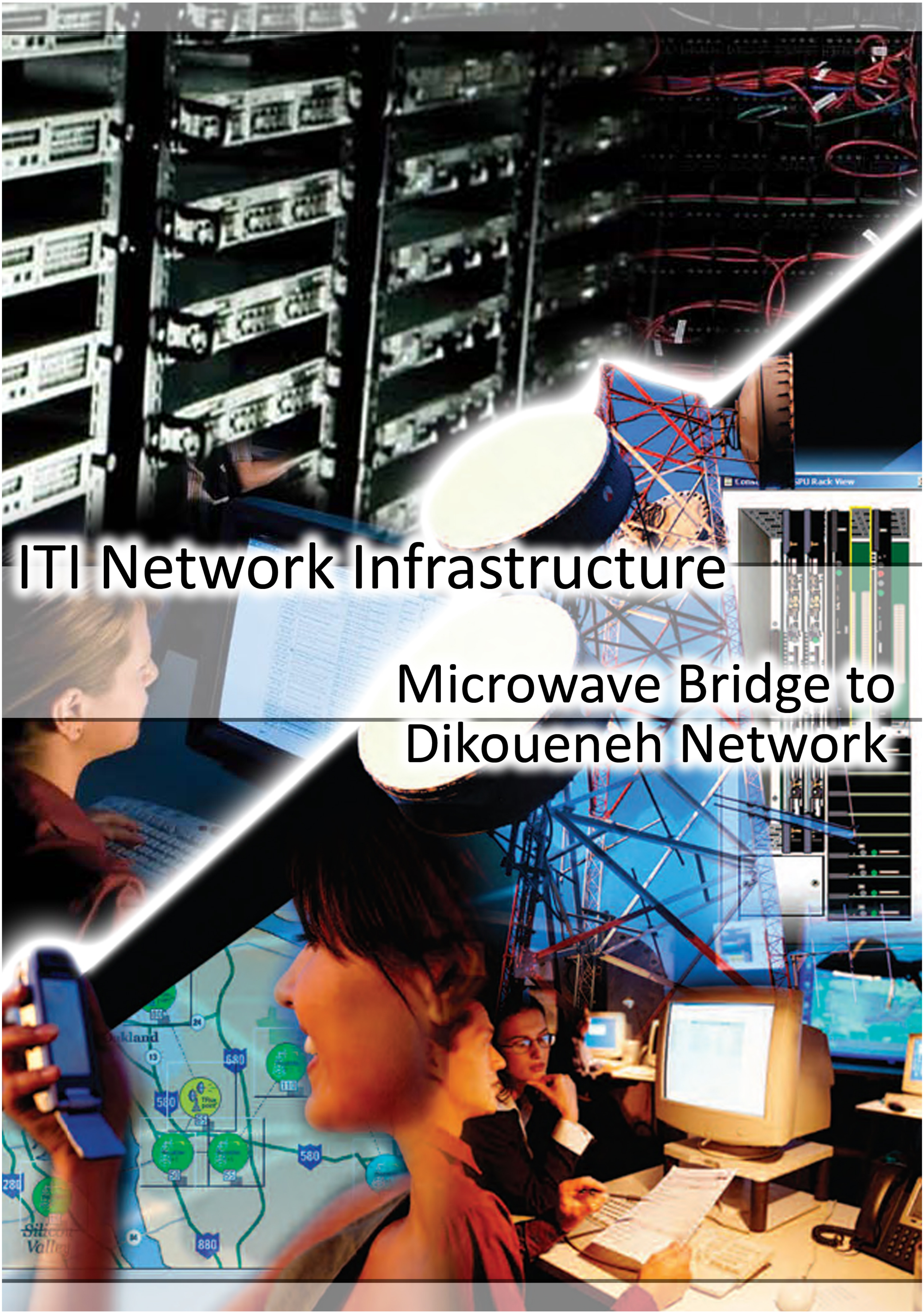


ITI Network Infrastructure

Microwave Bridge to Dikoueneh Network

Index

Introduction

After we have interviewed the director of **Industrial Technical Institute of Beer Hasan (ITI)** Mr. **Abed Kdouh** we have come up with an idea of this project which **computerizes** all the current administrative and educational process in the institute. In this process the institute will benefit a lot from this change and will gain more control over the data shared within it in a completely computerized and safe way.

This study is made out of two parts, the first is the ordinary **network design planning** with all its details and aspects, and the other part is basically based on **wireless network planning**, a microwave link through a vast distance. Along we have to mention that there is no kind of previous network design at the institute what so ever, there are only those labs found on floor two and that sums up the old design.

Our plan is to build a firm fast, safe, secure and reliable network for a 5 floors building known as the Academic Building [A] which is interconnected with another two floor building known as the Industrial Building [B]. Within our vision we have tried to keep track of the latest technologies built for the future but of course we have made a great deal of consideration to maintain a cost-effective design, thus ensuring a healthy network structure.

As we have said previously, since we do not have any kind of old network design, we made a plot for new network design for the whole institute based on maps and accurate measuring, where we had the aid of multiple applications to provide a clear and adequate defense.

Concerning our **Microwave Link** it will be based between **ITI** and the **General Directorate of Institutional and Industrial Education**, this link will be made up of three points which will mark the path of our link, this will have a whole part dedicated to it**.**

Our objective is to create a network that will provide a lot of facilities and new technological implementations that all who are part of the educational process will benefit from, namely the **Administration**, the **Teachers** and finally the **Students**.

Part I

ITI NETWORK INFRASTRUCTURE

Chapter I

Topologies and cables

A- TOPOLOGY

I-A-1- What does network topology mean?

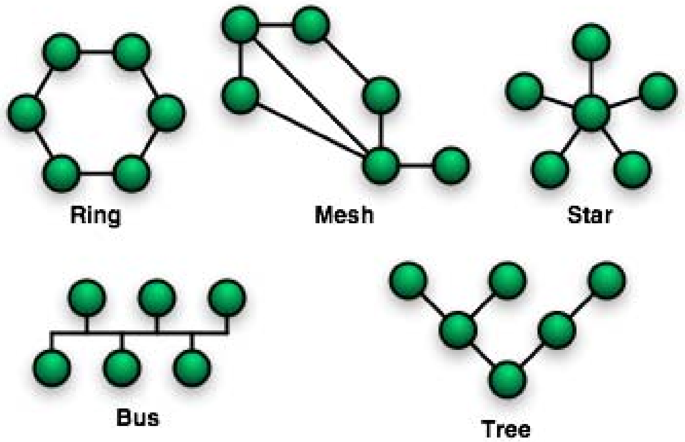
A network topology refers to either the physical or logical layout of a network installation.

Physical Topology when in the context of networking refers to the physical layout of the devices connected to the network, including the location and cable installation.

The Logical Topology refers to the way it actually operates (transfers data) as opposed to its layout.

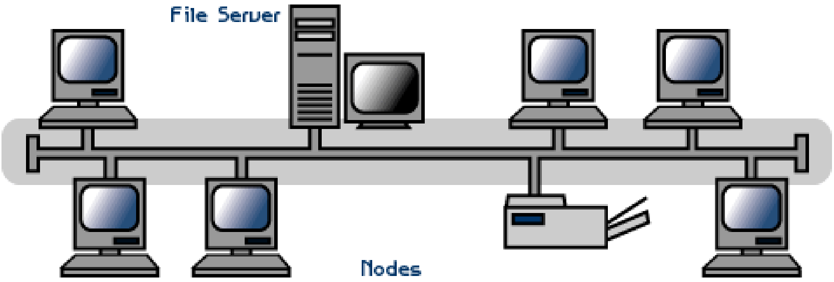
There are four main network topologies (and mixtures of the four) in common use today.

- Bus
- Star
- Tree
- Mesh
- Ring



We will take a closer look at these topologies below.

Linear Bus:



A linear bus topology consists of a main run of cable with a terminator at each end. All nodes (file server, workstations, and peripherals) are connected to the linear cable. Ethernet and LocalTalk networks use a linear bus topology. This topology is probably the cheapest network type of all to initially setup, as only one cable is used the installation is fairly simple and economical.

The problems can come when trying to add a device to an existing Bus topology network. To add a device requires physically linking it to the existing backbone which can turn out to be a major job. Another consideration if using a bus topology for a network is fault tolerance, or the lack of it, this type of network transfers data by passing messages through the same cable, so a break in any part of the cable will bring the whole network down.

Each device will check to see if the message is intended for them, the device to which the data is addressed will copy the contents to its network card's onboard RAM and process it accordingly.

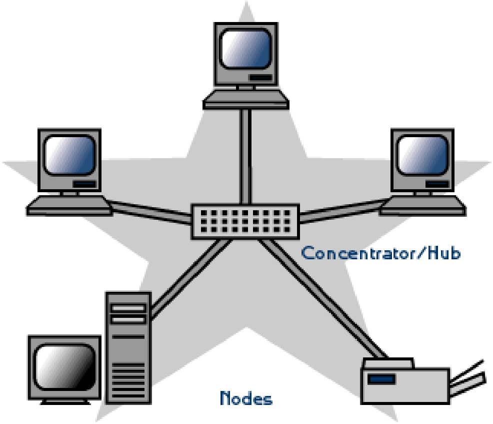
Advantages of a Linear Bus Topology

- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.

Disadvantages of a Linear Bus Topology

- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Not meant to be used as a stand-alone solution in a large building.

Star:



A star topology is designed with each node (file server, workstations, and peripherals) connected directly to a central network hub or concentrator.

Data on a star network passes through the hub or concentrator before continuing to its destination. The hub or concentrator manages and controls all functions of the network. It also acts as a repeater for the data flow. This configuration is common with twisted pair cable; however, it can also be used with coaxial cable or fiber optic cable.

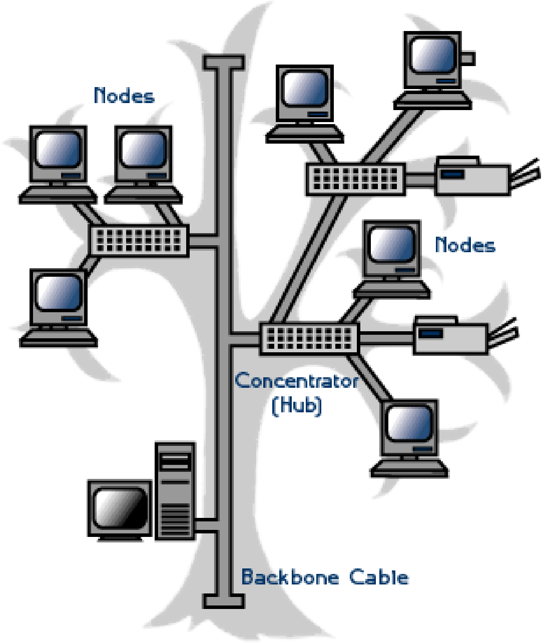
Advantages of a Star Topology

- Easy to install and wire.
- No disruptions to the network then connecting or removing devices.
- Easy to detect faults and to remove parts.

Disadvantages of a Star Topology

- Requires more cable length than a linear topology.
- If the hub or concentrator fails, nodes attached are disabled.
- More expensive than linear bus topologies because of the cost of the concentrators.

Tree:



A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable. Tree topologies allow for the expansion of an existing network, and enable schools to configure a network to meet their needs.

Tree topologies integrate multiple star topologies together onto a bus. Only the hub devices can connect directly with the tree bus and each Hub functions as a root of a tree of the network devices. This bus/star/hybrid combination supports future expandability of the computer networks, much better than a bus or star.

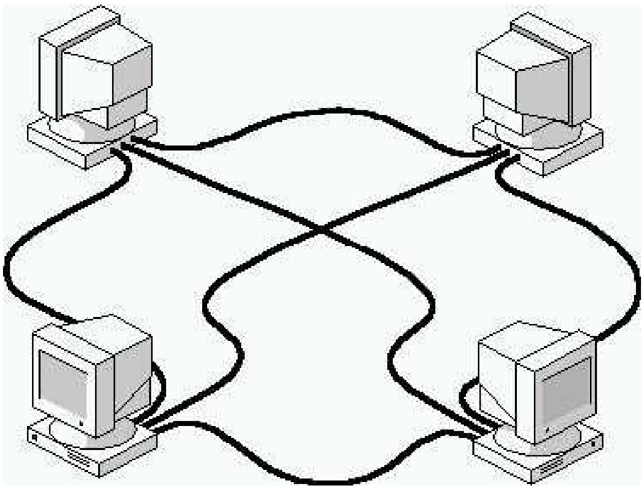
Advantages of a Tree Topology

- Point-to-point wiring for individual segments.
- Supported by several hardware and software venders.

Disadvantages of a Tree Topology

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.

Mesh:



Mesh topology work on the concept of routes. In Mesh topology, message sent to the destination can take any possible shortest, easiest route to reach its destination. In the previous topologies star and bus, messages are usually broadcasted to every computer, especially in bus topology. Similarly in the Ring topology message can travel in only one direction i.e clockwise or anticlockwise. Internet employs the Mesh topology and the message finds its route for its destination. Router works in find the routes for the messages and in reaching them to their destinations. The topology in which every device connects to every other device is called a full Mesh topology unlike in the partial mesh in which every device is indirectly connected to the other devices.

Advantages of a Mesh Topology

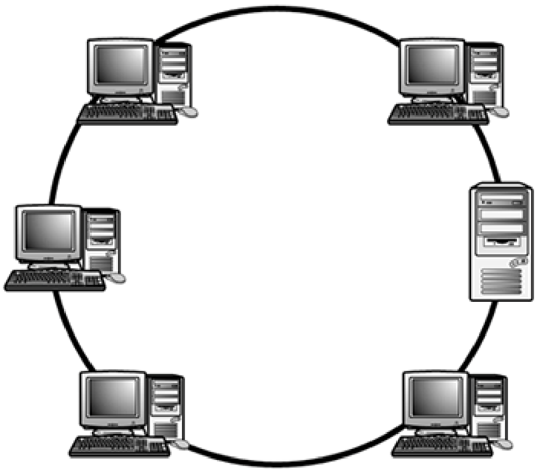
- The use of dedicated links guarantees that each connection can carry its data load, this eliminating the traffic problems that can occur when links must be shared by multiple devices.
- A mesh topology is robust. If one link becomes unusable, it does not halt the entire system.
- Excellent privacy and security.
- Point-To-Point links make fault identification and fault isolation easy.

Disadvantages of a Mesh Topology

- Impractical for large number of devices.
- Very expensive

- Installation and configuration are difficult
- The main disadvantages of a mesh are related to the amount of cabling and number of I/O ports required.

Ring:



The physical ring topology is rarely used these days, a Ring topology networks the devices by connecting each device to its two neighboring devices (see fig 1.3 below).

Diagram of a Ring Network Topology Data is passed one way from device to device, fault tolerance in a physical ring topology is non-existing, and if one device/cable fails then the whole network goes down.

Adding a new device to an existing physical Ring network can be complicated as any new device needs to go in between the existing devices.

Advantages of a Ring Topology

- Very orderly network where every device has access to the token and the opportunity to transmit
- Performs better than a star topology under heavy network load
- Can create much larger network using Token Ring
- Does not require network server to manage the connectivity between the computers

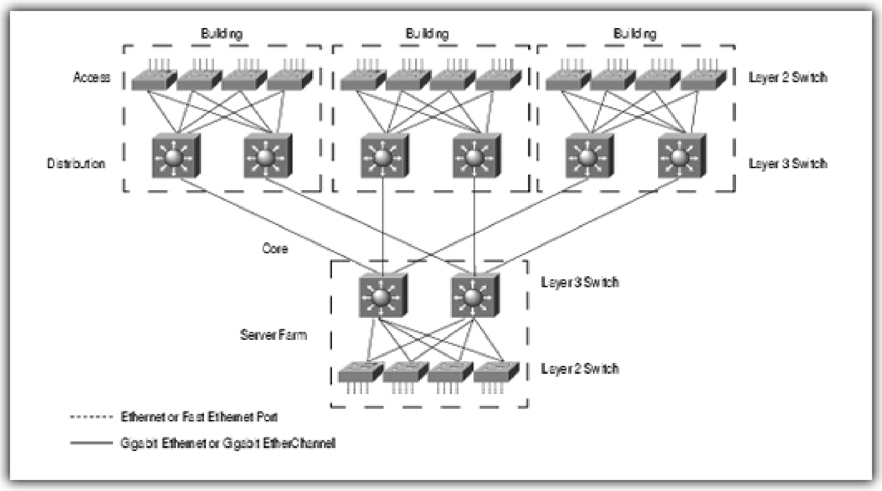
Disadvantages of a Ring Topology

- One malfunctioning workstation or bad port in the MAU can create problems for the entire network
- Moves, adds and changes of devices can affect the network
- Network adapter cards and MAU's are much more expensive than Ethernet cards and hubs
- Much slower than an Ethernet network under normal load.

I-A-2- Our Network Topology:

As a start we must bring to front the physical part of our project, and here are up against connecting two buildings one for academic studies and one for practical and technical applications. The academic building consists of four floors where we can find in the base floor the administration and going up through the first to the fourth are the classes and the labs within it.

Because we are organizing a whole new design for the network, each successful design must be based on an effective and almost fault free backbone, and here each building must have its own backbone that is interconnected with the other neighboring buildings. Here you must know that the industrial facility is surrounded with a lot of noise and contains a lot of equipment that can affect the wires and the transmission of any signal within its walls.



After thoroughly going through all of the existing topologies we have deiced to use the **mesh topology** which can give us the almost fault free result we require, but since we have no intention in increasing the redundancy on our backbone and for economic reasons it seems that using a type of mesh topology called **partial mesh** is even a more suitable to match what we seek, and as such a partial mesh topology is defined as a type of network topology in which some nodes are organized in a full mesh scheme but others are only connected to one or two in the network. Partial mesh topology is commonly found in peripheral networks connected to a full meshed backbone. It is **less expensive** to implement and yields **less redundancy** than full mesh topology.

