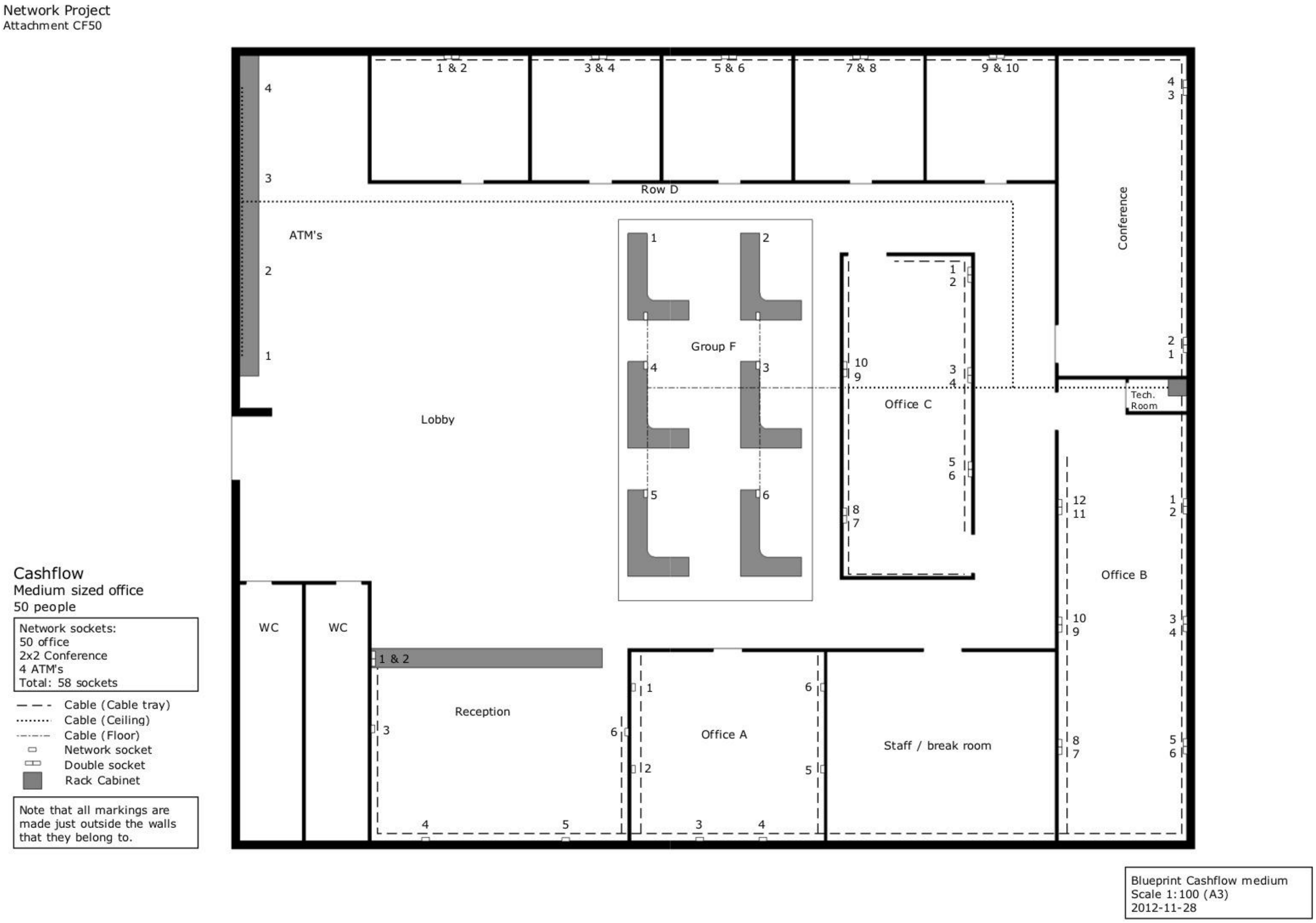

Network Project
Attachment CF50
1 & 2
3 & 4
5 & 6
7 & 8
9 & 10
4
3
2
1
Row D
ATM's
Group F
1
2
3
4
5
6
Office C
1
2
3
4
5
6
7
8
9
10
Conference
4
3
2
1
Tech. Room
Lobby
Office B
1
2
3
4
5
6
7
8
9
10
11
12
WC
WC
1 & 2
Reception
3
4
5
6
Office A
1
2
3
4
5
6
Staff / break room
Cashflow
Medium sized office
50 people
Network sockets:
50 office
2x2 Conference
4 ATM's
Total: 58 sockets
Cable (Cable tray)
Cable (Ceiling)
Cable (Floor)
Network socket
Double socket
Rack Cabinet
Note that all markings are made just outside the walls that they belong to.
Blueprint Cashflow medium
Scale 1:100 (A3)
2012-11-28

