

Word Count Word®: 3335 words



Networks and Protocols Project

Contents

Introduction.....	2
LAN Networks.....	3
Cabling technology.....	3
HUB/Switch	3
Wireless Access Point.....	4
Security	4
LAN sites.....	4
Cables used.....	5
Telephony	5
Cables used.....	5
Buildings connection	5
Birmingham	5
Geneva.....	6
Would WIMAX acceptable for 1.5 Km?	6
Sites connection	7
Financial purposes:	8
Visio Topology	10
Conclusion	13

Introduction

In this project, we have to restructure the network of a bank that is employing 2500 employees over several sites, distributed in three different countries:

- Geneva, Switzerland: headquarters.
- Plan-Les-Ouates, Switzerland: server farm.
- Birmingham, United Kingdom: admin office and branch office.
- Annecy, France: sales office.

Improving the current network installation means increasing bandwidth and improve the efficiency and quality of the communication through it. So, we write this report explaining technologies and how to use them in this context, commenting what could be the best for the company and how to apply such a technology.

There is everything but Simulations in this report, as I didn't succeed doing it with packet tracer. You will find the recreation of the Packet Tracer project under Microsoft Visio® (more convenient to put in a Word report) in the last part.

LAN Networks

There is a Local Area Network in each site. This type of networks purpose is to connect together a variety of different devices, communicating data between them over a limited zone. Sharing resources (documents, applications, printers) in an office is essential as it permit a better efficiency both the machines (you need less hardware to do the same) and the employees (they work more easily together) in a same office. These LANs can be connected to other network such as other LANs or WANs (Wide Area Network) and to the Internet. Plus, a LAN provides secure high-speed transfers with a good reliability on error rates.

Cabling technology

There are numerous choices for the technology to use when creating a network. Ethernet, ARCNET, Token Ring... As it is cheap and very common, we will use Ethernet. Most of hardware is built for this technology, so it is compatible with more different products and let us more choice for the other components of the network.

About topology, the more convenient standard is Star-Wired Bus. Most of cabling systems are based on it.

One advantage of the Ethernet technology is that you can choose the bandwidth accordingly to your needs. So different standards exist: Ethernet (10 Mbit/s), Fast Ethernet (100 Mbit/s), Gigabit Ethernet (1,000 Mbit/s), 10 Gigabit Ethernet (10,000 Mbit/s). As Gigabit Ethernet technologies are expensive and a waste of speed most of the time directly linked on normal PCs, it is better to use them for servers and important concentration of connection needs (routers and other devices). For PC purposes in office, we choose Ethernet and Fast Ethernet and for other needs, we'll take Gigabit technology. For now, the company sites are cabled using the old Cat3 (UTP) standard, popular in the early 1990's but not very used nowadays.

HUB/Switch

The current composition of the network is also based on HUB technology. The HUBs are used to extend a network. They are used to amplify the signal and broadcast it to any computer connected to it. This technology can actually be used with Ethernet, but it is not a good solution to carry on using it. As it emit its signal to any port and send the data to all equipment connected, when we increase the number of computers and devices, the collision rate also increase and it reduce the speed of the whole network. Bandwidth is actually shared over the network dividing the total by the number of users.

If we choose a switch instead, as it uses a specific process to solve this problem (micro segmentation), is able to create dedication full bandwidth link from one port to another. The data is not sent to any computer on the network, the recipient only receives it. Several communications can be done at the same time using this process.

The number of ports determines the bandwidth, when we're using switches. A Fast Ethernet one (100 Mbit/s) with 4 ports can support up to 400 Mbit/s with half duplex, and up to 800 Mbit/s using full duplex.

So, even if it is more expensive, it is better to replace the old HUB system and use switches. It would improve a lot speed and internal security al over the network. Not allowing anyone to listen all the data if they are simply connected to one of the HUB.