Aspects to consider in our network design:

Nowadays with the fast and vast development of network technologies we must protect out network with some rules that can give us the leverage of total control on it. The most important facts that we should handle are **Scalability**, **Redundancy** and **Fault Tolerance**.

a) **Scalability:** because this network design is meant for institutional facilities so we are facing a numerous number of incoming points and nodes in accordance with the development of each building and its classes. In order to relief the network of some of the capacity required on the base level of it we need to do some offloading here. So the best schema would be to separate the backbone layer from the distribution layer from the clients layer, as such we can do any upgrade to our topology without having to break the connectivity of the clients also called downtime which costs a lot.

b) **Redundancy**: our design gains more of it power as it diminishes redundancy more and more, and that's why implementation of layers between the backbone and the client is very critical, in such a way that having a distribution layer based on switching technologies would give us the privilege of non-redundant loops in our network. Because we can't trust any circumstances that are hidden from us in the future everything has its own backup plan, so if a backbone switch fails secondary ones commence their work no problems faced, the same thing goes for the distribution switches and as a result we have strong layers that are dedicated to ensure that the client layer won't fail at anytime.

c) **Fault Tolerance:** it is very critical to be in control over all segments of the network so that to be able to overcome any dilemma or faults that will surely build up in the future, so by using some advanced technologies such as **Layer 3 Switching** we can corner any problem smoothly and resiliently.

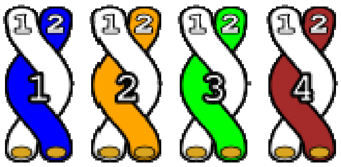
B- CABLES

I-B-1-Twister Pair Cables:

Twisted pair cabling is a form of wiring in which two conductors are wound together for the purposes of canceling out electromagnetic interference (EMI) from external sources, electromagnetic radiation from the UTP cable, and crosstalk between neighboring pairs.

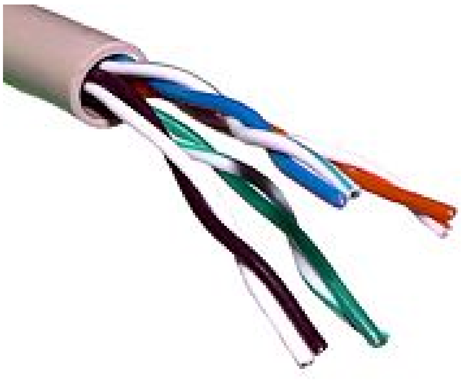
Twisting wires decreases interference because the loop area between the wires (which determines the magnetic coupling into the signal) is reduced. In balanced pair operation, the two wires typically carry equal and opposite signals (differential mode) which are combined by addition at the destination. The common-mode noise from the two wires (mostly) cancel each other in this addition because the two wires have similar amounts of EMI that are 180 degrees out of phase. This results in the same effect as subtraction. Differential mode also reduces electromagnetic radiation from the cable, along with the attenuation that it causes.

The twist rate (also called *pitch* of the twist, usually defined in twists per meter) makes up part of the specification for a given type of cable. Where pairs are not twisted, one member of the pair may be closer to the source than the other, and thus exposed to slightly different induced EMF.



Where twist rates are equal, the same conductors of different pairs may repeatedly lie next to each other, partially undoing the benefits of differential mode. For this reason it is commonly specified that, at least for cables containing small numbers of pairs, the twist rates must differ.

In contrast to **FTP** (foiled twisted pair) and **STP** (shielded twisted pair) cabling, **UTP** (unshielded twisted pair) cable is not surrounded by any shielding. It is the primary wire type for telephone usage and is very common for computer networking, especially as patch cables or temporary network connections due to the high flexibility of the cables.



Unshielded and shielded twisted pair cabling standards:

- **Cat 1**: Currently unrecognized by TIA/EIA. Previously used for POTS telephone communications, ISDN and doorbell wiring.
- **Cat 2**: Currently unrecognized by TIA/EIA. Previously was frequently used on 4 Mbit/s token ring networks.
- **Cat 3**: Currently defined in TIA/EIA-568-B, used for data networks using frequencies up to 16 MHz. Historically popular for 10 Mbit/s Ethernet networks.
- **Cat 4**: Currently unrecognized by TIA/EIA. Provided performance of up to 20 MHz, and was frequently used on 16 Mbit/s token ring networks.
- **Cat 5**: Currently unrecognized by TIA/EIA. Provided performance of up to 100 MHz, and was frequently used on 100 Mbit/s Ethernet networks. May be unsuitable for 1000BASE-T gigabit Ethernet.
- **Cat 5e**: Currently defined in TIA/EIA-568-B. Provides performance of up to 100 MHz, and is frequently used for both 100 Mbit/s and gigabit Ethernet networks.
- **Cat 6**: Currently defined in TIA/EIA-568-B. It provides performance of up to 250 MHz, more than double category 5 and 5e.
- **Cat 6a**: Future specification for 10 Gbit/s applications.
- **Cat 7**: An informal name applied to ISO/IEC 11801 Class F cabling. This standard specifies four individually-shielded pairs (STP) inside an overall shield. Designed for transmission at frequencies up to 600 MHz.

Advantages

- It is a thin, flexible cable that is easy to string between walls.
- Because UTP is small, it does not quickly fill up wiring ducts.
- UTP costs less per foot than any other type of LAN cable.

Disadvantages

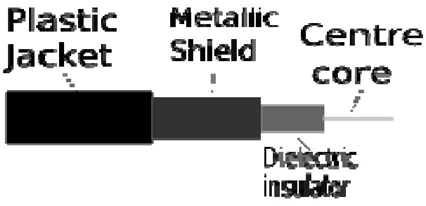
- Twisted pair's susceptibility to the electromagnetic interference greatly depends on the pair twisting schemes (usually patented by the manufacturers) staying intact during the installation. As a result, twisted pair cables usually have stringent requirements for maximum pulling tension as well as minimum bend radius. This relative fragility of twisted pair cables makes the installation practices an important part of ensuring the cable's performance.

I-B-2-Coaxial Cable

Coaxial cable is an electrical cable consisting of an inner conductor or several un-insulated conductors tightly twisted together, often surrounded by an insulating spacer, surrounded by an outer cylindrical conducting shield (sheath), and usually surrounded by a final insulating layer (jacket). The term coaxial comes from the inner conductor and the outer shield sharing ("co-") the same axis. It is often used as a high-frequency transmission line to carry a high-frequency or broadband signal but may also be used for frequencies as low as audio frequency. The electromagnetic field carrying the signal exists (ideally) only in the space between the inner and outer conductors. The shielding reduces interference from external electromagnetic fields, although coax cable does radiate energy, shielding does somewhat reduce the possibility of a transmitting device causing undesired interference through transmission line leakage.

The construction of coaxial cables varies substantially. Design choices affect the size, flexibility, and loss characteristics of the cable. The inner conductor might be a solid wire or stranded.

To get better high-frequency performance, the inner conductor may be silver plated. Sometimes copper-plated iron wire is used as an inner conductor. The insulator surrounding the inner conductor also has variations. The insulator is a dielectric, and the properties of dielectric control some electrical properties of the cable



A common choice is a solid polyethylene (PE) insulator. Lower-loss cables will use a polyethylene foam insulator. Solid Teflon is also used as an insulator. Some coaxial lines use air (or some other gas) and have spacers to keep the inner conductor from touching the shield.

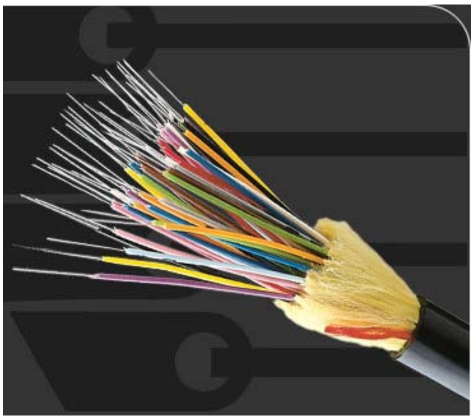
There is also a lot of variety in the shield. Convention coaxial cable had braided copper wire forming the shield. That allowed the cable to be flexible, but it also means there are gaps in the shield layer. It also means the inner dimension of the shield varies slightly because the braid cannot be flat. Sometimes the braid is silver plated. For better shield performance, some cables have a double-layer shield. The shield might be just two braids, but it is more common now to have a thin foil shield covered by a wire braid. Some cables may invest in more than two shield layers. Other shield designs sacrifice flexibility for better performance; some shields are a solid metal tube. Those cables cannot take sharp bends: the shield kinks. Many CATV distribution systems used such cables.

The insulating jacket can be made from many materials. A common choice is PVC, but applications may require fire-resistant materials. Outdoor applications may require the jacket to resist ultraviolet light and oxidation. For internal chassis connections the insulating jacket may be omitted.

I-B-3-Optical Fiber Cables

An optical fiber (or fibre) is a glass or plastic fiber designed to guide light along its length. Fiber optics is the overlap of applied science and engineering concerned with the design and application of optical fibers. Optical fibers are widely used in fiber-optic communication, which permits transmission over longer distances and at higher data rates than other forms of communications. Fibers are used instead of metal wires because signals travel along them with less loss, and they are immune to electromagnetic interference. Optical fibers are also used to form sensors, and in a variety of other applications.

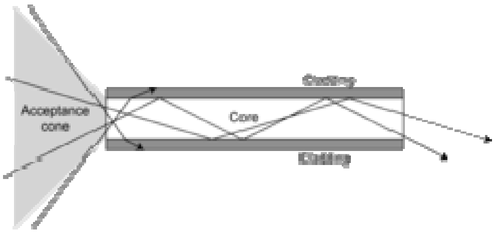
Light is kept in the "core" of the optical fiber by total internal reflection. This causes the fiber to act as a waveguide. Fibers which support many propagation paths or transverse modes are called multimode fibers (MMF). Fibers which support only a single mode are called singlemode fibers (SMF). Multimode fibers generally have a large-diameter core, and are used for short-distance communication links or for applications where high power must be transmitted. Singlemode fibers are used for most communication links longer than 200 meters.



Joining lengths of optical fiber is more complex than joining electrical wire or cable. The ends of the fibers must be carefully cleaved, and then spliced together either mechanically or by fusing them together with an electric arc. Special connectors are used to make removable connections.

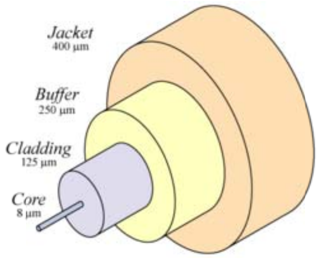
An optical fiber is a cylindrical dielectric waveguide that transmits light along its axis, by the process of total internal reflection. The fiber consists of a *core* surrounded by a cladding layer. To confine the optical signal in the core, the refractive index of the core must be greater than that of the cladding. The boundary between the core and cladding may either be abrupt, in *step-index fiber*, or gradual, in *graded-index fiber*.

Multi-mode fiber:



Fiber with large (greater than 10 µm) core diameter may be analyzed by geometric optics. Such fiber is called *multimode fiber*, from the electromagnetic analysis (see below). In a step-index multimode fiber, rays of light are guided along the fiber core by total internal reflection. Rays that meet the core-cladding boundary at a high angle (measured relative to a line normal to the boundary), greater than the critical angle for this boundary, are completely reflected. The critical angle (minimum angle for total internal reflection) is determined by the difference in index of refraction between the core and cladding materials. Rays that meet the boundary at a low angle are refracted from the core into the cladding, and do not convey light and hence information along the fiber. The critical angle determines the acceptance angle of the fiber, often reported as a numerical aperture. A high numerical aperture allows light to propagate down the fiber in rays both close to the axis and at various angles, allowing efficient coupling of light into the fiber. However, this high numerical aperture increases the amount of dispersion as rays at different angles have different path lengths and therefore take different times to traverse the fiber. A low numerical aperture may therefore be desirable.

Single-mode Fiber:



Fiber with a core diameter less than about ten times the wavelength of the propagating light cannot be modeled using geometric optics. Instead, it must be analyzed as an electromagnetic structure, by solution of Maxwell's equations as reduced to the electromagnetic wave equation. The electromagnetic analysis may also be required to understand behaviors such as speckle that occur when coherent light propagates in multi-mode fiber. As an optical waveguide, the fiber supports one or more confined transverse modes by which light can propagate along the fiber. Fiber supporting only one mode is called single-mode or *mono-mode* fiber. The behavior of larger-core multimode fiber can also be modeled using the wave equation, which shows that such fiber supports more than one mode of propagation (hence the name). The results of such modeling of multi-mode fiber approximately agree with the predictions of geometric optics, if the fiber core is large enough to support more than a few modes.

I-B-4-Cabling in our design:

The physical infrastructure of cabling is divided into two major sections **Backbone Cabling**, **Horizontal Cabling** where the horizontal part includes **Work Area Cabling**; in addition to the **Outside Cabling** all of them have their own special type of cables and characteristics that will be stated in specific later on.

Backbone Cabling:

The backbone cabling system provides interconnections between telecommunications rooms, equipment rooms, main terminal space, and entrance facilities. It includes backbone cables, intermediate and main cross-connects mechanical terminations, and patch cords or jumpers used for backbone-to-backbone cross-connections. The backbone also extends between buildings in a campus environment.

- Equipment connections to backbone cabling should be made with cable lengths of 30m (98 ft.) or less.
- The backbone cabling shall be configured in either star, mesh or partial-mesh topologies. Each horizontal cross-connect is connected directly to a main cross-connect or to an intermediate cross-connect, then to a main cross-connect.
- The backbone is limited to no more than two hierarchical levels of cross-connects (main and intermediate). No more than one cross-connect may exist between a main and a horizontal cross-connect and no more than three cross-connects may exist between any two horizontal cross connects.
- A total maximum backbone distance of 90m (295 ft.) is specified for high bandwidth capability over copper. This distance is for uninterrupted backbone runs. (No intermediate cross-connect).

- The distance between the terminations in the entrance facility and the main cross-connect shall be documented and should be made available to the service provider.
- Recognized media may be used individually or in combination, as required by the installation. Quantity of pairs and fibers needed in individual backbone runs depends on the area served.

Topology used: as we have previously stated that our backbone relies on the partial mesh topology which gives use aspects of control of leverage over our network.

Cables used:

- **Multimode Fiber** 62.5/125 micron code/cladding, enhanced grade, graded index glass fiber.
- **Single Mode Fiber** 8.3/125 micron code/cladding, enhanced grade, graded index glass fiber.

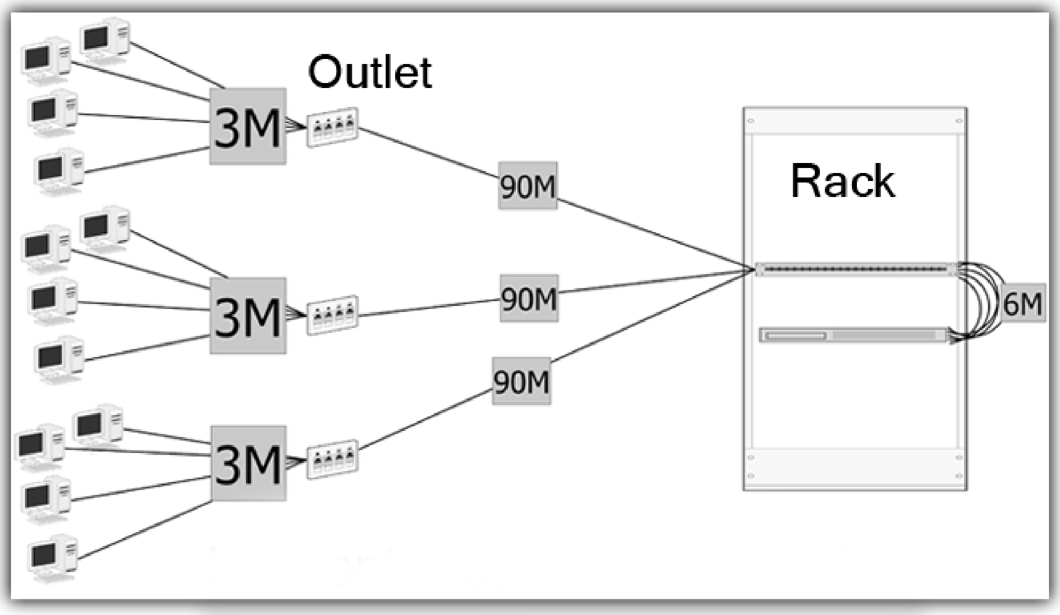
Horizontal Cabling:

The horizontal cabling system extends from the telecommunications outlet in the work area to the horizontal cross-connect in the telecommunications room. It includes the telecommunications outlet, an optional consolidation point or transition point connector, horizontal cable, and the mechanical terminations and patch cords (or jumpers) that comprise the horizontal cross-connect. An allowance of 10m (33 ft.) has been provided for the combined length of patch cords/cross-connect jumpers and equipment cables/cords in the HC, including the WA equipment cords.

- A minimum of two telecommunications outlets are required for each individual work area. First outlet: 100 Ω twisted-pair (category 6 is recommended). Second outlet: 100 Ω twisted-pair or two-fiber multimode optical fiber either 62.5/125µm or 50/125µm.
- Additional outlets may be provided. These outlets are in addition to, and may not replace, the minimum requirements of the standard.
- Bridged taps and splices are not allowed for copper-based horizontal cabling. (Fiber splices are allowed for fiber optic cables.)
- Application specific components shall not be installed as part of the horizontal cabling. When needed, they must be placed external to the telecommunications outlet or horizontal cross connect.
- The proximity of horizontal cabling to sources of electromagnetic interference (EMI) shall be taken into account.

Horizontal Cabling Standards: Horizontal cabling must apply a certain length standards that were based upon the capabilities of the cables and their positions as shown in the following figure.

Topology: this part of our network shall be based on a **Star** topology.