Figure 4.2.7

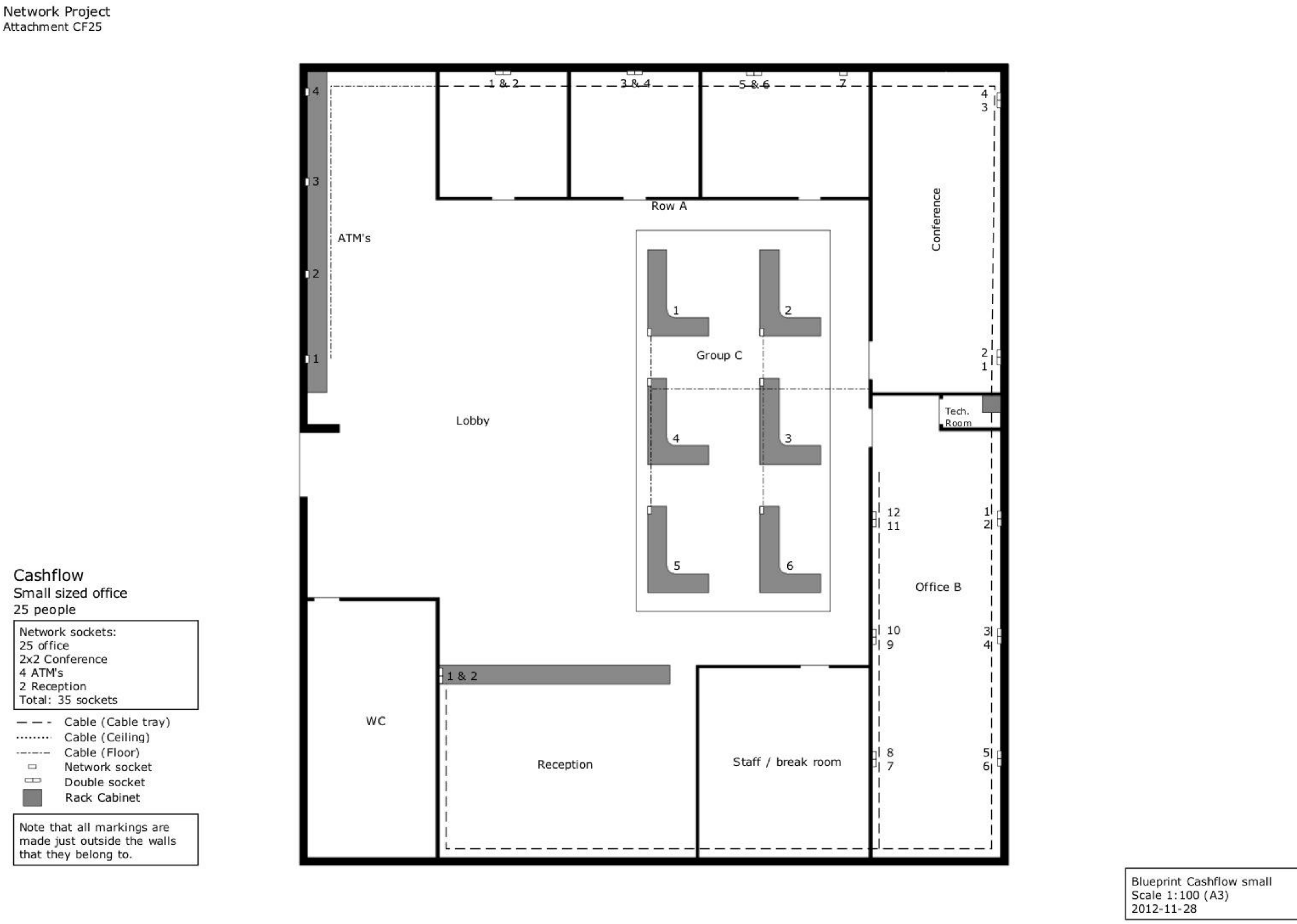

Network Project
Attachment CF25
4
3
2
1
ATM's
1 & 2
3 & 4
5 & 6
7
4
3
Conference
Row A
1
2
Group C
4
3
5
6
Lobby
2
1
Tech.
Room
12
11
1
2
Office B
10
9
3
4
8
7
5
6
1 & 2
WC
Reception
Staff / break room
Cashflow
Small sized office
25 people
Network sockets:
25 office
2x2 Conference
4 ATM's
2 Reception
Total: 35 sockets
Cable (Cable tray)
Cable (Ceiling)
Cable (Floor)
Network socket
Double socket
Rack Cabinet
Note that all markings are made just outside the walls that they belong to.
Blueprint Cashflow small
Scale 1:100 (A3)
2012-11-28