There are two different types of twisted pair cables: STP are shielded cables coated with aluminium to avoid and protect against problems due to electrostatic fields that can exist in places because of massive electrical installations. There are also UTP that is unshielded, less expensive and sufficient in most of the cases.

The sites are cabled with category 3 connections but it's not enough. What it is now used the more often is cat5 cables for PC connections and cat6 for devices that have to deal with massive amount of data transfers as routers and servers. We will use UTP for most of the installations except for the Secure Storage Area in Birmingham that is EMI shielded.

Wireless Access Point

Some of the employees and visitors need network and Internet connection wireless with their laptops. As we have two kinds of users, with a different status relating to the bank, we must also have two different accesses accordingly to needs and security. Visitors only need a way to access the Internet while people related to the company also want to access and work on files saved on the servers of the local network. We need to identify people connecting on the wireless access point to know what they are allowed to access. As users just need to access the Internet or to carry on working on their files, they don't need a really big broadband and 802.11g standard is good for this type of utilisation. Plus, not all the computers are compatible with the most recent Wi-Fi standard.

Security

Nowadays, a good Wi-Fi encryption is WPA2 to secure the access point WPA and WEP are way too weak for a company security needs and is even less recommended talking about a bank. So only visitors that ask for the key can have an access to Internet, limiting the amount of user to the actual clients and people related to the bank. Then, to know who can access to the actual network, we can use a MAC address filtering; only authorising registered computers to access it because each network card has a unique MAC address. In fact it is possible to mimic these addresses so we need to establish an authentication system with a login and a password to be really sure that people not allowed can access files on the local networks.

LAN sites

In every site, we have one switch per floor and all the PCs there are connected on it. All the switches of a building are connected together, not to paralyze the entire network if we have one of them not working.

Let's take an example: the French sales centre in Annecy. There are three floors, so three arrays of PCs connected to three switches.

In each site (main building talking about Birmingham and Geneva sites) there are both servers and a router connected to the Internet. Each switch of one site is directly connected to the local router. Centralizing a network too much is not really good idea because if a device breaks down, the whole sub network that comes after stop working as well.

Cables used

To interconnect switches, servers and router all together, we need at least the Gigabit Ethernet standard so we have a 125 MByte/s bandwidth for each local network between switches and the router. We could also use 10 Gigabit Ethernet connections, but we don't need to have 1250 MByte/s for this network even if the amount of data can be really large. These LANs are still relatively small.

About PCs the best to do seems to use a less fast standard as Fast Ethernet. We don't need more for work purpose and files management. The bandwidth between a PC and a Switch is up to 12 MByte/s that is already a lot for a single user but not really expensive to establish.

Telephony

In the old network a PBX is used to connect all the phones to the public landline. PBX is a range of multiline telephone systems used in business environments, encompassing systems ranging from small key systems to large scale private branch exchanges. Its advantage is cost saving when calls are internal because the circuit is switching locally reducing charges.

The problem is that for cost saving and to keep the network simple, there is not a router in each building like in the former network. So we can't keep this system for telephony in these places. But we can advantageously replace this system with IP phones. They are cheaper to use for both internal and external calls as they use the local network or the Internet. So we replace phones by IP phones when we don't have a router in the building, but we keep the old PBX system in the main buildings.

Cables used

To connect these phones, we use UTP for cost purposes. We only use STP cables for the Secure Storage Area in Birmingham, as it is EMI shielded, also in Plan-Les-Ouates because there is the Server Room just near the reception. IP phones are connected to the network with Fast Ethernet standard cables (100 Mbit/s).

Buildings connection**Birmingham**

The Birmingham site has two buildings. There is the branch office that is supposed to be the main building and the Administration centre. A two-lane road only separates these buildings and the two teams may need to share their resources. So, we need to connect their LANs together to create a bigger one. We have several solutions to achieve this task.

We could connect the buildings with a line, but we would need to dig under the road. We would need a permit both for the digging and to bury a communication line. This is really hard to obtain, as we would stop the circulation for a while. Anyway, even with a permit it would be really expensive and would cost way too much for a network update.