Horizontal cabling is a subject of the following measurements and lengths which is limited as we can see in the above image and according to the following:

- Each cable from each node to the nearby outlet must not exceed **3 meters**.
- Each cable from the outlet to the patch panel must not exceed **90 meters**.
- Each cable from the patch panel to the switch must not exceed **6 meters**.

Cables used:

- **Unshielded Twisted Pair (UTP)** cable – 100**Ohms** (**+ -** 15% at 1MHz to 100Mhz)
- **Shielded Twisted Pair (STP)** cable – 100**Ohms** (**+ -** 15% at 1MHz to 100MHz)

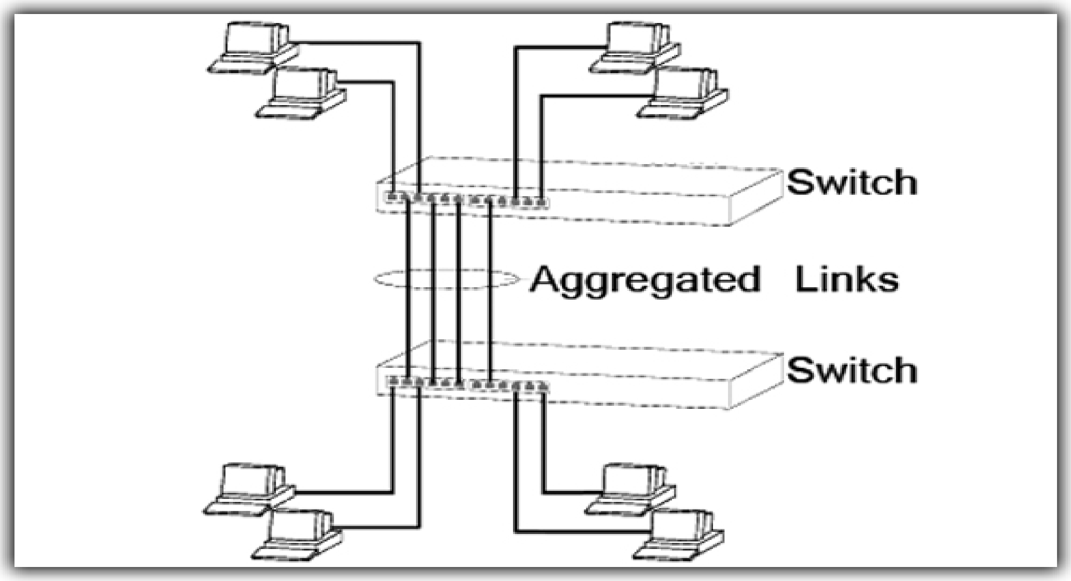
Chapter II

Network Devices and Technologies

II- Network Infrastructure Layers and Components:

Link aggregation is the bonding together of two or more data channels into a single channel that appears as a single, higher-bandwidth logical link. Aggregated links also provide redundancy and fault tolerance if each of the aggregated links follows a different physical path. Link aggregation may be used to improve access to public networks by aggregating modem links or digital lines. Link aggregation may also be used in the enterprise network to build multigigabit backbone links between Gigabit Ethernet switches.

Link aggregation is sometimes referred to as load balancing since traffic loads are distributed across multiple links. However, load balancing is also a data center technique in which incoming requests from clients are distributed to two or more servers.



Aggregation is sometimes called *inverse multiplexing* or *IMUX.*

Since we have adopted the 3Com technology in our infrastructure it provided us with the capability of implementing a newer technology called **XRN Stacking**.

XRN technology enables multiple interconnected **Gigabit switches** to behave as a single management switching entity, across Layer 2 and Layer 3, acting together to form a Distributed Fabric. XRN technology logically binds all the functions, performance and resilience together, allowing stackable switches to act like a chassis. And, while traditional solutions offer little more than **Distributed Device Management** (DDM) for stacking, 3Com XRN technology consists of the following three main technical components, which help companies to minimize their overall resource requirements and reduce associated costs:

- **Distributed Device Management (DDM)** – enables the multiple switches in an XRN stack to operate as if they were a single device on the network. DDM lets customers configure and manage all ports and devices in the XRN fabric as a single entity via the command line interface (CLI), web interface, or simple network management protocol (SNMP). In the event of a failure in one of the switches, management access to the remaining switch is retained on the same Internet Protocol (IP) address.
- **Distributed Link Aggregations (DLA)** – allows wiring closet switches or hosts to create an aggregated link that is dual-homed across the switches in the XRN fabric. If a port in the aggregated link fails, traffic is forwarded via the remaining ports. DLA provides intelligent local forwarding, enabling each switch in the fabric to make its own forwarding decisions without sending traffic across the aggregated link. Features such as DLA enable companies to make sure that their networks continue to operate in the event of equipment or cabling failures. DLA also allows managers to schedule maintenance during planned times that are least disruptive to the company's operations, rather than undertaking costly emergency repairs during peak times.
- **Distributed Resilient Routing (DRR)** – lets all switches in the XRN fabric act as a single logical router. The switches use the same router interfaces and mirror each other's routing tables. This protects the network against unit failure and enables each switch to locally route traffic for greater Layer 3 forwarding performance. Using DRR functionality allows managers to configure routing for a stack of switches so that multiple switches can function as a single routing engine. DRR significantly reduces the overall complexity related to configuring separate routers. It also helps to ensure that there are fewer network issues resulting from miss-configurations. In order to realize the above-mentioned attributes, all members of the XRN stack must be joined together via special stacking-enabled connections.
- **Resilient links**: they are a feature unique to 3Com Ethernet Campus Solutions. They safeguard

against device or link failure. Resilient links provide secondary back-up links that take over traffic should a primary link fail. They are available for Ethernet, Fast Ethernet and Gigabit Ethernet. We will be automatically notified whenever a secondary link is activated. Resilient links provide effective protection in critical areas of our LAN, such as between the switches in our wiring closets and the data center. Additionally, 3Com Fast Ether-Link Server NICs provide resilient links between switches and my key servers. Depending on the protection we need, we deploy resilient links in either single-homed or dual homed configurations. In a single-homed configuration, there is a primary link and a secondary link between two switches or a server and a switch. This protects against failure of the primary link or an interface, but not against device failure. For additional security, we use a dual-homed configuration. Here, the secondary link is installed on a third device. Should one of the first two devices fail, traffic is automatically routed to the third over the backup link. As a result, I'm ensured that any problems will not disrupt my users or their traffic.

The campus of the institute includes two buildings each having different infrastructure layers with separate equipment for each. The layers are divided into three categories: **Core Layer**, **Distribution Layer** and **Access Layer**.

Next Generation Switches:

These next-generation Layer 2/3/4, Fast Ethernet and Gigabit Ethernet switches can be deployed at the network edge, for distribution, or small core switching. They offer flexible and scalable connectivity for a heterogeneous mix of data, voice, video, and other business-critical services and are particularly suited for building highly available and resilient architectures.

All switches share the same operating system as our premium modular switches and routers. This permits you to manage an entire distributed switching and routing infrastructure from a single CLI or SNMP management platform.

Fast Ethernet 10/100 models deliver premium levels of performance, security and reliability for robust switching at the enterprise network edge.

Gigabit 10/100/1000 models offer industry-leading stackable performance and features for Gigabit-to-the-desktop, distribution and stackable core deployments.

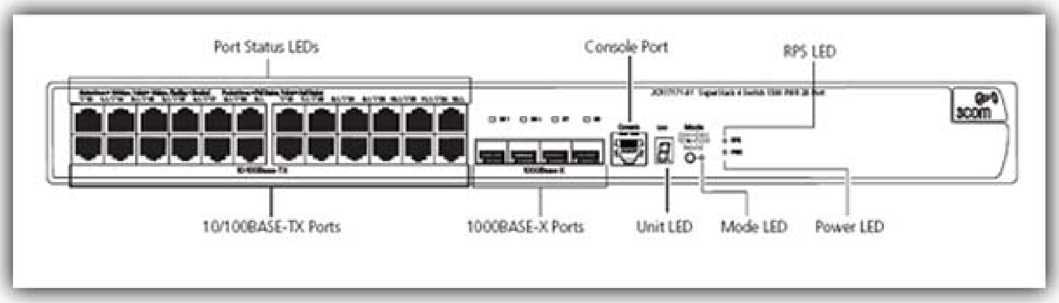
Core Layer:

Equipment (Components):

3Com® Switch 5500-EI (premium stackable switches):

The 3Com Switch 5500-EI 28-Port FX is a premium stackable Fast Ethernet SFP-based fiber switch with Enhanced Image (EI) software for businesses running the most demanding network applications requiring the highest "five 9s" network uptime.

24 SFP ports, to be populated with 100BASE-X SFP transceivers with multi- or single-mode connectors, provide Fast Ethernet fiber connections. Two Gigabit SFP ports and two 10/100/1000 ports are available for stacking, inter-switch connections, and/or uplinks to the network core.



The Switch 5500-EI supports distributed, resilient 3Com XRN® Stacking Technology and advanced Layer 3 (RIP / OSPF) routing, Layer 2-4 QoS, and rate limiting features.

This switch provides extensive security features—SNMP v3, SSH, network login—and resilient hot-swap stacking for simplified management and monitoring.

• 24 SFP ports, to be populated with 100BASE-X SFP transceivers with multi- or single-mode connectors; 2 Gigabit SFP and 2 10/100/1000 ports.	• Scalable stackable design with resilient stacking up to eight units high, or 384 Fast Ethernet ports using 2 Gbps stacking bandwidth (4Gbps full duplex).
• Available DC Redundant Power Supply (RPS), designed by Eaton Powerware Corporation, a leading provider of integrated power systems.	• Wirespeed performance across all ports within a stack delivers optimal throughputs and bandwidth for business-critical data and high-speed communications.
• Load-sharing and cross-stack trunking features help eliminate dropped packets, clear up traffic bottlenecks, and improve server availability	• Shared 3Com Operating System consolidates administrative control over the entire switching infrastructure—providing unparalleled edge-to-core visibility and control.
• Advanced, time-based Access Control Lists (ACLs) help safeguard key network resources from unauthorized access and data corruption.	• User-based authentication and DES 56-bit or 168-bit encryption help secure Layer 3 protocols and management controls.
• 3Com XRN® Stacking Technology provides for the creation of eight-unit stacks that offer chassis-like availability and resiliency over traditional aggregated-trunk configurations.	• Built-in support for AC- and DC-powered operations enables you to leverage existing power schemes and cost-effectively extend power to the edge of the network.
• Integrated distributed security enforcement.	• 12.8 Gbps switching capacity, 9.5 Mpps forwarding rate, maximum.

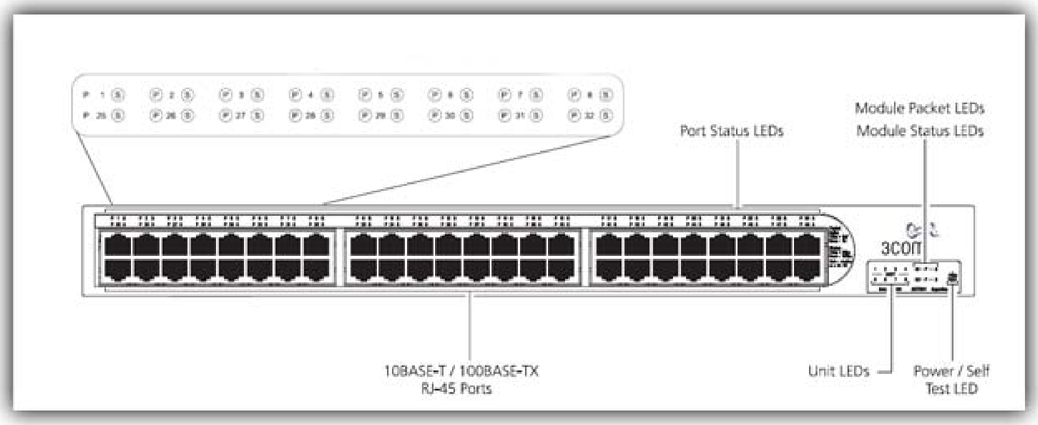
Distribution Layer:

Equipment (Switches):

The 3Com® SuperStack® 3 Switch 4400 also helps increase network availability and reliability. The switch optimizes and controls data flow through the use of advanced quality of service, helping to ensure that mission-critical traffic reaches the intended users every time.

Rapid Spanning Tree, stack-wide trunking, resilient stacking, link aggregation and built-in redundant power supply support deliver robust performance and fault tolerance.

Optional switching modules provide resilient high-speed connections such as Fast Ethernet, including 100BASE-LX (Ethernet in the First Mile), and Gigabit Ethernet copper or fiber links.



• User network login with IEEE 802.1X and RADIUS, combined with RADIUS Authenticated Device Access (RADA), based on MAC address, provide secure network access control at the network edge	• Authenticated users can be automatically placed into a specific VLAN, restricting access only to the data needed
• Secure Shell (SSH) encryption of login passwords, management VLANs, and management station "trusted IP address" lists help protect network from rogue management threats	• LACP (IEEE 802.3ad) intelligently detects configuration duplicity and uses it to trunk up to 4Gb of bandwidth across a stack, while nullifying single points of failure from the network's edge infrastructure
• Advanced Layer 4 functionality identifies and prioritizes real-time or business-critical applications such as enterprise resource planning (ERP) systems, LAN telephony, and video streaming	• Add optional switching modules to provide resilient high-speed connections, such as Gigabit Ethernet backbone links, or 100BASE-LX 10 links for Ethernet in First Mile over Point to Point Fiber (EFMF)
• Backup and restore functionality enables switch configurations to be captured and reapplied individually to a single switch or across a whole network at a push of a button	• Forwarding up to 10.1 million pps, with a massive switching fabric of 13.6 Gbps, provides industry-leading performance
• Mix and match 24-port and 48-port SuperStack 3 Switch 4400s to create a resilient stack of up to a total of 384 10/100 connections	• Stackable architecture increases scalability and allows high-speed trunks between workgroup and other resources
• 3Com Network Supervisor 3.0 software (60-day trial included) supports automatic prioritization of real-time or critical traffic	• Resilient hot-swappable stacking and network connections enhance network availability and usability

Access Layer:

Each floor will have in it a number of classrooms and might include some laboratories; each lab will have an average of 20PCs thus we will use layer 2 switches to connect these PCs to the IDF rather than putting them within the IDF which will save us a lot of cables and effort and as such we have chosen 3Com Baseline Switch 2126-G 24 ports and 3Com Baseline Switch 2126-G 48 ports. On the other hand each classroom will have a PC for the use by teachers so they will be directly connected to the switch in the distribution layer to as an Access Layer switch for those computers.

3Com Baseline Switch 2126-G 24-Port and 3Com Switch Baseline Switch 2126-G 48-Ports:

The 3Com® Baseline Switch 2126-G is an unmanaged, fixed configuration Layer 2 Switch with 24 10/100 ports and two copper 10/100/1000 uplinks, designed for small to midsize offices. This rack mountable, business-class switch can be installed in a wiring closet or as a free-standing unit.	The switch comes preconfigured for fast, easy installation using economical copper wiring. Auto-negotiation adjusts the port speed to match the communicating device. To simplify cable connections, all 26 ports come with automatic detection of the Ethernet cable type (MDI/MDIX).
Like all 3Com Baseline products, this switch provides powerful practicality in a sturdy package designed for reliability, long life, and low total cost of ownership.	

Internet connection used:

According to our statistics of internet usage at the institute we have come up with a plan that suits our needs and copes with the budget. The connection will be **HDSL** which is the equivalent of a **1024Kbit/sec** download speed and upload speed of **512Kbit/sec** and to back up our theory we based this decision on the fact that:

1- Computer labs will be provided internet access for **researching**.
2- Teachers will be the only ones with access for **download stream**.
3- A good speed connection is required for **online exams**.
4- A good speed connection is required for **updating the institute's website**.
5- It is critical to have a good internet connection that provides **real time remote access** to the hardware in order to **troubleshoot** and **monitor** any problem that occurs in the network at anytime.

Our internet service provider (ISP) will be OGERO Telecom which is the nearest to the facilities and do not require a lot of equipment to connect.

Internet connection hardware:

3Com Router 3000 for **DSL** and **Ethernet**, The 3Com Router 3000 DSL and Ethernet Family provides all of the components needed to give remote office and tele-workers secure, reliable, cost-effective access to the Internet or corporate networks over a DSL connection.

The **3Com Router 3000** includes a four-port switch for local LAN connections; consisting of a 64MB DRAM, 8MB flash memory, and operating software support a full complement of routing, integrated

security, and quality of service features required by today's remote office.

The **3Com Router 3000** is equipped with a full complement of memory and routing functionality; there are no hardware, memory or software upgrades required or available—everything a business needs is included with the base system.

The **3Com Router 3000** supports the standards based routing: choice of ADSL over analog POTS, ADSL/ADSL2/ADSL2+ over analog POTS, ADSL over ISDN, or G.SHDSL; available ISDN BRI S/T dial backup; IP, RIP v1 and v2, OSPF.

Chapter III

Infrastructure Network Design

III-1- Network Architecture Applied:

The following are the network maps from the institute's building with everything applied to them in detail.

III-2- Rooms and Racks:

Telecommunication Rooms (TR - IDFs/MDFs) Location:

IDF - Intermediate Distribution Frame: Located in a central office or customer premises, a frame that cross-connects the user cable media to individual user line circuits and may serve as a distribution point for multi-pair cables from the main distribution frame (MDF) or combined distribution frame (CDF) to individual cables connected to equipment in areas remote from these frames.

Using common sense and relying on the floor plans of each building we have chosen to place our IDFs in a midpoint at each floor in order to have more flexibility in cabling and troubleshooting. Also you must know that all the IDFs are vertically symmetrical to each other since they are all in the same location at each floor.

MDF – Main Distribution Frame: In telecommunication, Main Distribution Frame (MDF) is a distribution frame on one part of which the external trunk cables entering a facility terminate, and on another part of which the internal user subscriber lines and trunk cabling to any intermediate distribution frames terminate. MDF is a cable rack that interconnects and manages the telecommunications wiring between itself and any number of IDFs (Intermediate distribution frame), which connects internal lines to the MDF.