Figure 4.2.8

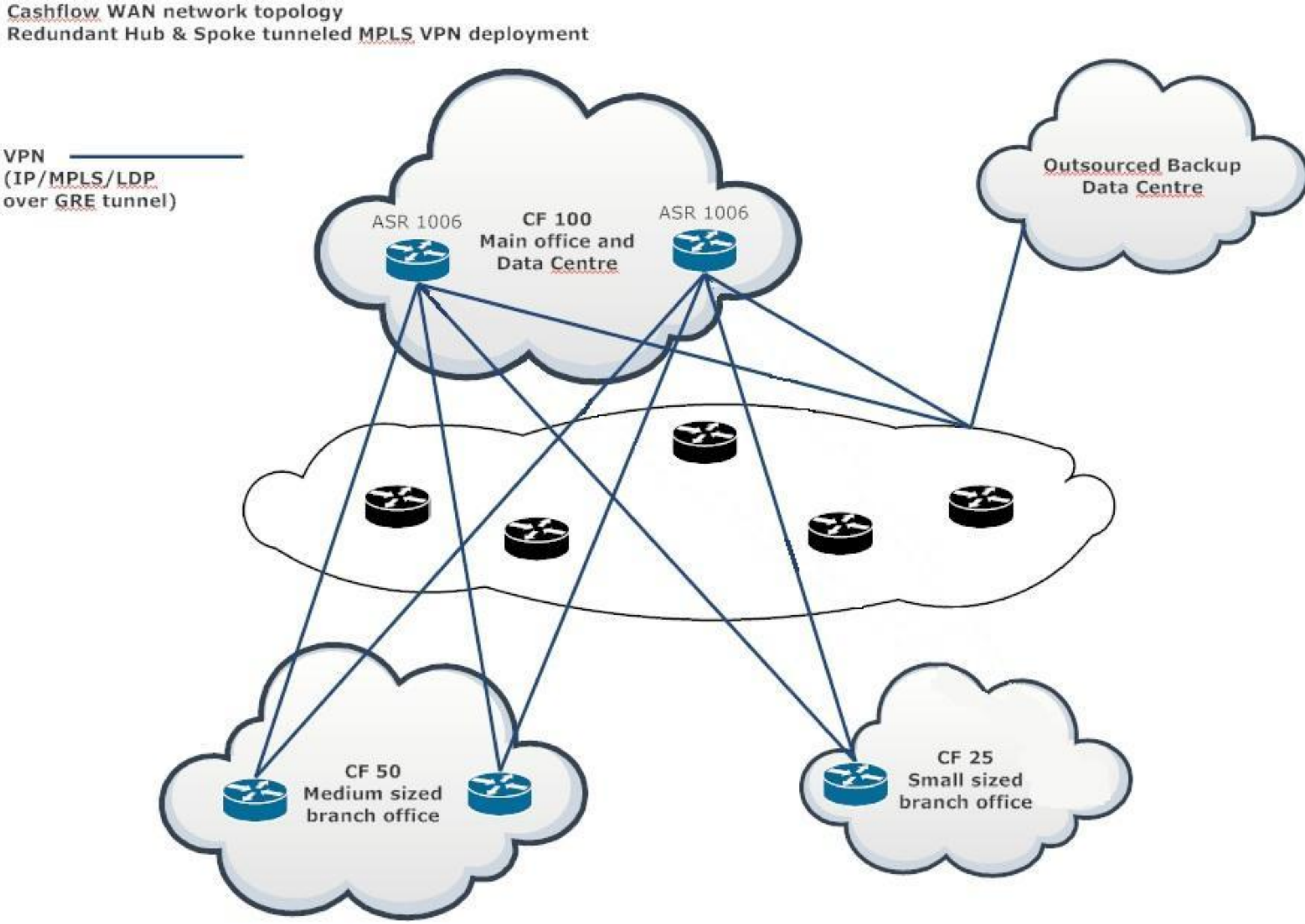

Cashflow WAN network topology
Redundant Hub & Spoke tunneled MPLS VPN deployment
VPN
(IP/MPLS/LDP
over GRE tunnel)
ASR 1006
CF 100
Main office and
Data Centre
ASR 1006
Outsourced Backup
Data Centre
CF 50
Medium sized
branch office
CF 25
Small sized
branch office