Another solution is to pay another connection to a WAN for the second building. But paying two subscriptions to an ISP is not the best solution as the two buildings are so close. So the cheapest and easiest solution is to establish a wireless bridge.

To create one, it is possible to use a Laser or Wi-Fi. Establish a laser link is really good for security, as you can't listen the data without cutting the connexion. It is also really fast as it worth the Gigabit Ethernet technology. But it is also really expensive to buy and to install if you want a good bandwidth and the devices can be damaged.

Wi-Fi is way cheaper and really easy to install. Of course the bandwidth is not the same. It can in theory up to 300 Mbit/s using the last 802.11n standard in the best conditions. Taking the 802.11b/g (54 Mbit/s) standard would be too slow; it is twice less than what we choose to connect a normal PC to a switch.

So the best solution is to use the last Wi-Fi standard as it is cheaper and there's no obstruction in the line of sight. Security is not as good than with a laser, but you can actually protect enough the access as it's supposed to be a point-to-point link and not directly communicate with computers.

To connect the two buildings, we need a device on each of them. I selected the 'Ruckus ZoneFlex 7731 802.11n Bridge' as it is really fast and modern product built to be installed outdoors but with a reasonable price. With this, we mustn't need antennas to have a good connection but the better to do is to place the two devices in front of each other. For security purpose, choosing WPA2 with AES encryption as we chose for the wireless access points is the best we can actually do.

Geneva

In this site the two buildings are separated by 3.5 km. Even if it is possible to use wireless technology, this time we would have to use WIMAX that is expensive enough to consider another solution first and that would be quite slow with this distance as it would have interferences. There's also a lot of obstacles between the two places and a slow and unstable connection is out of the question as we have to connect a server farm with critical data to the main LAN and to the internet to be used by the all three sites of the company and may be by external users if the bank deploy an interactive banking service on it. The other solution is to connect the two locations with a leased line. There is a monthly cost as this solution supposes that we have to find a provider to connect our two places. At least it is fast enough and does not imply to bury cables over 3.5 km.

Would WIMAX acceptable for 1.5 Km?

At this distance, WIMAX would provide a 100 Mbit/s connection. It is correct to have an access to the Internet for normal computer. But, as explained just before, we're not just extending the network to an office. We have to connect a server farm and we need an extremely fast connection. Leased line can be up to 10 Gbit/s there is no comparison, even less far. To have an acceptable connection for our ten servers, we need to pay every month, even if it's more expensive on years (And leased line price also depend of the distance).

Sites connection

As the three sites are really distant (not even the same country), we can't connect them with company owned cabling. So the routers inter-connect them through the Internet that is the ultimate WAN on earth. Internet is a collection of routers belonging to multiple public and private organizations that are interconnected, connecting almost all parts of the world. ATMs, Frame relays and multiple servers compose it. The routers are devices that connect LANs to a WAN that does not belong to our Bank. So we need an Internet Service Provider (ISP) to successfully connect the different sites.

The two choices when connecting to the Internet are DSL (Digital Subscriber Line) and ISDN (Integrated Services Digital Network). Both can carry voice, video and data packets.

ISDN is quite slow and has a 128 Kbit/s bandwidth using a classic phone landline. As we installed really fast Ethernet and Wi-Fi technology over our five buildings, it would be a waste of money and not a productive technology. So anyway we must use DSL technology and forget IDNS.

Even choosing DSL, we still have a choice. In fact, the two main types of DSL are ADSL (asymmetric DSL) and SDSL (symmetric DSL). Individuals mainly use ADSL. When the need is more to access and use Internet services it is a good choice as it provides a faster download bandwidth than upload bandwidth. SDSL as its name implies, gives the same bandwidth in the two ways. The only limit is we can't use a SDSL line as both a WAN access and as a way to make phone calls. As our needs are both a good upstream (files servers, networks sharing, website hosting...) and a good downstream (Internet as a working tool and an information access, downloading served files), we must choose a SDSL offer and pay for another lines, in the buildings that still use the PBXs.