In both building we have chosen to locate our MDF in the base floor because of its significance to all other floors as shown in the maps.

The Academic building's MDF consists of a rack that contains two patch panels, a small sized one for the UTP cables and a midsized one for the fiber optic cables. In addition we have two identical switches 3Com 3 Switch 5500 EI FX / 28 Ports, 24 fiber optic ports and 4 10/100/1000

UTP ports one for actual usage and another for backup/aggregation where the two switches will be connected to each other by two fiber optic cables.

Server Room: Since all the servers should be connected to high speed link we have chosen to deliver them to the MDF through two high speed gigabit switches provided by 3Com, the reason for the two switches is for aggregation.

3Com® Gigabit Switch 8 is designed for small offices and remote branch offices requiring high network performance to exchange large data files and images, and access real-time information or connect to high-speed servers or a high-speed network backbone.

The 3Com Gigabit Switch 8 automatically finds the fastest connection speed, the autosensing 10/100/1000 ports automatically adjust to the speed of network devices communicating at 1000, 100, or 10 Mbps, so the switch can accommodate a range of workgroup applications. All that is needed is to connect the power and Ethernet cables.

Auto-speed sensing 10/100/1000 Mbps connectivity enables connection at 1000 Mbps, 100 Mbps and 10 Mbps, ensuring optimum throughput for bandwidth intensive applications and compatibility with legacy equipment.

III-3- Onsite Infrastructure Planning:

III-3-1- Building [A] Academic:

The building is made up of four floors plus one base floor; on one hand each floor has its own specific room divisions, on the other hand you can find that all the floors have common location for the IDF which is located in a separate room that can reach out to the whole building. Moreover since we plan on installing a microwave radio based link between ITI and Dikoueneh we are going to use the roof as well in this architecture.

A) Base Floor [Administration]: This floor is divided into 10 rooms excluding the MDF, IDF and Servers room; most of the rooms such as 2,4,8,10,5,7 and 9 have one administration personnel operating in them so a single computer was placed for each, along you can notice that there is a room for the teachers to confer and prepare their course materials so we have placed a sum of 5 computers in room 6 to meet their needs. Room 1 and 3 are special case rooms because they are for ITI head administration where the first room is for the secretaries and registrations where there is about 3 personnel working in that room so 3 computers were installed there, directly facing the secretary’s room you can notice a wide room and that’s the room of the director of the institute, so we have placed two computers in that room where the first is for his personal usage and the other is for usage when conferring with other academic parties.

The other three rooms that exist in this level are the IDF, MDF and the Servers room which we have talked about earlier, because we have a single almost a single computer in each office so we decided that there is no need for switches and thus they are connected directly to the IDF, the Servers room is connected directly to the MDF.

Wi-Fi:

The administration floor will be provided with wireless access to our network in order to facilitate access to Wi-Fi supported devices such as laptops. And as such, we need a wireless access point, so we got a 3Com access point and an additional 8dB antenna to gives us a wider range of coverage and a good strength of signal.

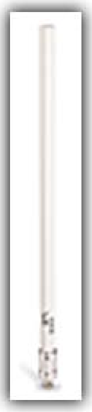
3Com® Wireless 8760 Dual-Radio 11a/b/g PoE Access Point:

It is a cost-effective dual-band, Power over Ethernet (PoE) wireless solution for enterprises of all sizes. This access point is a fully-featured dual-radio access point that functions simultaneously with an 802.11b/g and an 802.11a radio. Providing ultra-fast speed of up to 108 Mbps in turbo mode this access point supports up to 64 wireless users per radio, a total of up to 128 wireless users in all leaving plenty of room for growth.

PoE support overcomes installation problems by eliminating the need for an AC power plug at each AP. The 3Com Switch 5500-EI PWR, 3Com Baseline Switch 2226- PWR Plus or other IEEE 802.3af-compliant PoE products can supply both power and data to the access points through Category 5 or 6 Ethernet cabling, giving you flexible installation options in hard to wire or reach locations. For convenience a PoE adapter is supplied with the unit.

3Com® 8dBi Dual-Band Omni Antenna:

This antenna is ideal for midrange, point-to-multipoint connections with indoor building-to-building bridges. The antenna also increases the coverage area of 3Com enterprise wireless LAN (WLAN) access points with removable antennas. Omni-directional antenna provides uniform coverage in all directions in large open areas



Wireless Configuration:
SSID: ITIAdmin
Signal Encryption: WEP
Data Encryption: 128bits
WEP Mode: HEX
WEP Key: A105FC4A7B
Power: Standard
IP Address: 172.16.64.12

Administrator Configuration:
Admin Username: ITIAdmin
Console Password: 1pN3t*!

MAC Address Control: 00 E2 AF 7B 3B 3P

Switches used:

For the IDF we used 3Com SuperStack 3 Switch 4400 / 24 ports, and this was chosen relying on the number of PCs which is 17. The Servers will be connected to the MDF through a 3Com Gigabit Switch with 8 ports 10/100/1000 Mbps. The MDF contains two switch 3 5500-EI from 3Com.

B) First Floor: This floor is not much of a trouble since it hold only one lab that is connected to the IDF through a switch, all other 12 class rooms have a single computer for the teacher and it is connected directly to the IDF. The room of the principle contains two computers that are directly connected to the IDF.

Switches used:

Since the lab has many computers we are going to use layer2 3Com Baseline Switch 2126-G 24 port, and SuperStack 3 Switch 4400 / 24 ports for the IDF as well.

C) Second Floor: The floor is the heavy duty level because 90% of the laboratories are placed in it, a sum of 6 labs with a minimum of 16 PCs and a maximum of 25 PCs for a single lab including the teachers PC. More over we have 6 class rooms with a single PC in each, and there exists two rooms the first for the principle with three PCs and the second the director of laboratories with two PCs.

Switches used:

Not Like all other floors the IDF will hold one switch SuperStack 3 Switch 4400 / 48 ports since we have a huge number of PCs and switches connected to it, to avoid the cabling mess and for financial assessment reasons we have chosen to put in each lab a layer 2 switch while here we have a diversity in the labs in such a way that some has more PCs than others, as you can notice on the map labs 1,5,9 and 11 are choking with PCs and since there might be more additions in the future we have put a 3Com Baseline Switch 2126-G 48 port in the labs, one the other hand labs 3 and 9 will be equipped with a 3Com Baseline Switch 2126-G 24 ports.

D) Third Floor: You can see in this floor we do not have such pressure on the network, we have 10 class rooms with a single computer for the teacher, a room for the principle with two PCs and the major feature of this level which is the library which has 6 PCs for the scholars to research and reading and an additional PC for the librarian.

Switches used:

Here we have two switches, a SuperStack 3 Switch 4400 / 24 ports in the IDF and the second will be switch 3Com Baseline Switch 2126-G 24-Port which is used in the library room.

E) Fourth Floor: This level of the building has 13 class rooms with a PC in each for the teacher, and a single lab with 19 PCs including the teacher's PC. The principle's room has two PCs in it.

Switches used:

The IDF has a SuperStack 3 Switch 4400 / 24 ports, and the lab's switch is 3Com Baseline Switch 2126-G 24-Port.

Backbone: we will from each IDF two multimode fiber optic cables directly to the 5500 switch in the MDF which will represent our backbone, the reason for two the two cables is redundancy and for aggregation.

III-3-2-Building [B] Industrial:

The industrial facility in a huge cubical building that is divided into two floors, the base floor which has all the industrial labs and the first floor that holds within the classes and administration rooms.

A) Base Floor: each lab has two PCs in it and all the PCs are connected directly to the IDF since there is no need to put a switch between them because of the low number of PCs used here.

Switches used:

For the IDF we are going to use a SuperStack 3 Switch 4400 / 24 ports, and for the MDF we will use the same SuperStack 3 Switch 4400 / 24 ports since the number of PCs is not that vast and we do not have that much of bandwidth consumption so rather than getting a 5500 switch we used this one and we are going to add to it a module that supports fiber optics for the building-to-building link.

B) First Floor: each class room will have a single PC for use by teachers and they are directly connected to the IDF.

Switches used:

We are going to use a SuperStack 3 Switch 4400 / 24 ports for the IDF.

Backbone: we will from each IDF two multimode fiber optic cables directly to the 4400 switch in the MDF which will represent our backbone, the reason for two the two cables is redundancy and for aggregation.

III-3-3-Actual Building Cabling:

A) UTP/STP:

Here we have actually measured all points of cabling between all ends so you must know that all measurements have at least **95% of accuracy** and can be relied on for real implementation in the future, the following measurements are from each PC to its switch and from each lab switch to its designated IDF.

You also must know that in the industrial building base floor there is a lot of noise due to the use of mechanical, electronic and electromagnetic devices that will for sure put a base influence on our network thus we are forced to used **Shielded Twisted Pair – STP** cables.

Floor 0 (Administration)

Room 1	
PC1	32.03
PC2	26.17
PC3	24.18
Total	82.38

Room 2	
PC1	22.16
Total	22.16

Room 3	
PC1	36.73
PC2	31.11
Total	67.84

Room 4	

Room 5	
PC1	41.30
Total	41.30

Room 6	
PC1	33.88
PC2	32.37
PC3	30.87
PC4	29.37
PC5	27.87
Total	154.36

Room 7	
PC1	44.85
Total	44.85

Room 9	
PC1	44.36
Total	44.36

Room 10	
PC1	40.40
Total	40.40

Total Lengths	**560**
Number of PCs	**17**

PC1	25.10
Total	25.10

Room 8	
PC1	36.72
Total	36.72

Floor 1

Room 2	
PC1	4.92
PC2	8.47
PC3	7.10
PC4	5.74
PC5	4.37
PC6	9.84
PC7	8.47
PC8	7.10
PC9	5.74
PC10	11.20
PC11	9.84
PC12	8.47
PC13	7.10
PC14	12.57
PC15	11.20
PC16	9.84
PC17	8.47
Total	140.42

Room 1	
PC1	43.18
Total	43.18

Room 3	
PC1	36.92
Total	36.92

Room 4	
PC1	10.34
PC2	11.72
Total	22.06

Room 5	
PC1	30.67
Total	30.67

Room 6	
PC1	24.42
Total	24.42

Room 7	
PC1	17.67
Total	17.67

Room 8	
PC1	28.13
Total	28.13

Room 9	
PC1	24.5
Total	24.5

Room 10	
PC1	34.96
Total	34.96

Room 11	
PC1	31.3
Total	31.3

Room 12	
PC1	42.73
Total	42.73

Room 13	
PC1	38
Total	38

Room 14	
PC1	28.60
Total	28.60

Room 15	
PC1	38.60
Total	38.60

Total Lengths	**600**

Number of PCs	**32**

Switches	
Room 2	15.30
Total	15.30

Floor 2

Room 1	
PC1	3.53
PC2	16.78
PC3	9.75
PC4	5.28
PC5	4.01

Room 2	
PC1	13.88
Total	13.88

Room 3	
PC1	3.53

Room 5	
PC1	3.53
PC2	16.78
PC3	9.75
PC4	5.28
PC5	4.01

Room 6	
PC1	10.34
PC2	11.7
Total	22

Room 7	

PC6	9.68
PC7	10.20
PC8	6.37
PC9	5.10
PC10	10.77
PC11	11.93
PC12	7.46
PC13	6.19
PC14	11.86
PC15	13.02
PC16	8.56
PC17	7.28
PC18	12.95
PC19	14.12
PC20	9.65
PC21	8.38
PC22	14.05
PC23	15.21
PC24	10.74
PC25	9.47
Total	242.34

PC2	16.78
PC3	9.75
PC4	5.28
PC5	4.01
PC6	9.68
PC7	10.20
PC8	6.37
PC9	5.10
PC10	10.77
PC11	11.93
PC12	7.46
PC13	6.19
PC14	11.86
PC15	8.56
PC16	7.28
Total	134.75

Room 4	
PC1	9.88
PC2	12.89
PC3	19.00
Total	41.77

PC6	9.68
PC7	10.20
PC8	6.37
PC9	5.10
PC10	10.77
PC11	11.93
PC12	7.46
PC13	6.19
PC14	11.86
PC15	13.02
PC16	8.56
PC17	7.28
PC18	12.95
PC19	14.12
PC20	9.65
PC21	8.38
PC22	14.05
PC23	15.21
PC24	10.74
PC25	9.47
Total	242.34

PC1	15.20
Total	15.20

Room 8	
PC1	17.67
Total	17.67

Room 9	
PC1	3.53
PC2	16.78
PC3	9.75
PC4	5.28
PC5	4.01
PC6	9.68
PC7	10.20
PC8	6.37
PC9	5.10
PC10	10.77
PC11	6.19
PC12	11.86
PC13	7.28
PC14	12.95
PC15	8.38
PC16	14.05
PC17	9.47
Total	151.65

Room 10	
PC1	24.5
Total	24.5

Room 11	
PC1	3.53
PC2	16.78
PC3	9.75
PC4	5.28
PC5	4.01
PC6	9.68
PC7	10.20

Room 12	
PC1	31.3
Total	31.3

Room 13	
PC1	3.53
PC2	16.78
PC3	9.75
PC4	5.28
PC5	4.01
PC6	9.68
PC7	10.20

Total Lengths	**1527**

Number of PCs	**133**

Switches	
Room 1	37.16
Room 3	35.38

PC8	6.37
PC9	5.10
PC10	10.77
PC11	11.93
PC12	7.46
PC13	6.19
PC14	11.86
PC15	13.02
PC16	8.56
PC17	7.28
PC18	12.95
PC19	14.12
PC20	9.65
PC21	8.38
PC22	9.47
Total	202.34

PC8	6.37
PC9	5.10
PC10	10.77
PC11	11.93
PC12	7.46
PC13	6.19
PC14	11.86
PC15	13.02
PC16	7.28
Total	139.21

Room 14	
PC1	38.16
Total	38.16

Room 15	
PC1	28.60
Total	28.60

Room 5	24.59
Room 9	21.45
Room 11	28.00
Room 13	34.29
Total	180.87

Floor 3

Room 1	
PC1	14.34
PC2	9.93
PC3	12.02
PC4	14.11
PC5	16.28
PC6	18.37
PC7	7.84
Total	92.90

Room 2	
PC1	13.88
Total	13.88

Room 3	
PC1	9.88
Total	9.88

Room 4	
PC1	10.34
PC2	11.72
Total	22.07

Room 5	
PC1	17.67
Total	17.67

Room 6	
PC1	18.09
Total	18.09

Room 9	
PC1	31.33
Total	31.33

Room 10

Room 12	
PC1	42.73
Total	42.73

Switches

Room 7	
PC1	24.5
Total	25.5

Room 8	
PC1	26.37
Total	26.37

PC1	35.70
Total	35.70

Room 11	
PC1	38.16
Total	38.16

Room 1	19.67
Total	19.67

Total Lengths	**394**

Number of PCs	**21**

Floor 4

Room 1	
PC1	3.53
PC2	16.78
PC3	9.75
PC4	5.28
PC5	4.01
PC6	9.68
PC7	10.20
PC8	6.37
PC9	5.10
PC10	10.77
PC11	11.93
PC12	7.46
PC13	6.19
PC14	11.86
PC15	13.02
PC16	8.56
PC17	7.28
PC18	12.95
PC19	8.38
Total	169.10

Room 2	
PC1	13.88
Total	13.88

Room 3	
PC1	16.38
Total	16.38

Room 4	
PC1	9.88
Total	9.88

Room 5	
PC1	22.63
Total	22.63

Room 6	
PC1	10.34
PC2	11.72
Total	22.07

Room 7	
PC1	24.42
Total	24.42

Room 8	
PC1	17.67
Total	17.67

Room 9	
PC1	18.09
Total	18.09

Room 10	
PC1	24.5
Total	24.5

Room 11	
PC1	14.92
Total	14.92

Room 12	
PC1	21.33
Total	21.33

Room 13	
PC1	31.75
Total	31.75

Room 14	
PC1	38.16
Total	38.16

Room 15	
PC1	42.73
Total	42.73

Switches	
Room 1	37.16
Total	37.16

Total Lengths	**525**

Number of PCs	**37**

Industrial Building
Floor 0

Room 1	
PC1	22.98
PC2	21.37
Total	44.35

Room 2	
PC1	14.69
PC2	13.09
Total	27.78

Room 3	
PC1	10.14
PC2	8.53
Total	18.67

Room 4	
PC1	19.12
PC2	17.52
Total	36.64

Room 5	
PC1	23.05
PC2	21.45
Total	44.50

Room 6	
PC1	22.98
PC2	21.37
Total	44.35

Room 7	
PC1	14.69
PC2	13.09
Total	27.78

Room 8	
PC1	10.14
PC2	8.53
Total	18.67

Room 9	
PC1	19.12
PC2	17.52
Total	36.64

Room 10	
PC1	23.05
PC2	21.45
Total	44.50

Total Lengths	**344**
Number of PCs	**20**

Floor 1

Room 1	
PC1	26.94

Room 2	
PC1	27.58

Room 3	
PC1	19.23

Room 4	
PC1	15.10

Room 5	
PC1	11.24

Room 6	
PC1	18.31

Room 7	
PC1	10.75

Room 8	
PC1	10.75

Room 9	
PC1	26.03

Room 10	
PC1	33.68

Room 11	
PC1	28.63

Total Lengths	**229**
Number of PCs	**11**

In addition to the above measurements we must add additional cable of length 1.5 meters from each node to its outlet and the length that we have mentioned before is a standard for all nodes. We have **251 UTP connected PCs** and **20 STP connected PCs** as such we must add ((1.5*251 UTP) + (1.5*20 STP)) about 376.5 meters of UTP cables and 30 meters of STP cables.

Moreover we have all nodes connected to a patch panel and as such we have an additional 1 meter cable from the patch panel to the switch which means ((1*251UTP) + (1*20STP)) about 251 meters of UTP cables, and 20 meters of STP cables.