Figure 4.2.9

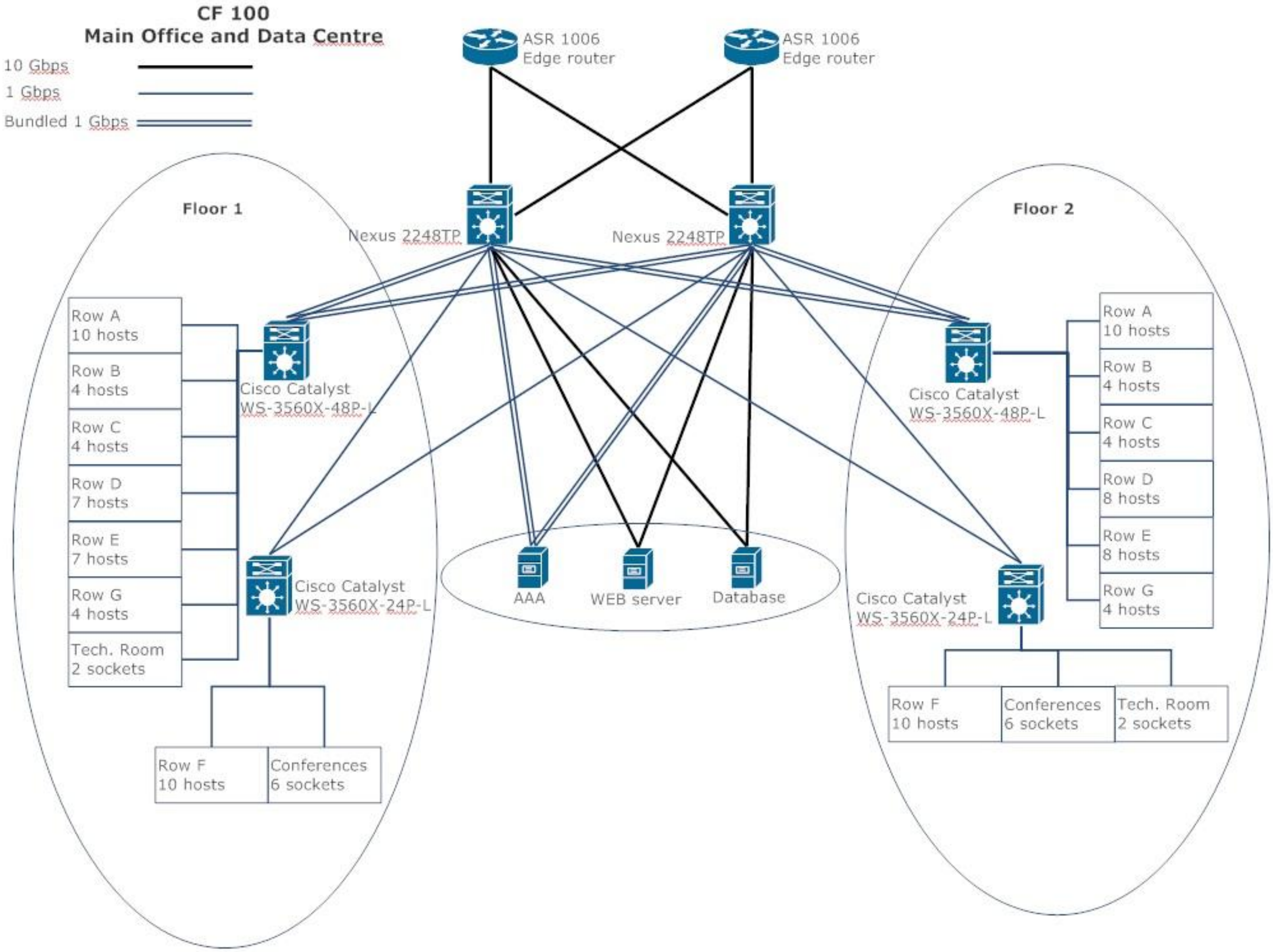

CF 100
Main Office and Data Centre
10 Gbps
1 Gbps
Bundled 1 Gbps
ASR 1006
Edge router
ASR 1006
Edge router
Floor 1
Floor 2
Nexus 2248TP
Nexus 2248TP
Row A
10 hosts
Row B
4 hosts
Row C
4 hosts
Row D
7 hosts
Row E
7 hosts
Row G
4 hosts
Tech. Room
2 sockets
Cisco Catalyst
WS-3560X-48P-L
Cisco Catalyst
WS-3560X-24P-L
Row F
10 hosts
Conferences
6 sockets
AAA
WEB server
Database
Row A
10 hosts
Row B
4 hosts
Row C
4 hosts
Row D
8 hosts
Row E
8 hosts
Row G
4 hosts
Cisco Catalyst
WS-3560X-48P-L
Cisco Catalyst
WS-3560X-24P-L
Row F
10 hosts
Conferences
6 sockets
Tech. Room
2 sockets