This technology delivers a constant flow for our network traffic. We must have everything always available. A good way to do that is two put two entrances on two different networks to take over the failed link if we have a problem with one.

A lot of companies provide specific offers for our type of needs. We choose an offer with a coupled line as we need one for telephonic purposes. Take two SDSL would be too expensive as we can do the same with a coupled both SDSL and ADSL.

Accordingly, The router must be dual WAN port to support the two different lines and so, connections. It must also be protected with a firewall, not to allow unexpected connection but not blocking the ones we need. Installing a VPN (Virtual Private Network) is also a good idea because it permits a private and secure context over our network communications even if we are connected to Internet, so we are a part of a very large a public and not protected WAN. VPN IPsec uses a high standard authentication and encryption system. It's exactly what we need from our VPN.

To support all these features, we can choose as I suggest it in the next part, the Cisco RV082 Dual WAN VPN Router that provide aforesaid purposes and is still relatively cheap.

Financial purposes:

Type	Product	~Price (\$)
Switch	Cisco SLM2024 24-port Gigabit Smart Switch	400
Router	Cisco RV082 Dual WAN VPN Router	300
IP Phone	Cisco SPA921	80
E 100btx	Cable RJ45 Cat 5 20m	10
E 1000btx	Cable RJ45 Cat 5e 50m	20
Wireless AP	Netgear PROSAFE® WIRELESS AP 802.11G WG302	150
Server	DELL PowerVault MD1200 Direct Attached Storage	3900
Bridge	Ruckus ZoneFlex 7731 Outdoor 802.11n bridge AP	1000

Site 1 : HQ, Geneva			41 PC
Equipment	to intall	Price	Total price
Switch	3	400	1200
Router	1	300	300
IP Phone	0	80	0
100 btx	46	10	460
1000 btx	5	20	100
Access Point	1	150	150
Server	1	3900	3900
Bridge	0	500	0
		Total	6110

Site 1 : Server Farm			2 PC
Equipment	to intall	Price	Total price
Switch	1	400	400
Router	1	300	300
IP Phone	3	80	240
100 btx	5	10	50
1000 btx	20	20	400
Access Point	1	150	150
Server	0	3900	0
Bridge	0	500	0
		Total	1540

Site 2 : French Sales Center, Annecy			31 PC
Equipment	to intall	Price	Total price
Switch	3	400	1200
Router	1	300	300
IP Phone	0	80	0
100 btx	31	10	310
1000 btx	5	20	100
Access Point	1	150	150
Server	1	3900	3900
Bridge	0	500	0
Total			5960