From Wireless Radio Access Point to the MDF:

On the building A roof we have a **Microwave Radio Antenna** that connects **ITI** to **Dikoueneh**, we decided to connect the **ECLIPSE** access point directly to our MDF in building A using UTP cable that ends in the **3Com 5500-EI FX Switch**, and as such we are given the ability to control the access from/to the Dikoueneh network. As such we need about **65 meters** of UTP cable and another **65 meters** for link aggregation.

From Wi-Fi Access Point to the IDF:

Because the base floor is an administrative floor, most of the teachers might have laptops and would need access to the network or internet to achieve a certain task, thus we have placed a **WiFi** access points that is connected directly to the IDF, so we need about **24 meters** of UTP cables from the access point to the IDF.

	UTP	STP
Building [A] Floor [0]	584 m	
Building [A] Floor [1]	616 m	
Building [A] Floor [2]	1708 m	
Building [A] Floor [3]	414 m	
Building [A] Floor [4]	563 m	
Building [B] Floor [0]		344 m
Building [B] Floor [1]	229 m	
Wireless to MDF	130 m	
Outlet to PCs	377 m	30 m
Patch panels to switches	251 m	20 m
Totals	4551.5 m	394 m
Totals + 10%	Approximately 5000m	Approximately 430m

All cables from lab switches to the IDF are aggregated with another cable which doubled its cable lengths; also an additional 10% of cable will be added as a safety margin to the total length of cables.

B) Fiber Optics:

Building [A]: In the academic facility a **Multi-Mode** Fiber Optics cable runs down from the fourth floor IDF down to the base floor MDF through its IDF, thus as we have previously said that we need **50 meters** of Fiber Optics cable, and since we are using link aggregation technology we need another **50 meters** of cable to go with the first one.

Building [B]: In the industrial facility a **Multi-Mode** Fiber Optics cable runs down from the second floor IDF down to the base floor MDF through its IDF, thus we need here **16 meters** of Fiber Optics cable, also we need another **16 meters** to go along with the link aggregation specs we are using.

Between building backbone lengths: Because the buildings are interconnected with each other we need another **35 meters** of **Single-Mode** Fiber Optics between both buildings MDFs with an addition **35 meters** for link aggregation.

There will be an additional 5% for both single mode and multi mode cables, thus the totals would be as follows:

Single Mode Fiber Optic	**139 meters**
Multi Mode Fiber Optic	**74 meters**

C) Raceways:

Cable that cannot be run inside a protected space must be enclosed in protective raceway such as cable tray. Protective raceways must be permanently attached to underlying wall surfaces with appropriate wall anchors.

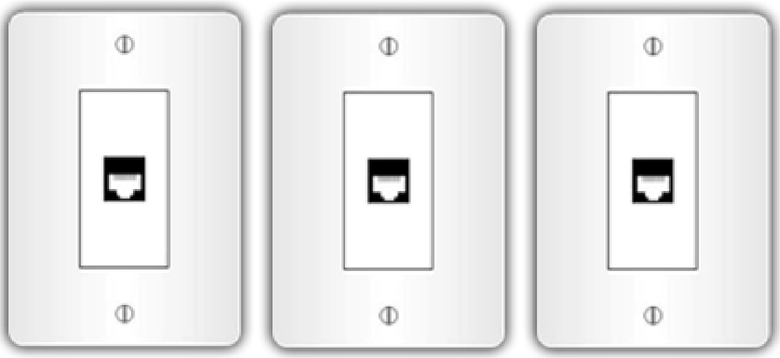
For UTP/STP Cables we need **680 meters** of plastic cable trays in addition to the in-building Fiber Optic backbone which is **140 meters**.

Since we have a fiber optic backbone, we require another type of raceways that would keep safe our cables and ensure nothing happens to them under the ground, there for we are going to use a Gel filled buffer tube, 250 um acrylate.

Single-Mode Fiber Optic backbone which is underground, need **70 meters** of Gel filled buffer tube.

D) Outlets:

We have 271 PCs , 5 Servers and a node for the wireless link which means that we need 277 outlets.



E) Racks: All of the equipment found in the MDFs and IDFs are mounted on a rack where each rack is chosen according to the number of devices used, to gain more space and for professional reasons we have chosen to place the lab switches inside a wall mounted rack, and on the other hand all the IDFs and MDFs will be mounted on to a tower shaped rack.

Wall Mounted Rack

Rack

F) Patch Panels: A patch panel or patch bay is a panel, typically rack-mounted, that houses cable connections. One typically shorter patch cable will plug into the front side, while the back will hold the connection of a much longer and more permanent cable. The assembly of hardware is arranged so that a number of circuits, usually of the same or similar type, appear on jacks for monitoring, interconnecting, and testing circuits in a convenient, flexible manner. Patch panels offer the convenience of allowing technicians to quickly change the path of select signals, without the expense of dedicated switching equipment.

Above each 4400 mounted switch there'll be a patch panel with the same number of ports, more over a 4 port patch panel will be placed in each IDF and a 24 fiber optic patch panel will be placed in each MDF.

Fiber optic patch panel description: 24-Port (24-Fiber) ST SM/MM Fiber Patch Panel and 8-Port (8-Fiber) ST SM/MM Fiber Patch Panel.

G) **Power supplies** will be placed inside each rack, a 650VA power supply will be installed inside each rack except the one found in the MDF because we are going to use a rack mounted power supply, and there will also be an 1000VA power supply to support each server.

APC Back-UPS 650VA 220V:

Specifications		
Output Power Capacity	400 Watts / 650 VA	
Nominal Input Voltage	230V	
Efficiency at Full Load	95.00%	
Typical recharge time	24 hour(s)	
Net Weight	6.70 KG	

APC Smart-UPS 750VA USB Rack Mounted 1U 230V:

Specifications		
Output Power Capacity	480 Watts / 750 VA	
Nominal Input Voltage	230V	
Efficiency at Full Load	98.00%	
Typical recharge time	2 hour(s)	
Net Weight	21.82 KG	

APC Smart-UPS 1000VA USB & Serial 230V:

Specifications		
Output Power Capacity	670 Watts / 1000 VA	
Nominal Input Voltage	230V	
Efficiency at Full Load	98.00%	
Typical recharge time	3 hour(s)	
Net Weight	18.86 KG	

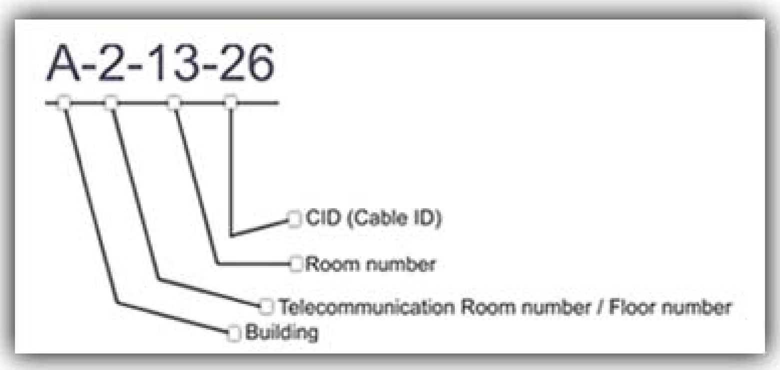
	4400 SW		2126-G SW		5500 SW	UTP Patch panel		Fiber Optic Patch panel	
	24 ports	48 ports	24	48		24 ports	48 ports	8 ports	24 ports
Bldg[A] Fl[0]	**1**	--------	---	---	**2**	**2**	--------	**1**	**1**
Bldg[A] Fl[1]	**1**	--------	**1**	---	------	**2**	--------	**1**	--------
Bldg[A] Fl[2]	--------	**1**	**2**	**4**	------	**2**	**5**	**1**	--------
Bldg[A] Fl[3]	**1**	--------	**1**	---	------	**2**	--------	**1**	--------
Bldg[A] Fl[4]	**1**	--------	**1**	---	------	**2**	--------	**1**	--------
Bldg[B] Fl[0]	**2**	--------	---	---	------	**2**	--------	**2**	--------
Bldg[B] Fl[1]	**1**	--------	---	---	------	**1**	--------	**1**	--------
Totals	**8**	**1**	**5**	**4**	**2**	**12**	**5**	**8**	**1**

	Power Supplies UPS			Racks	
	650VA	750VA	1000VA	Tower	Wall Mounted
Bldg[A] Fl[0]	**1**	**2**	**5**	**2**	**1**
Bldg[A] Fl[1]	**2**	--------	--------	**1**	**1**
Bldg[A] Fl[2]	**8**	--------	--------	**1**	**6**
Bldg[A] Fl[3]	**2**	--------	--------	**1**	**1**
Bldg[A] Fl[4]	**2**	--------	--------	**1**	**1**
Bldg[B] Fl[0]	**1**	**1**	--------	**2**	--------
Bldg[B] Fl[1]	**1**	--------	--------	**1**	--------
Totals	**17**	**3**	**5**	**9**	**10**

III-3-4-Labeling:

Each individual cable and communications outlet shall be labeled. Cable labels shall be attached from between 6 and 9 inches from both cable ends. Labels must be machine printed with permanent black ink on laminated white label material also installers shall label each copper station cable and its associated jack at the telecommunication outlet.

So the chosen label is as follows in detail:



In addition each CID above 10 refers to a cable that exists in a lab, and this will be understood more when viewing the following labeling tables:

Building **[A]** Academic:

IDF to PCs			**IDF to PCs/Lab Switches**		
	to Area	Cable ID		to Area	Cable ID
Floor 0	Room 1	A-0-01-1 To A-0-01-3	Floor 1	Room 1	A-1-01-1
	Room 2	A-0-02-1		Room 2	A-1-02-1 , A-1-02-2
	Room 3	A-0-03-1 To A-0-03-2		Room 3	A-1-03-1
	Room 4	A-0-04-1		Room 4	A-1-04-1 , A-1-04-2
	Room 5	A-0-05-1		Room 5	A-1-05-1
	Room 6	A-0-06-1 To A-0-06-5		Room 6	A-1-06-1
	Room 7	A-0-07-1		Room 7	A-1-07-1
	Room 8	A-0-08-1		Room 8	A-1-08-1
	Room 9	A-0-09-1		Room 9	A-1-09-1

	Room 10	A-0-10-1		Room 10	A-1-10-1
				Room 11	A-1-11-1
				Room 12	A-1-12-1
				Room 13	A-1-13-1
				Room 14	A-1-14-1
				Room 15	A-1-15-1

IDF to PCs/Lab Switches			IDF to PCs/Lab Switches		
	to Area	Cable ID		to Area	Cable ID
Floor 2	Room 1	A-2-01-1 , A-2-01-2	Floor 3	Room 1	A-3-01-1 , A-3-01-2
	Room 2	A-2-02-1		Room 2	A-3-02-1
	Room 3	A-2-03-1 , A-2-03-2		Room 3	A-3-03-1 To A-3-03-4
	Room 4	A-2-04-1 To A-2-04-3		Room 4	A-3-04-1 , A-3-03-2
	Room 5	A-2-05-1 , A-2-05-2		Room 5	A-3-05-1
	Room 6	A-2-06-1 , A-2-06-2		Room 6	A-3-06-1 , A-3-06-2
	Room 7	A-2-07-1		Room 7	A-3-07-1
	Room 8	A-2-0-1		Room 8	A-3-08-1
	Room 9	A-2-09-1 , A-2-09-2		Room 9	A-3-09-1
	Room 10	A-2-10-1		Room 10	A-3-10-1
	Room 11	A-2-11-1 , A-2-11-2		Room 11	A-3-11-1
	Room 12	A-2-12-1		Room 12	A-3-12-1
	Room 13	A-2-13-1 , A-2-13-2			
	Room 14	A-2-14-1			
	Room 15	A-2-15-1			

IDF to PCs/Lab Switches		
	to Area	Cable ID
Floor 4	Room 1	A-4-01-1 , A-4-01-2
	Room 2	A-4-02-1
	Room 3	A-4-03-1
	Room 4	A-4-04-1 To A-4-04-4
	Room 5	A-4-05-1
	Room 6	A-4-06-1 , A-4-06-2
	Room 7	A-4-07-1
	Room 8	A-4-08-1
	Room 9	A-4-09-1
	Room 10	A-4-10-1
	Room 11	A-4-11-1
	Room 12	A-4-12-1
	Room 13	A-4-13-1
	Room 14	A-4-14-1
	Room 15	A-4-15-1

Lab Switches to PCs		
	Area	Cable ID
Floor 1	Room 2	A-1-02-10 To A-1-02-27
Floor 2	Room 1	A-2-01-10 To A-2-01-35
	Room 3	A-2-03-10 To A-2-03-26
	Room 5	A-2-05-10 To A-2-05-35
	Room 9	A-2-09-10 To A-2-09-27
	Room 11	A-2-11-10 To A-2-11-32
	Room 13	A-2-13-10 To A-2-13-26
Floor 3	Room 1	A-3-01-10 To A-3-01-17
Floor 4	Room 1	A-4-01-10 To A-4-01-29

Building **[B]** Industrial:

IDF to PCs		
	to Area	Cable ID
Floor 0	Room 1	B-0-01-1 , B-0-01-2
	Room 2	B-0-02-1 , B-0-02-2
	Room 3	B-0-03-1 , B-0-03-2
	Room 4	B-0-04-1 , B-0-04-2
	Room 5	B-0-05-1 , B-0-05-2
	Room 6	B-0-06-1 , B-0-06-2
	Room 7	B-0-07-1 , B-0-07-2
	Room 8	B-0-08-1 , B-0-08-2
	Room 9	B-0-09-1 , B-0-09-2
	Room 10	B-0-10-1 , B-0-10-2

IDF to PCs		
	to Area	Cable ID
Floor 1	Room 1	B-1-01-1
	Room 2	B-1-02-1
	Room 3	B-1-03-1
	Room 4	B-1-04-1
	Room 5	B-1-05-1
	Room 6	B-1-06-1
	Room 7	B-1-07-1
	Room 8	B-1-08-1
	Room 9	B-1-09-1
	Room 10	B-1-10-1
	Room 11	B-1-11-1

Chapter IV

Logical Network Design

IV-1-Network Logical Structure:

IV-1-1- IP Addressing

After calculating the number of nodes and links needed, and since everything in the world of network is about efficiency we have decided to use the **B address class** taking into consideration that sub-netting this IP address will be of great value to our network for vital future uses such as VLANs and because it will give us a number of broadcast domains.

According to the administration's request and security reasons we are required to have 2 subnets, the first will be used in administration and for administrative people, and the second will be used for the rest of the network. The first subnet is physically located on the base floor of building A and the administrative rooms of building B located on floor 2, an additional subnet will be created for the purpose of junction between subnets through ISA firewall which will be the default gateway for other subnets to grab their internet connection from.

Number of nodes: 271 => 2^9 = 512 maximum number of hosts there for the designated network IP will be **172.16.0.0**

We need two subnets so we have this rule 2^n – 2 >= 2 so N=2 thus we need to borrow two bits from the hosts to the subnets and this result with the following IPs for each subnet:

Subnet|1: **172.16.32.1** and **172.16.32.2**

Subnet|2 (Administration): From **172.16.64.1** scalable to maximum of **172.16.95.254**.

Subnet|3 (The Rest): From **172.16.96.1** scalable to maximum of **172.16.127.254**

The default subnet mask for the entire network will be **255.255.224.0**.

Device	IP
DSL Router	172.16.32.2
ISA Server	172.16.32.1
Server	**From** 172.16.64.1 **to** 172.16.64.10
Wireless Radio	172.16.64.11
Others	**From** 172.16.96.1 **to** 172.16.127.254

IV-1-2- Servers' room:

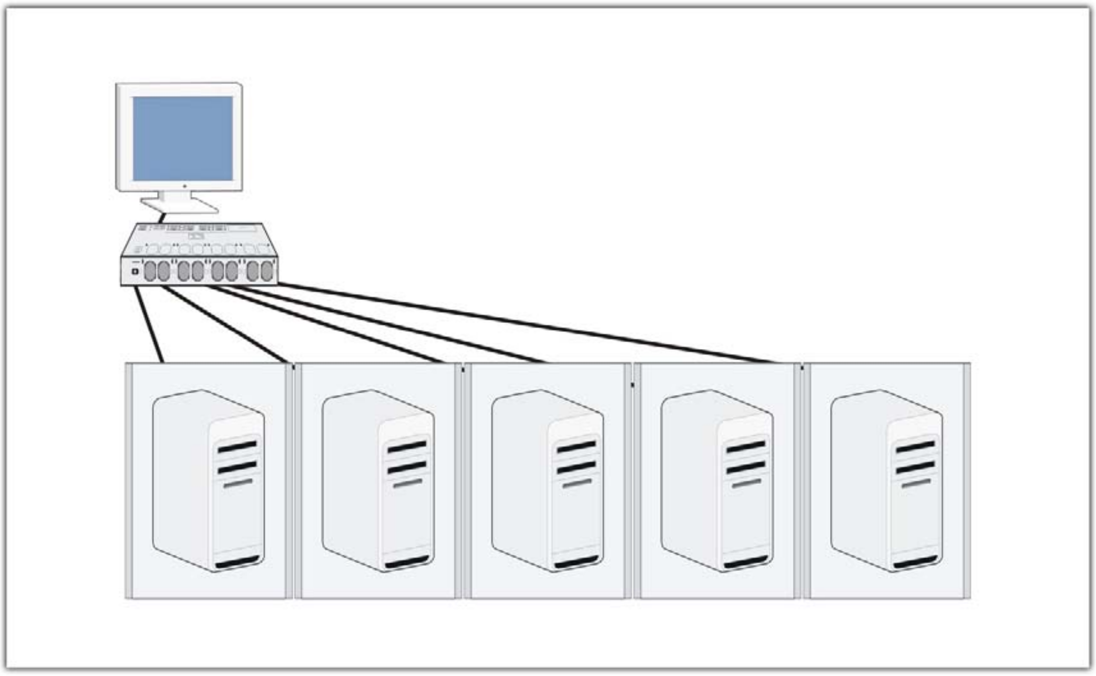
Our server room is formed of separate boxes each with a specific task, each box will host two major tasks one that acts as a primary operative and the other as a secondary operative, in this way we make sure that all the servers are giving the 100% performance they're required to provide and be certain that no major fall backs or failures will have an influence that might lead us into the down time zone. So as you can see in the figure our servers are connected to the MDF through a switch, where all the boxes are also connected to a D-Link 8 port **KVM switch** device that would allow us to use a single monitor, keyboard and mouse for all the boxes.