Figure 4.2.10

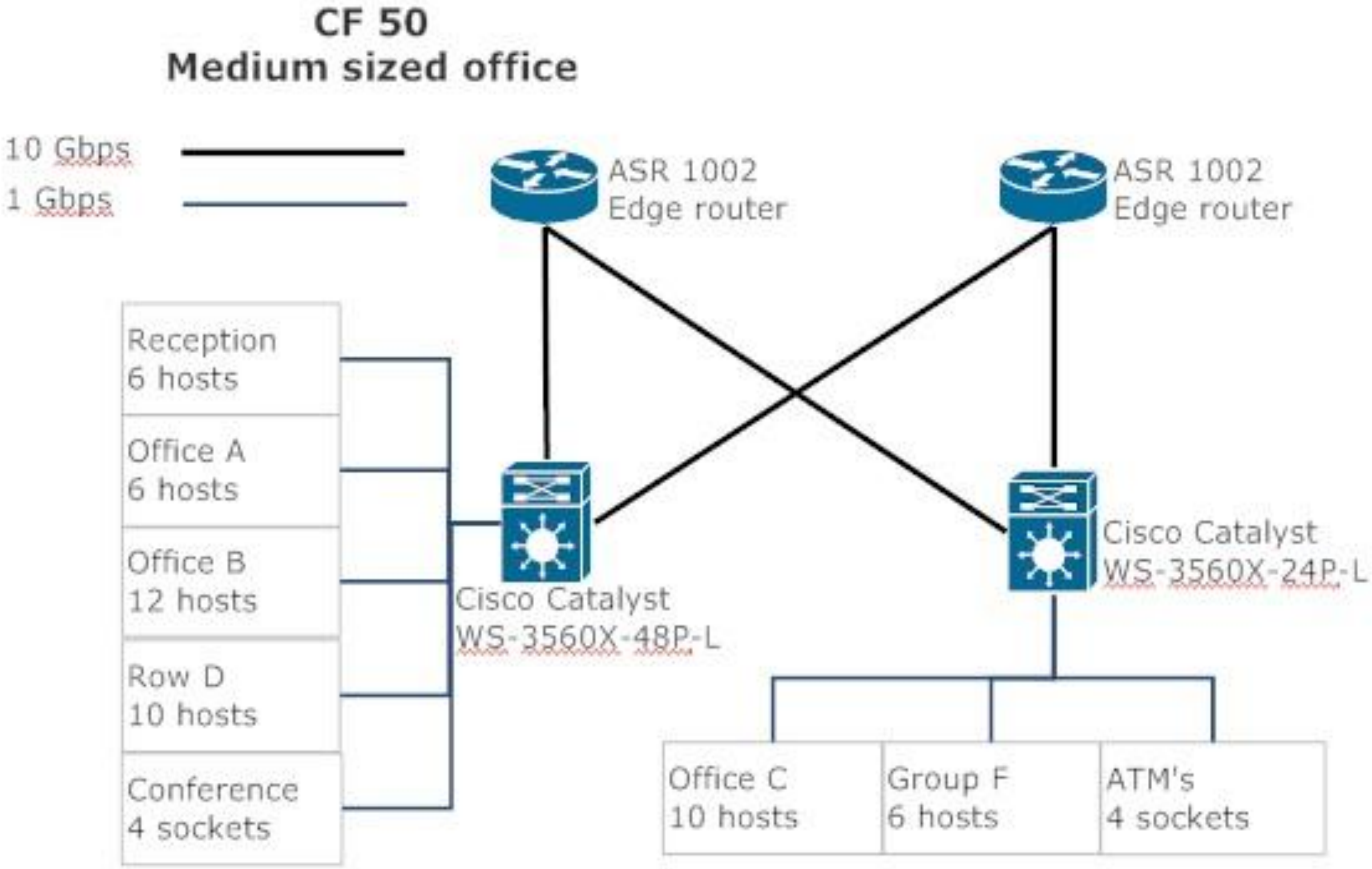

CF 50
Medium sized office
10 Gbps
1 Gbps
ASR 1002
Edge router
ASR 1002
Edge router
Reception
6 hosts
Office A
6 hosts
Office B
12 hosts
Row D
10 hosts
Conference
4 sockets
Cisco Catalyst
WS-3560X-48P-L
Cisco Catalyst
WS-3560X-24P-L
Office C
10 hosts
Group F
6 hosts
ATM's
4 sockets