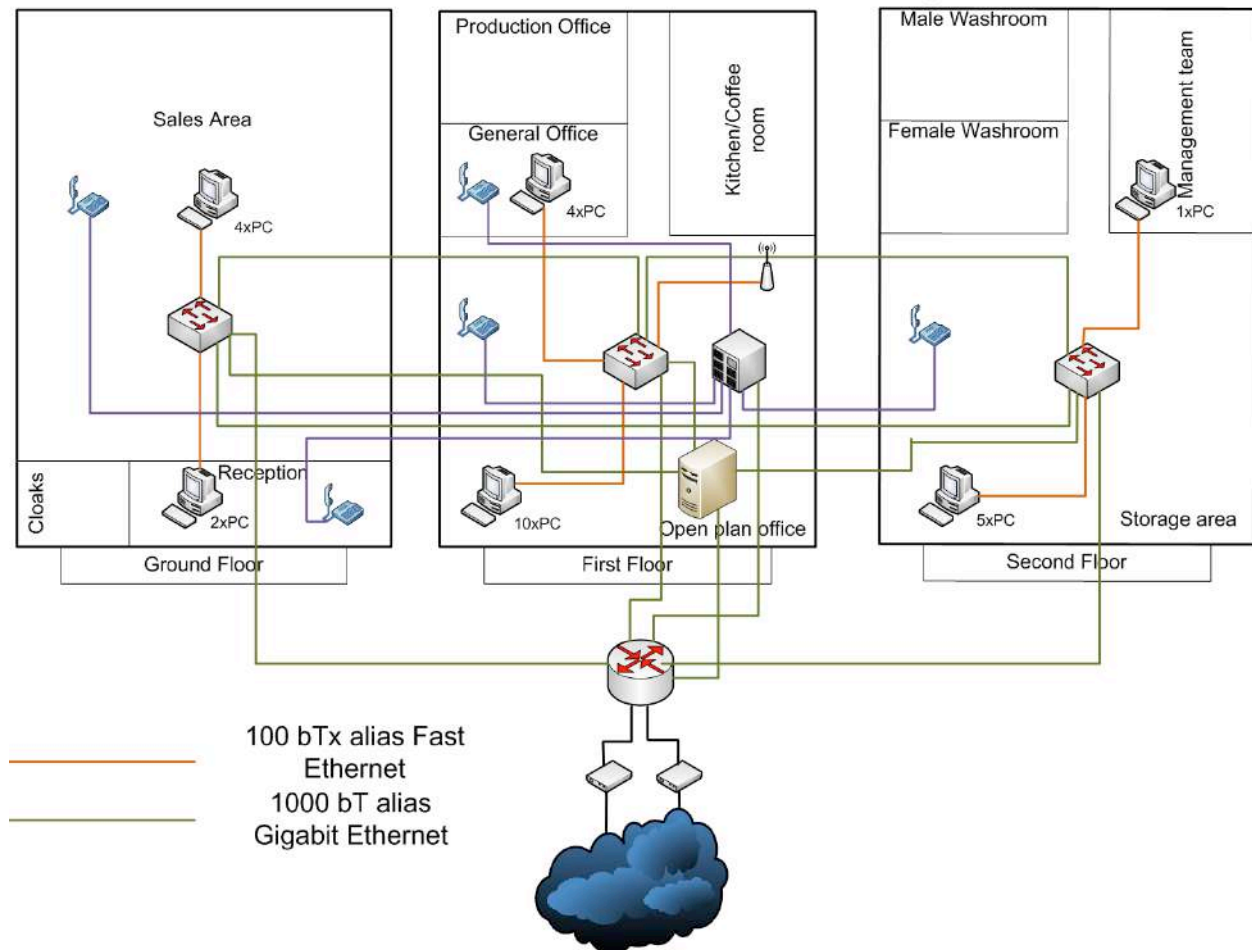
Site 3 : Branch Office, Birmingham			21 PC
Equipment	to intall	Price	Total price
Switch	2	400	800
Router	1	300	300
IP Phone	0	80	0
100 btx	21	10	210
1000 btx	5	20	100
Access Point	1	150	150
Server	1	3900	3900
Bridge	1	1000	1000
Total			5960