KVM Switch:

A KVM switch (with KVM being an abbreviation for Keyboard, Video or Visual Display Unit, Mouse) is a hardware device that allows a user to control multiple computers from a single keyboard, video monitor and mouse. Although multiple computers are connected to the KVM, typically a smaller number of computers can be controlled at any given time. Modern devices have also added the ability to share USB devices and speakers with multiple computers. Some KVM switches can also function in reverse - that is, a single PC can be connected to multiple monitors, keyboards, and mice. While not as common as the former, this configuration is useful when the operator wants to access a single computer from two or more (usually close) locations - for example, a public kiosk machine that also has a staff maintenance interface behind the counter, or a home office computer that doubles as a home theater PC.

A user connects a monitor, keyboard, and mouse to the KVM device, then uses special cables (generally USB and VGA) to connect the KVM device to the computers. Control is switched from one computer to another by the use of a switch or buttons on the KVM device, with the KVM passing the signals between the computers and the keyboard, mouse and monitor depending on which computer is currently selected. Most electronic devices also allow control to be switched through keyboard commands (such as hitting a certain key, often Scroll Lock, rapidly two or three times).

Server room planning:



Server [1]:

- Domain Controller – **Primary**
- DNS (Domain Name System) Server – **Secondary**

Server [2]:

- Dynamic Host Configuration Protocol (DHCP) – **Primary**

Server [3]:

- Internet Security and Acceleration Server (ISA) – **Primary**

Server [4]:

- Data Server - **Primary**
- Domain Controller – **Bridgehead Server**

Server [5]:

- Local Web-Server – **Primary**
- Data Server Backup – **Secondary**

Domain Controller: On Windows Server Systems, a domain controller (DC) is a server that responds to security authentication requests (logging in, checking permissions, etc.) within the Windows Server domain.

In Windows NT, one domain controller per domain was configured as the Primary Domain Controller (PDC); all other domain controllers were Backup Domain Controllers (BDC). A BDC could authenticate the users in a domain, but all updates to the domain (new users, changed passwords, group membership, etc) could only be made via the PDC, which would then propagate these changes to all BDCs in the domain. If the PDC was unavailable or unable to communicate with the user requesting the change, the update would fail. If the PDC was permanently unavailable (e.g. if the machine failed), an existing BDC could be promoted to PDC. Because of the critical nature of the PDC, best practices dictated that the PDC should be dedicated solely to domain services, and not used for file/print/application services that could slow down or crash the system. Some network administrators took the additional step of having a dedicated BDC online for the express purpose of being available for promotion if the PDC failed.

Windows 2000 and later introduced Active Directory ("AD"), which largely eliminated the concept of primary and backup domain controllers in favor of the multi-master replication technology available in Windows. However, there are still a number of roles that only one domain controller can perform, called the "Flexible Single Master Operation" roles (some of these roles must be filled by one DC per domain, while others only require one DC per AD forest). If the server performing one of these roles is lost the domain can still function, and if the server will not be available again an administrator can designate an alternate DC to assume the role (a process known as "seizing" the role).

DNS: The Domain Name System (DNS) associates various information with domain names; most importantly, it serves as the "phone book" for the Internet by translating human-readable computer hostnames, e.g. www.example.com, into IP addresses, e.g. 208.77.188.166, which networking equipment needs to deliver information. It also stores other information such as the list of mail servers that accept email for a given domain. In providing a worldwide keyword-based redirection service, the Domain Name System is an essential component of contemporary Internet use.

The most basic task of DNS is to translate hostnames to IP addresses. In very simple terms, it can be compared to a phone book. DNS also has other important uses.

Above all, DNS makes it possible to assign Internet names to organizations (or concerns they represent) independent of the physical routing hierarchy represented by the numerical IP address. Because of this, hyperlinks and Internet contact information can remain the same, whatever the current IP routing arrangements may be, and can take a human-readable form (such as "example.com"), which is easier to remember than the IP address 208.77.188.166. People take advantage of this when they recite meaningful URLs and e-mail addresses without caring how the machine will actually locate them.

The Domain Name System distributes the responsibility for assigning domain names and mapping them to IP networks by allowing an authoritative name server for each domain to keep track of its own changes, avoiding the need for a central register to be continually consulted and updated.

DHCP: Dynamic Host Configuration Protocol (DHCP) is a protocol used by networked devices (clients) to obtain various parameters necessary for the clients to operate in an Internet Protocol (IP) network. By using this protocol, system administration workload greatly decreases, and devices can be added to the network with minimal or no manual configurations.

Dynamic Host Configuration Protocol is a way to administer network parameter assignment from a single DHCP server, or a group of DHCP servers arranged in a fault-tolerant manner. Even in small networks, Dynamic Host Configuration Protocol is useful because it can make it easy to add new machines to the local network.

DHCP is also recommended even in the case of servers whose addresses rarely change, so that if a server need to be readdressed (RFC2071), changes can be made in as few places as possible. For devices such as routers and firewalls, that should not use DHCP, it can be useful to put Trivial File Transfer Protocol (TFTP) or SSH servers on the same machine that runs DHCP, which also serves to centralize administration.

DHCP can be used to directly assign addresses to servers and desktop machines, and, through a Point-to-Point Protocol (PPP) proxy, to dialup and broadband on-demand hosts, as well as for residential Network address translation (NAT) gateways and routers. DHCP is generally not appropriate for infrastructure such as non-edge routers and DNS servers.

Bridgehead: In Windows 2000 Server, bridgehead servers are the contact point for the exchange of directory information between sites. A bridgehead server is a domain controller that has been either administratively assigned or automatically chosen to replicate changes collected from other domain controllers in the site to bridgehead servers in other sites.

By default, the Active Directory replication topology generator, the Knowledge Consistency Checker (KCC), automatically chooses servers to act as bridgehead servers. However, if you are an administrator, you may select one or more domain controllers in the site to be preferred bridgehead servers. These servers are used exclusively to replicate changes collected from the site. Even though you may have administratively configured several domain controllers as preferred bridgehead servers, the KCC chooses one of these servers to become the bridgehead server for the site. However, if you choose only one bridgehead server for a particular site, and that server becomes unavailable, the KCC does not choose another domain controller to be the bridgehead server. Therefore, if you assign a preferred bridgehead server, you should assign more than one.

Multiple bridgehead servers may be required to replicate full copies of data from one site to another. This behavior depends on the transports available, the directory partitions that have to be replicated, and the availability of global catalog servers. You must assign one bridgehead server for each writable directory partition in your forest. When you assign a bridgehead server, you can establish a preferred bridgehead server for one or more protocols such as IP or SMTP.

When you configure a domain controller to be the preferred bridgehead server, you must specify the transports that are preferred for replication.

Web Server: Is a computer that delivers web pages to browsers, also other files to other applications via the HTTP protocol. It includes the hardware, operating system, Web-Server software, TCP/IP protocols and site content (Web pages and other files). If a web server is used internally and not by the public it may be called an "intranet server."

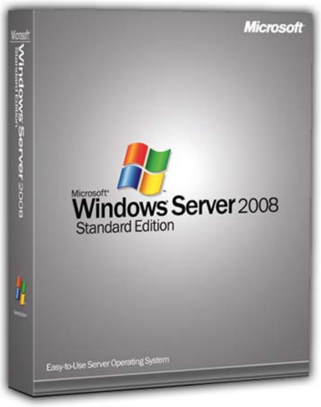
HTTP Server "Web server" may refer to just the software and not the entire computer system. In such cases, it refers to the HTTP server (IIS, Apache, etc.) that manages requests from the browser and delivers HTML documents and files in response. It also executes server-side scripts (CGI scripts, JSPs, ASPs, etc.) that provide functions such as database searching and e-commerce.

Hardware Specifications & Operating Systems:

Operating System:

All the servers will be installed with a fresh copy of Windows Server 2008 Standard Edition, which is the most advanced server product provided by Microsoft.

Windows Server 2008 is the most advanced Windows Server operating system yet, designed to power the next-generation of networks, applications, and Web services. With Windows Server 2008 you can develop, deliver, and manage rich user experiences and applications, provide a highly secure network infrastructure, and increase technological efficiency and value within your organization.



Windows Server 2008 builds on the success and strengths of its Windows Server predecessors while delivering valuable new functionality and powerful improvements to the base operating system. New Web tools, virtualization technologies, security enhancements, and management utilities help save time, reduce costs, and provide a solid foundation for your information technology (IT) infrastructure.

A Solid Foundation for Your Business: Windows Server 2008 provides a solid foundation for all of your server workload and application requirements while also being easy to deploy and manage. The all new Server Manager provides a unified management console that simplifies and streamlines server setup, configuration, and ongoing management. Windows PowerShell, a new command-line shell, helps enable administrators to automate routine system administration tasks across multiple servers. Windows Deployment Services provides a simplified, highly secure means of rapidly deploying the operating system via network-based installations. And Windows Server 2008 Failover Clustering wizards, and full Internet Protocol version 6 (IPv6) support plus consolidated management of Network Load Balancing, make high availability easy to implement even by IT generalists.

The new Server Core installation option of Windows Server 2008 allows for installation of server roles with only the necessary components and subsystems without a graphical user interface. Fewer roles and features means minimizing disk and service footprints while reducing attack surfaces. It also enables your IT staff to specialize according to the server roles they need to support.

Virtualization Built-in: Windows Server Hyper-V, the next-generation hypervisor-based server virtualization technology, allows you to make the best use of your server hardware investments by consolidating multiple server roles as separate virtual machines running on a single physical machine. You can also efficiently run multiple operating systems - Windows, Linux, and others – in parallel on a single server. With Hyper-V and simple licensing policies, it's now easier than ever to take advantage of the cost savings of virtualization.

Applications can also be efficiently virtualized using Windows Server 2008 centralized application access technologies. Terminal Services Gateway and Terminal Services Remote App allow easy remote access to standard Windows-based programs from anywhere by running them on a terminal server instead of directly on a client computer - without the need for a complicated virtual private network (VPN).

Built for the Web: Windows Server 2008 comes with Internet Information Services 7.0 (IIS 7.0), a Web server and security-enhanced, easy-to-manage platform for developing and reliably hosting Web applications and services. A major enhancement to the Windows Web platform, IIS 7.0 includes a componentized architecture for greater flexibility and control. IIS 7.0 also provides simplified management, powerful diagnostic and troubleshooting capabilities that save time, and comprehensive extensibility.

Internet Information Server IIS 7.0 together with the .NET Framework 3.0 provides a comprehensive platform for building applications that connect users and data, enabling them to visualize, share, and act on information. Additionally, IIS 7.0 plays a central role in unifying Microsoft's Web platform technologies—ASP.NET, Windows Communication Foundation Web services, and Windows SharePoint Services.

High Security: Windows Server 2008 is the most secure Windows Server yet. The operating system has been hardened to help protect against failure and several new technologies help prevent unauthorized connections to your networks, servers, data, and user accounts. Network Access Protection (NAP) helps ensure that computers that try to connect to your network comply with your organization's security policy. Technology integration and several enhancements make Active Directory services a potent unified and integrated Identity and Access (IDA) solution. And Read-Only Domain Controller (RODC) and BitLocker Drive Encryption allow you to more securely deploy your AD database at branch office locations.

High Performance Computing: The benefits and cost savings of Windows Server 2008 extend to Windows HPC Server 2008 for your high performance computing (HPC) environment. Windows HPC Server 2008 is built on Windows Server 2008, x64-bit technology and can efficiently scale to thousands of processing cores with out-of-the-box functionality to improve the productivity, and reduce the complexity of your HPC environment. Windows HPC Server 2008 enables broader adoption by providing a rich and integrated end-user experience that scales from the desktop application to the clusters, and includes a comprehensive set of deployment, administration, and monitoring tools that are easy to deploy, manage, and integrate with your existing infrastructure.

Hardware requirements:

Since each server does a certain job, each one has its own hardware specifications according to its task.

3 x Servers [Servers [1 to 3]]:

- **Motherboard**: Intel Server Board S5000PSL supports up to 2 XEON CPUs
- **Processor**: Intel XOEN Processor 5000 Sequence X5472, 12MB Cache, 3.00GHz clock speed, 1600Mhz Front Side Bus, Power 120Watts, Quad Core.
- **Memory**: 8GB DDR2.
- **Ethernet:** Two 10/100/1000 Intel Ethernet network adapter with support of 1000Base-T interface.
- **Interfaces:**

Serial	2 x RS232 serial ports
USB	4 x 2.0 High Speed 480Mbps
PS2	2 x PS2 Interface ports

- **HDD:** 1 x 500GB SATA 2 Segate Barracuda 3.0Gb/s Hard Drive / 16Mb Buffer
- **Optical:** Pioneer 16x DVD-RW+-
- **Power Supply:** 560Watt with double fans

2 x Servers [Servers [4 and 5]]:

- **Motherboard**: Intel Server Board S5000PSL supports up to 2 XEON CPUs
- **Processor**: Intel XEON Processor 5000 Sequence X5472, 12MB Cache, 3.00GHz clock speed, 1600Mhz Front Side Bus, Power 120Watts, Quad Core.
- **Memory**: 4GB DDR2.
- **Ethernet:** Two 10/100/1000 Intel Ethernet network adapter with support of 1000Base-T interface.
- **Interfaces:**

Serial	2 x RS232 serial ports
USB	4 x 2.0 High Speed 480Mbps
PS2	2 x PS2 Interface ports

- **HDD:** 2 x 500GB SATA 2 Segate Barracuda 3.0Gb/s Hard Drive / 16Mb Buffer
- **Optical:** Pioneer 16x DVD-RW+-
- **Power Supply:** 560Watt with double fans

Since we are using a KVM system we require a single Monitor, Mouse and Keyboard:

- **Monitor**: 21” LCD Sony True Bright LMD-212S
- **Mouse/Keyboard**: Logitech Multimedia Combo EX-110

Chapter V

Network Security Planning

V-1 - Security:

Nowadays it is well known that what characterizes any communication related project is it is capability of keeping safe that which is secret from the any intrusion since connecting to the Internet opens the computer or the entire network to the outside world. If **security** methods are not implemented, the computers or the **Internet** may be at risk of being **exploited**. Security threats come in various forms and can cause loss of connectivity or loss of valuable data and in order to stand against these threats firmly we have a security scheme for our network that includes both **Software** and **Hardware firewalls** in addition to an **Antivirus** software that meets both client and server needs and as such we have chosen:

Scheme	Hardware Firewall	Software Firewall	Antivirus
	3Com Tipping Point 50 Intrusion Prevention System IPS	Internet Security & Acceleration Server 2006	Symantec Antivirus Corporate Edition 10.2

Additional software could be added to the above scheme which gives more strength and power to the administrator to gain even more control over the network, the program is called Ethereal and it is a Network Protocol Analyzer.

V-2- 3Com Tipping Point 50 Intrusion Prevention System – Hardware Firewall:

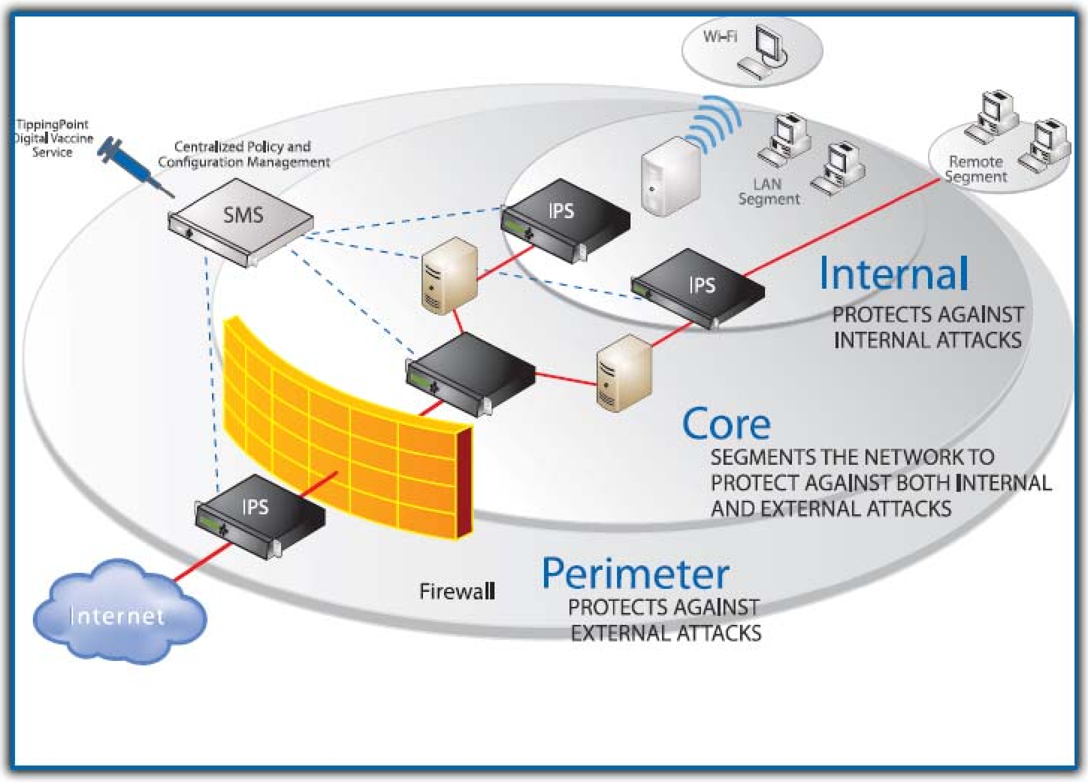
What is a Hardware Firewall?