Figure 4.2.11

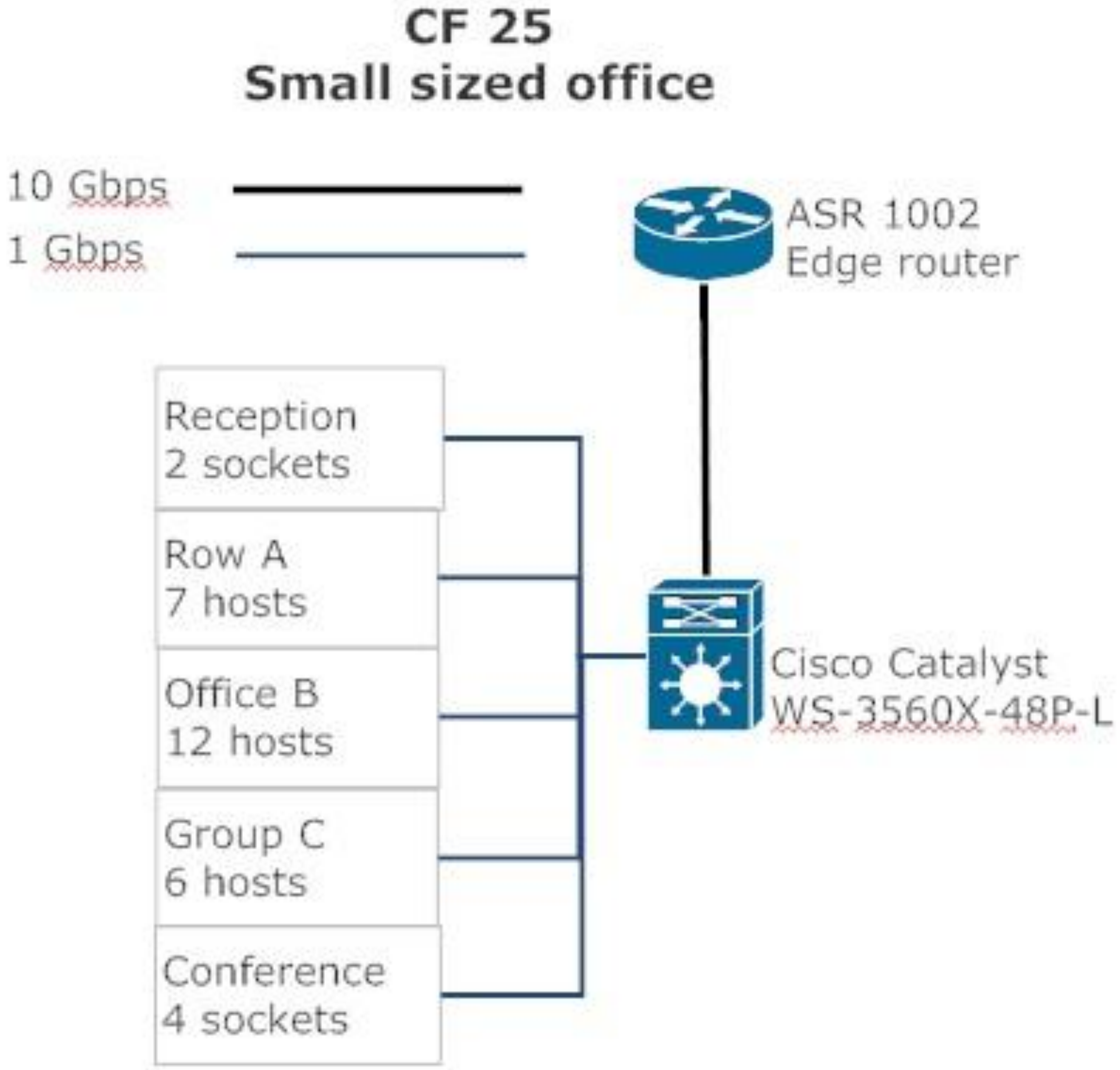

CF 25
Small sized office
10 Gbps
1 Gbps
ASR 1002
Edge router
Reception
2 sockets
Row A
7 hosts
Office B
12 hosts
Group C
6 hosts
Conference
4 sockets
Cisco Catalyst
WS-3560X-48P-L

Figure 4.2.12

HALMSTAD UNIVERSITY • PO Box 823 • SE-301 18 Halmstad, Sweden • www.hh.se