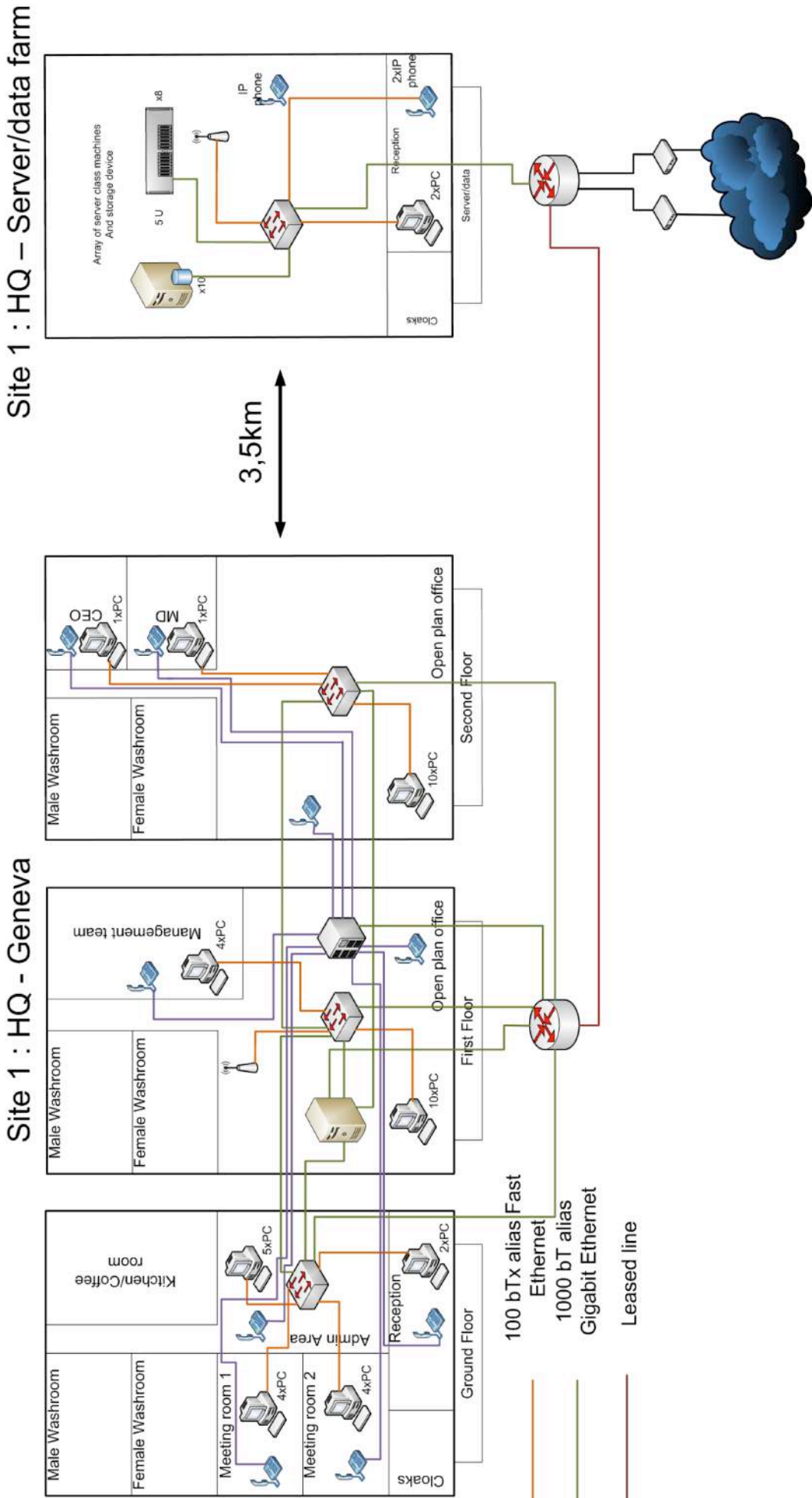
Site 3 : Admin Center, Birmingham			34 PC
Equipment	to intall	Price	Total price
Switch	3	400	1200
Router	0	300	0
IP Phone	34	80	2720
100 btx	68	10	680
1000 btx	4	20	80
Access Point	1	150	150
Server	0	3900	0
Bridge	1	1000	1000
Total			5320