A firewall is a barrier that is placed in between your computer and other computers that may be able to connect to your computer, via means such as the internet. Firewalls stop unauthorized users gaining access to your computer, which they may attempt to do in order to steal your data, install 'malware' or simply be 'nosy'. They do this by blocking access to 'ports' on your computer and also by hiding your computer from the view of other internet users. They also keep a monitor on any network traffic that is passed to or from your computer.

TippingPoint is the industry's leading Intrusion Prevention System (IPS), unrivaled in security, performance, high availability and ease-of-use. TippingPoint is the defining benchmark for network-based intrusion prevention.

The TippingPoint 50 is specifically a **Proactive Network Security** module!

With the TippingPoint IPS operating in-line in the network, malicious and unwanted traffic is blocked, while good traffic passes unimpeded. It optimizes the performance of good traffic by continually cleansing the network and prioritizing applications that are mission critical. TippingPoint's high performance and extraordinary intrusion prevention accuracy have redefined network security, and fundamentally changed the way people protect their organization.



TippingPoint also significantly reduces the amount of time and resources needed to maintain a healthy network. State of the art “Recommended Filter” settings allow instant deployment out-of-the-box with no tuning required. No longer is it necessary to clean up after cyber attacks have compromised your servers and workstations. No more ad-hoc and emergency patching. No more out of control, rogue applications like Peer-to-Peer and Instant Messaging running rampant throughout the network. Denial-of-Service attacks that choke Internet connections or crash mission critical applications are a thing of the past.

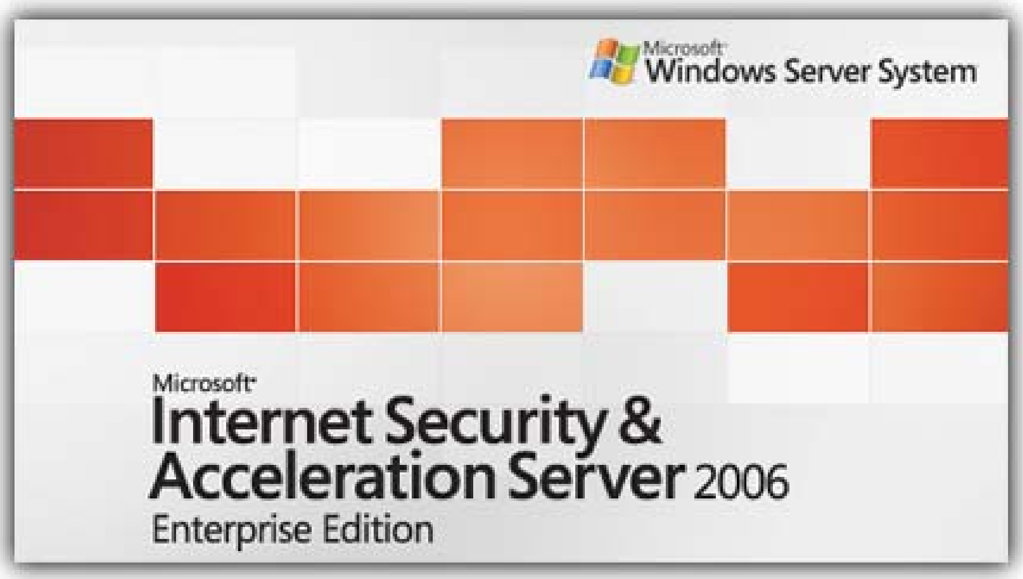
TippingPoint enables traffic shaping to support critical applications and infrastructure, as well as provides attack isolation and network discovery of vulnerable devices, also it enables deployment at the network core, protecting from external/internal threats.

Technical Specifications	
Switch-Like Performance	**Client and Server Protection**
• 50 Mbps Attack Filtering • Latency < 1 millisecond • Real World TCP/UDP Traffic Mix • 500,000 Simultaneous Sessions - TCP/UDP/ICMP • 5,000+ Connections Per Second	• Prevent Attacks on Vulnerable Applications and Operating Systems • Eliminate Costly Ad-Hoc Patching • Multi-Mode Attack Blocking
Network Infrastructure Protection	**Digital Vaccine® Real-Time Inoculation**
• Protect Cisco IOS, DNS and Other Infrastructure • Protect Against Traffic Anomaly, DoS, SYN Floods, Process Table Floods • Access Control Lists	• Protection Against Zero-Day Attacks • Automatic Distribution of Latest Filters
Traffic Normalization	**Power Dissipation**
• Increase Network Bandwidth and Router Performance • Normalize Invalid Network Traffic • Optimize Network Performance	• Units: AC • Amps: 6/3 • V: 100-240 • Efficiency: 72% • Freq. Range (Hz): 50-60
Application Performance Protection	**Dimensions**
• Increase Bandwidth and Server Capacity • Rate-Limit or Block Unwanted Traffic - Peer-to-Peer/Instant Messaging	• Height (in): 1.75 Height (cm): 4.4 • Width (in): 17.25 Width (cm): 43.8 • Depth (in): 12 Depth (cm): 30.5 • Weight (lb): 12.5 Weight (kg): 5.8

V-3- Internet Security & Acceleration Server 2006 – Software Firewall:

What is a Software Firewall?

A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks where it also implies the security policy that is used in order to create some restrictions on certain access levels of the network.


Microsoft Windows Server System
Microsoft
Internet Security & Acceleration Server 2006
Enterprise Edition

Microsoft's **ISA Server** (Internet Security and Acceleration Server) is the successor to Microsoft's **Proxy Server 2.0** and is part of Microsoft's .NET support. ISA Server provides the two basic services of an enterprise firewall and a Web proxy/cache server. ISA Server's firewall screens all packet-level, circuit-level, and application-level traffic. The Web cache stores and serves all regularly accessed Web content in order to reduce network traffic and provide faster access to frequently-accessed Web pages. ISA Server also schedule downloads of Web page updates for non-peak times.

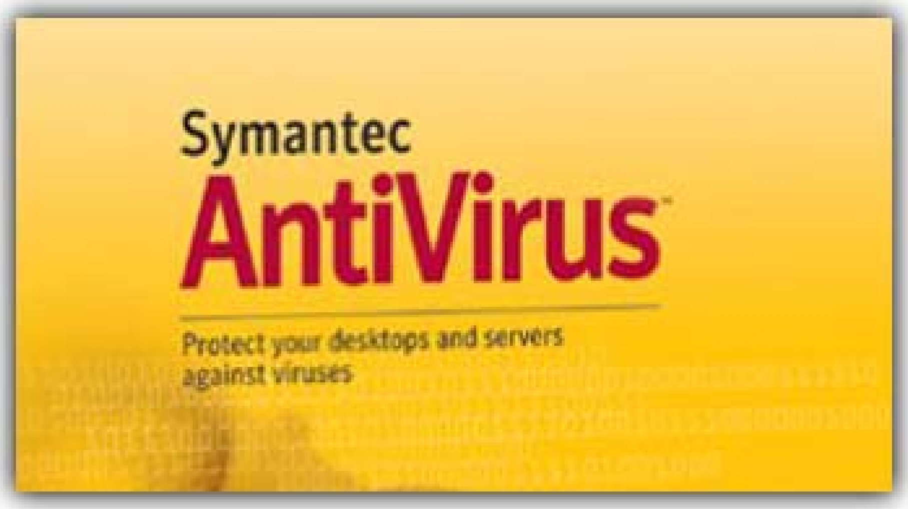
ISA Server allows administrators to create policies for regulating usage based on user, group, application, destination, schedule, and content type criteria. ISA Server is designed to work with Windows 2000 and later operating systems and to take advantage of Windows' Kerberos security. ISA Server includes a software development kit (SDK).

ISA Server comes in two editions, Standard Edition and Enterprise Edition. Standard Edition is a stand-alone server that supports up to four processors. Enterprise Edition is for large-scale deployments, server array support, multi-level policy, and computers with more than four processors. Licenses are based on the number of processors.

V-4- Symantec Antivirus Corporate Edition 10.2 – Antivirus Software:

What is an Antivirus?

Antivirus is protective software designed to defend your computer against malicious software. Malicious software or "malware" includes: viruses, Trojans, key loggers, hijackers, dialers, and other code that vandalizes or steals your computer contents.



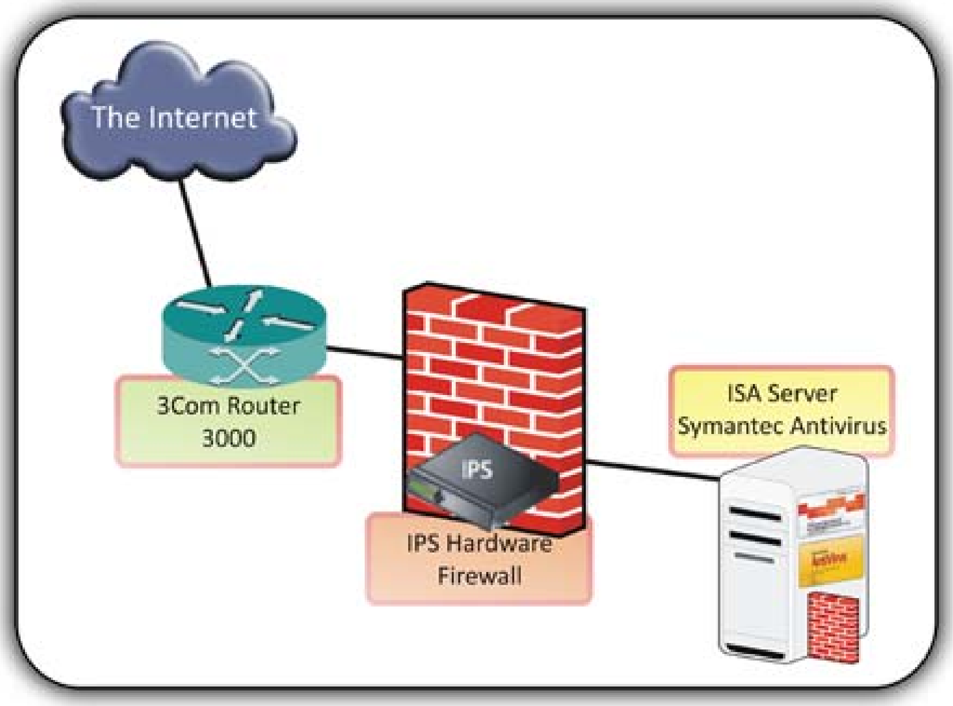
Symantec Antivirus Corporate Edition provides real-time virus and spyware protection for workstations and network servers to enable enterprise-wide system uptime. The solution automatically detects and repairs the effects of spyware, adware, viruses, and other malicious intrusions, and side-effect repair keeps systems operational during security disruptions. A comprehensive view of clients via centralized logging, threshold alerting, and graphical reporting helps transform security data into actionable information. Symantec Antivirus Corporate Edition now offers support for Microsoft® Windows Server® 2008 clients as well as Linux® clients, and is highly scalable for extensive use throughout even the largest enterprise.

Features:

- Advanced enterprise-wide virus protection and monitoring from a single management console.
- Integrated Web-based graphical reporting.
- Support for Symantec Antivirus Client on Microsoft Windows Vista and Windows Server 2008.
- Effective protection from spyware and adware.

- Symantec tamper protection guards against unauthorized antivirus access and attacks, protecting users from viruses that attempt to disable security measures.
- Backed by Symantec Security Response, the world's leading Internet security research and support organization.

Now that we have explained the mechanism and specifications of each security element that forms our scheme it is important to let you know about the implementation of it in accordance to our floor plans and devices.



Part II

WIRELESS BRIDGING

Chapter VI

NETWORK BRIDGE DESIGN

VI-1- Why Wireless?

Wireless networks have had a significant impact on the world as far back as World War II. Through the use of wireless networks, information could be sent overseas or behind enemy lines easily, efficiently and more reliably. Since then wireless networks have continued to develop and its uses have significantly grown. Cellular phones are part of huge wireless network systems. People use these phones daily to communicate with one another. Sending information overseas is possible through wireless network systems using satellites and other signals to communicate across the world. Emergency services such as the police department utilize wireless networks to communicate important information quickly. People and businesses use wireless networks to send and share data quickly whether it be in a small office building or across the world.

Another important use for wireless networks is as an inexpensive and rapid way to be connected to the Internet in countries and regions where the telecom infrastructure is poor or there is a lack of resources, like most developing countries.

Compatibility issues also arise when dealing with wireless networks. Different components not made by the same company may not work together, or might require extra work to fix compatibility issues. Wireless networks are typically slower than those that are directly connected through an Ethernet cable.

A wireless network is more vulnerable because anyone can try to break into a network broadcasting a signal. Many networks offer WEP - Wired Equivalent Privacy - security systems which have been found to be vulnerable to intrusion. Though WEP does block some intruders, the security problems have caused some businesses to stick with wired networks until security can be improved. Another type of security for wireless networks is WPA - Wi-Fi Protected

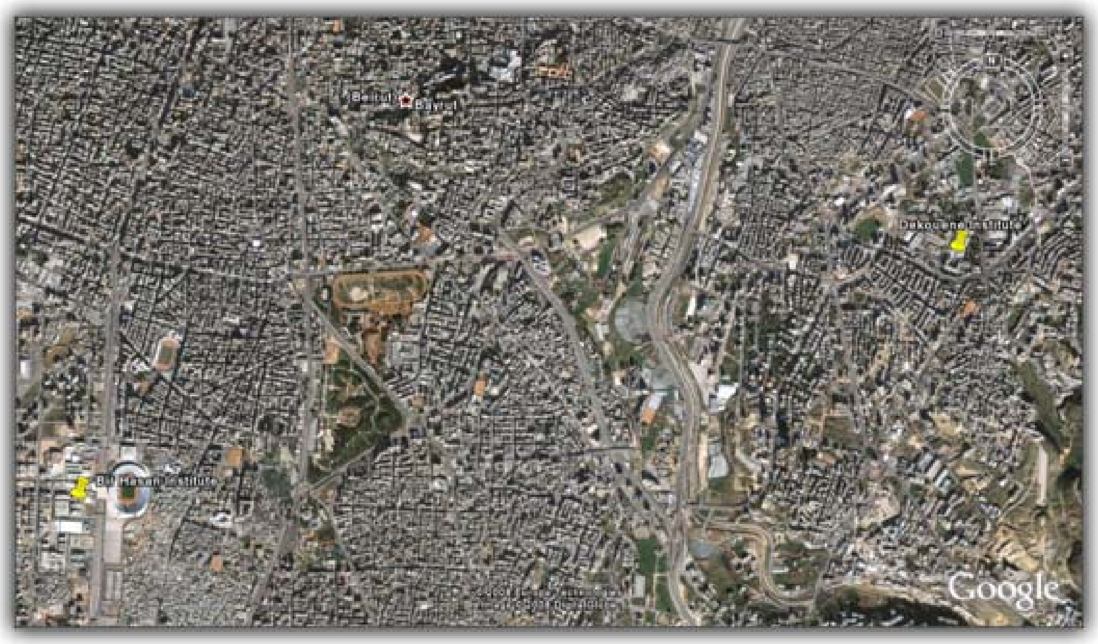
Access. WPA provides more security to wireless networks than a WEP security set up. The use of firewalls will help with security breaches which can help to fix security problems in some wireless networks that are more vulnerable.

VI-2- Microwave Technology

Microwave radio relay is a technology for transmitting digital and analog signals, such as long-distance telephone calls and the relay of television programs to transmitters, between two locations on a line of sight radio path. In microwave radio relay, radio waves are transmitted between the two locations with directional antennas, forming a fixed radio connection between the two points. Long daisy-chained series of such links form transcontinental telephone and/or television communication systems.

Because a line of sight radio link is made, the radio frequencies used occupy only a narrow path between stations (with the exception of a certain radius of each station). Antennas used must have a high directive effect; these antennas are installed in elevated locations such as large radio towers in order to be able to transmit across long distances. Typical types of antenna used in radio relay link installations are parabolic reflectors, shell antennas and horn radiators, which have a diameter of up to 4 meters. Highly directive antennas permit an economical use of the available frequency spectrum, despite long transmission distances.

In order to obtain the scales about both sites we use the program Google Earth to get both x, y coordinates and the altitude for the two sites (**Bir Hasan / Dikoueneh**).



	Site 1 (Beer Hasan)			Site 2 (Dikoueneh)		
	Degrees	Minutes	Seconds	Degrees	Minutes	Seconds
Latitude	33	52	01	33	52	46
Longitude	53	29	27	35	32	47
Ground Elevation	50 m			32 m		

Site 1 (Beer Hasan)

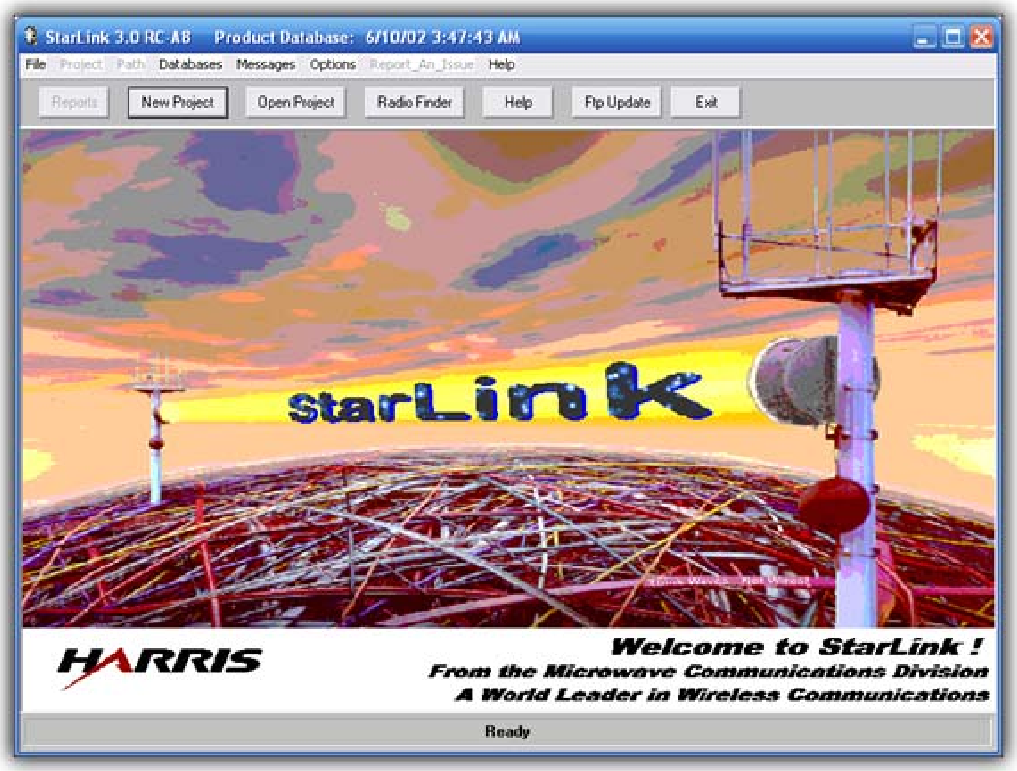
Site 2 (Dikoueneh)

At first we need to know the frequency to be used in our Microwave link in addition to the equipment that provides us with the reliability and availability that will cope with our need so we used Starlink 3.0.