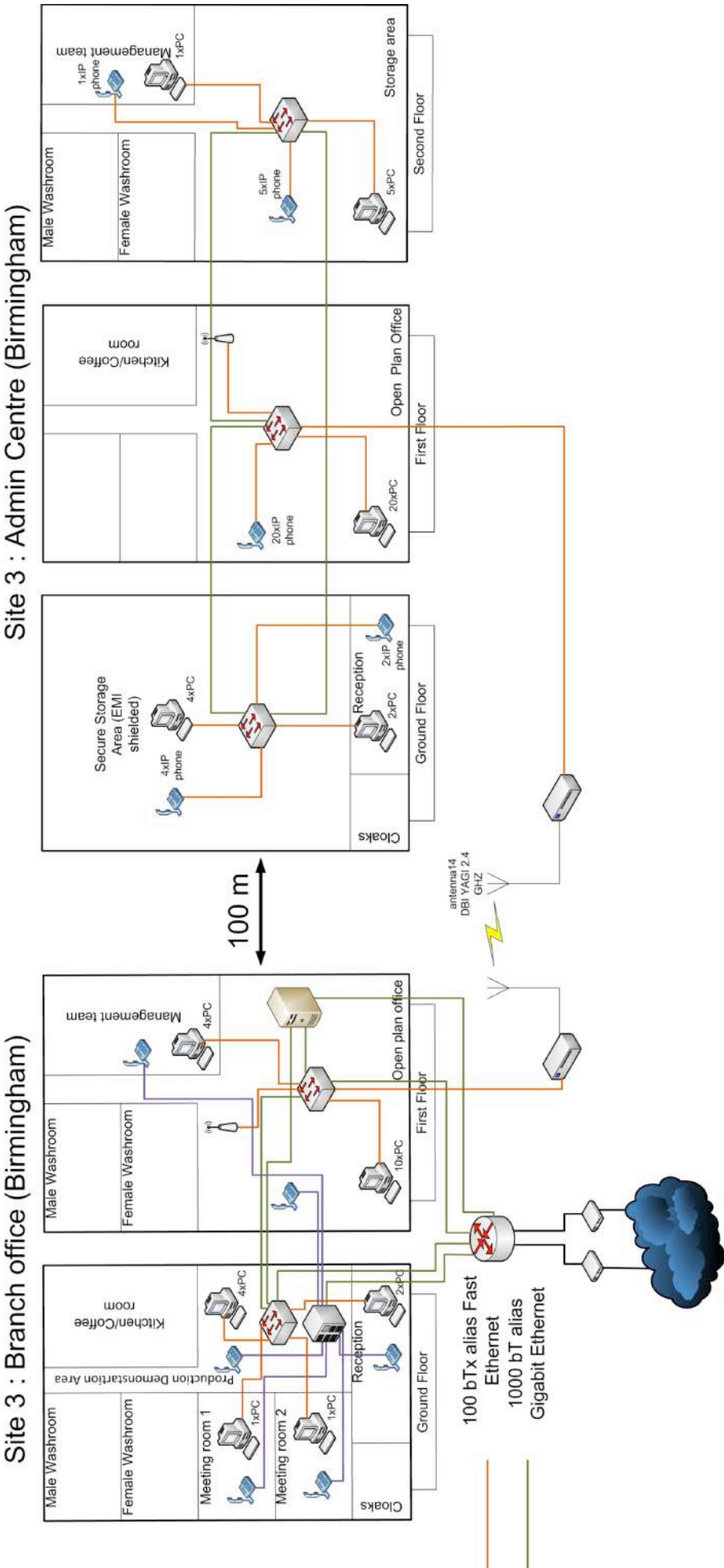
Total cost is around 25,880\$ so ~ 16,420 £

Visio Topology

Site 2 : French sales office, Annecy







Conclusion

This project was a good step learning Network conception and installation, as it was the first time I had to do such a report on this subject. It was interesting to compare different products from various companies and to analyse them to know which one best fit for all the different devices we would have bought. Of course, answers will be quite different for each student as there are so many ways to conceive a Network. It depends each time of both needs and problems and of the subjectivity of the network consultant. Technologies in this domain, as for the other IT ones is in constant evolution and there are new standards and specific technologies/solutions all the time to more and more fit with the needs of any company and interconnect the entire world.