It is imperative to mention that Microwave links operate on a range between 450MHz and 60GHz and among these ranges exits two types:

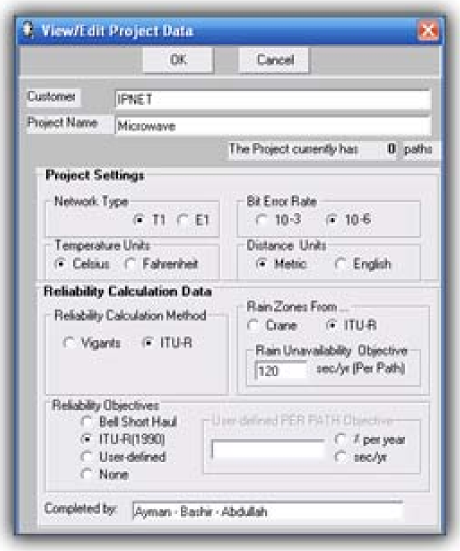
- Licensed Frequencies: between 2 and 38GHz. The advantage of the licensed frequencies is that they will insure that each operator will not cause interference to other links operating in the same area as each operator will obligated to use his own unique frequency. In order to obtain a fully legally and private licensed frequency and to obtain assurance of non-interference the following process must take place before commencing any further steps and as such we need to distribute the prior coordination notifications (PCNs) to the operator sharing the same frequency band within the coordination distance. Other parties using Microwave links in the same area are given 30 days to review our system technical data and insure it will not interfere with their Microwave links then respond to a PCN with an acceptance or objection. After the confirmation form the PCN we can move to handling the SM Licensing to obtain authorization and operate the system, the SM department requires to be provided with all the system's technical data and administrative data where all of these are submitted and file electronically afterwards submitting of the license application normally allows operation to commence immediately.

Unlicensed Frequencies: between 2.4 and 5.8GHz, the unlicensed ones will have very low link reliability since anyone can interfere and use the same frequency thus causing a disruption in frequency and weakness in the link.



Starlink 3.0: The following are the steps to calculate our path availability and reliability:

1- Creating a new project.
2- Selecting project settings
   a. Network type : T1
   b. Bit error rate: 10-6
   c. Temperature units: Celsius
   d. Distance unit: Metric
   e. Reliability calculation method: ITU-R(International Telecommunication Union)
   f. Rain Zones: ITU-R
   g. Rain unavailability objective: 120sec/yr
   h. Reliability objective: ITU-R(1990)



Customer: IPNET
Project Name: Microwave
The Project currently has 0 paths

Project Settings

Network Type: ● T1 ○ E1
Bit Error Rate: ○ 10-3 ● 10-6
Temperature Units: ● Celsius ○ Fahrenheit
Distance Units: ● Metric ○ English

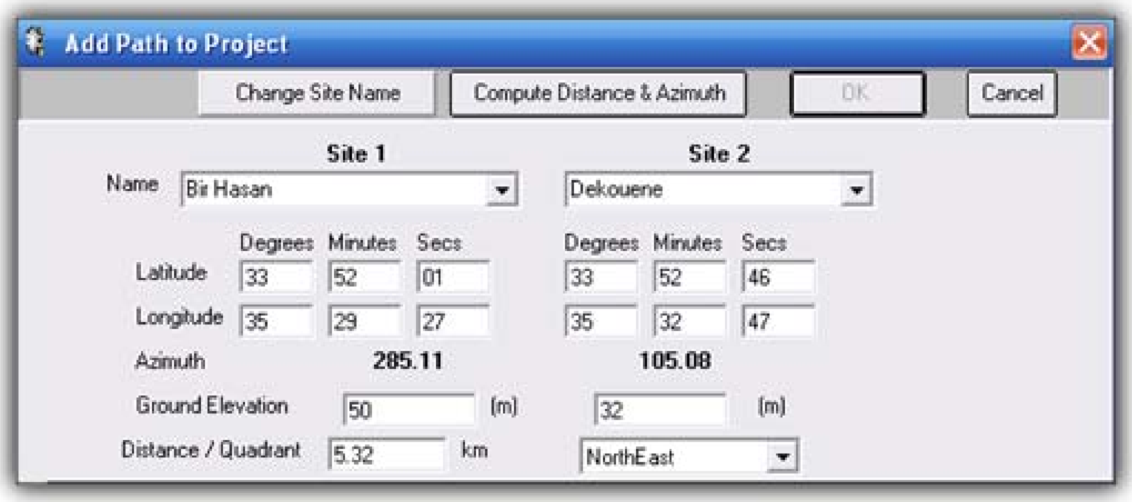
Reliability Calculation Data

Reliability Calculation Method: ○ Vigants ● ITU-R
Rain Zones From ...: ○ Crane ● ITU-R
Rain Unavailability Objective: 120 sec/yr (Per Path)

Reliability Objectives: ○ Bell Short Haul ● ITU-R(1990) ○ User-defined ○ None
User-defined PER PATH Objective: ○ % per year ○ sec/yr

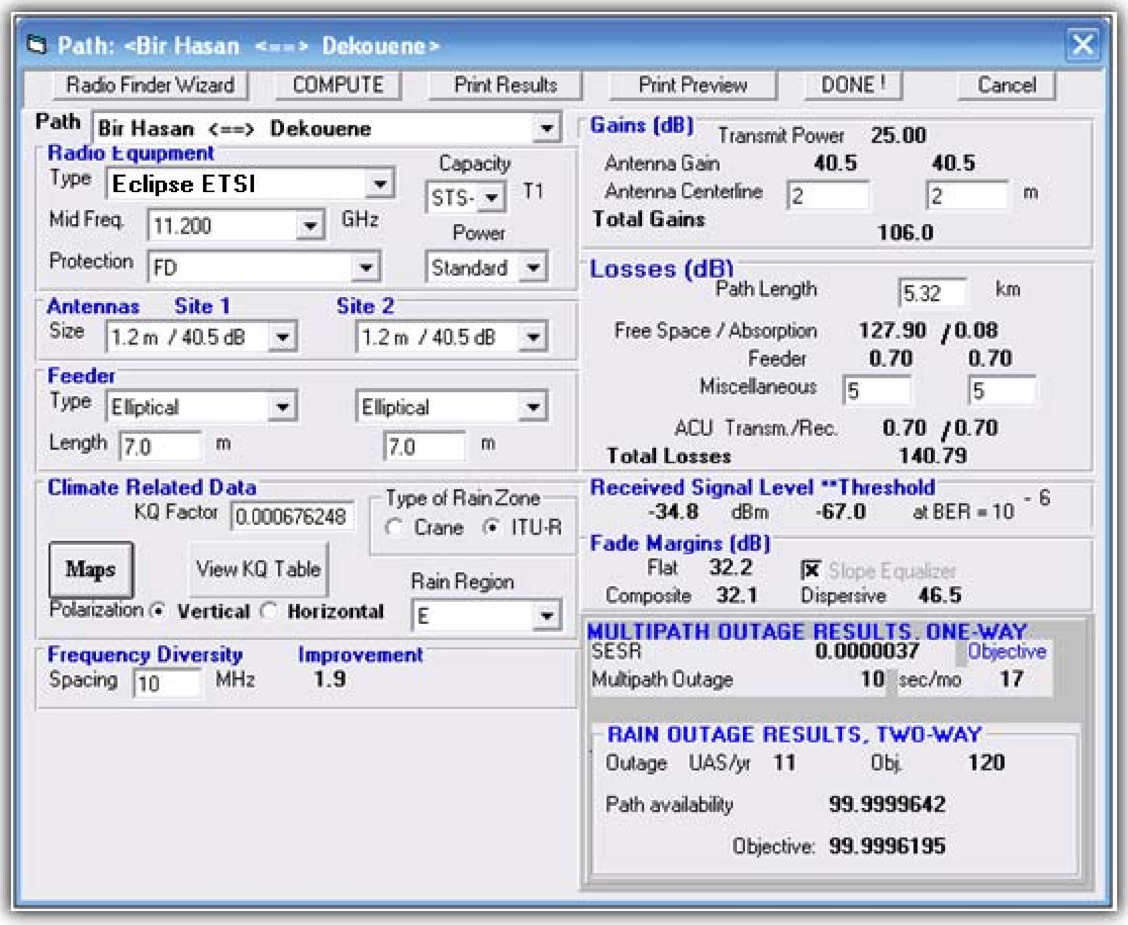
Completed by: Ayman - Bashir - Abdullah

3- Add a new path:
   a. Site1: Bir Hasan
      i. Latitude(Degrees(33)/Minutes(52)/secs(01))
      ii. Longitude(Degrees(35)/Minutes(29)/secs(27))
      iii. 50m
   b. Site2: Dikouene
      i. Latitude(Degrees(33)/Minutes(52)/Secs(46))
      ii. Longitude(Degrees(35)/Minutes(32)/Secs(47))
      iii. 32m
   c. The program automatically calculated the following:
      i. Distance: 5.32Km
      ii. Quadrant: North East
      iii. Azimuth: Site1(74.89) Site2(254.92)



	Site 1				Site 2		
Name	Bir Hasan				Dekouene		
	Degrees	Minutes	Secs		Degrees	Minutes	Secs
Latitude	33	52	01		33	52	46
Longitude	35	29	27		35	32	47
Azimuth	285.11				105.08		
Ground Elevation	50	(m)			32	(m)	
Distance / Quadrant	5.32	km			NorthEast		

4- Path reliability Calculations:



Path: <Bir Hasan <==> Dekouene>

Path: Bir Hasan <==> Dekouene

Radio Equipment
Type: Eclipse ETSI
Mid Freq. 11.200 GHz
Protection: FD
Capacity: STS- T1
Power: Standard

Antennas Site 1 / Site 2
Size: 1.2 m / 40.5 dB — 1.2 m / 40.5 dB

Feeder
Type: Elliptical — Elliptical
Length: 7.0 m — 7.0 m

Climate Related Data
KQ Factor: 0.000676248
Type of Rain Zone: ○ Crane ● ITU-R
Polarization: ● Vertical ○ Horizontal
Rain Region: E

Frequency Diversity Improvement
Spacing: 10 MHz — 1.9

Gains (dB) Transmit Power 25.00
Antenna Gain: 40.5 — 40.5
Antenna Centerline: 2 — 2 m
Total Gains: 106.0

Losses (dB)
Path Length: 5.32 km
Free Space / Absorption: 127.90 / 0.08
Feeder: 0.70 — 0.70
Miscellaneous: 5 — 5
ACU Transm./Rec.: 0.70 / 0.70
Total Losses: 140.79

Received Signal Level **Threshold
-34.8 dBm — -67.0 at BER = 10 $^{-6}$

Fade Margins (dB)
Flat: 32.2 ☒ Slope Equalizer
Composite: 32.1 Dispersive: 46.5

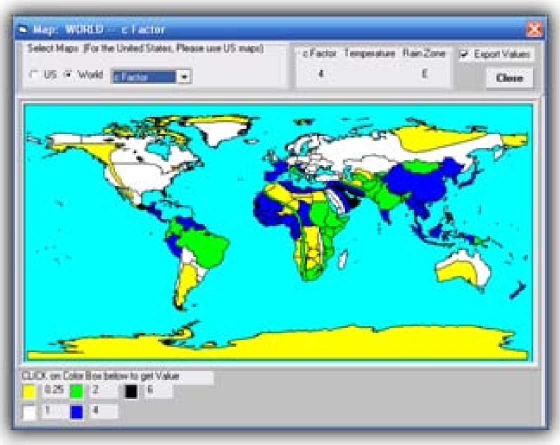
MULTIPATH OUTAGE RESULTS, ONE-WAY
SESR: 0.0000037 Objective
Multipath Outage: 10 sec/mo 17

RAIN OUTAGE RESULTS, TWO-WAY
Outage UAS/yr: 11 Obj. 120
Path availability: 99.9999642
Objective: 99.9996195

a. Radio Equipment:
   i. Type: ECLIPSE ETSI
   ii. Frequency: 11.200GHz
   iii. Capacity: 3 DS TS
   iv. Protection: FD (Frequency Diversity)
   v. Power: Standard
   vi. Antennas:
      1. Site1: 1.2m/ 40.5 dB
      2. Site2: 1.2m/ 40.5 dB
   vii. Feeder:
      1. Type: Elliptical
      2. Length: 7m

viii. Climate Related Data: the program calculates the KQ factor after we specify the region our link and as such we have:

1. cFactor: 4



Map: WORLD -- c Factor

Select Maps (For the United States, Please use US maps)

○ US ● World c Factor

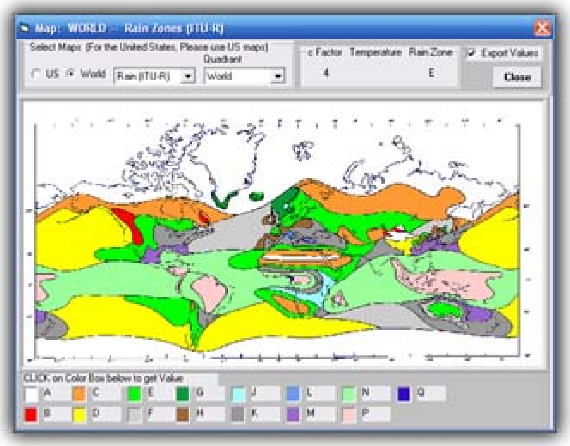
c Factor	Temperature	Rain Zone
4		E

☑ Export Values

CLICK on Color Box below to get Value

🟨 0.25 🟩 2 ⬛ 6
⬜ 1 🟦 4

2. Rain Zone: E



Map: WORLD -- Rain Zones (ITU-R)

Select Maps (For the United States, Please use US maps)

○ US ● World Rain (ITU-R) Quadrant World

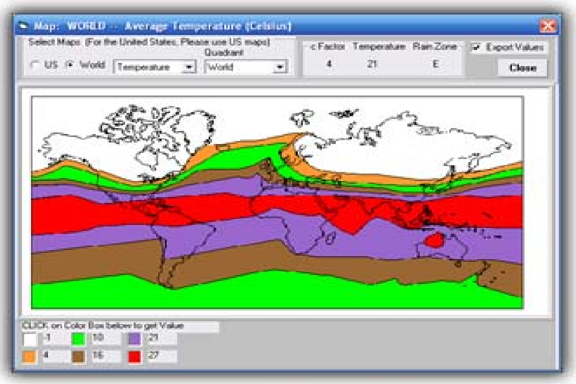
c Factor	Temperature	Rain Zone
4		E

☑ Export Values

CLICK on Color Box below to get Value

⬜ A 🟧 C 🟩 E 🟩 G 🟦 J 🟦 L 🟩 N 🟦 Q
🟥 B 🟨 D ⬜ F 🟫 H ⬛ K 🟪 M 🟥 P

3. Temperature: 21



Map: WORLD -- Average Temperature (Celsius)

Select Maps (For the United States, Please use US maps)

○ US ● World Temperature Quadrant World

c Factor	Temperature	Rain Zone
4	21	E

☑ Export Values

CLICK on Color Box below to get Value

⬜ -1 🟩 10 🟪 21
🟧 4 🟫 16 🟥 27

ix. Frequency Diversity:
    1. Spacing: 10.0MHz (It improves our signal by 1.9)

x. Gains:
    1. Transmist power: 25.00 dB
    2. Antenna gain: 40.5 dB
    3. Antenna Centerline: 0m
    4. Total gains: 106.0

xi. Losses
    1. Path lengh: 5.32Km
    2. Free Space/Absorption: 127.90 / 0.08 dB
    3. Feeder: 0.70 dB
    4. ACU Transmission: 0.00
    5. Total Losses: 128.25 dB
    6. Miscellaneous: 5.00 dB

Using the input parameters listed above the StarLink program generated and calculated the Multi-path Outage, Rain Outage, Fade Margins and Path Availability and as such there were the results:

Signal Strength	
Received Signal Level	Threshold
-34.8 dBm	-67.0 dBm

Fade Margins		
Flat	Composite	Dispersive
32.2 dB	32.1 dB	46.5 dB

Multi-path Outage Results One-Way		
SESR	Muti-path Outage	Objective
0.0000054	14	17

SESR: Severely-Errored Second Ratio

Rain Outage Results Two-Way			
Outage UAS/yr	Objective	Path Availablity	Objective
11	120	99.9999642%	99.9996195%

After we have studied the path reliability of the wireless bridge, we have to determine if the connecting link is fault free and has the capability of connecting two points without any physical interference, thus we need to use a software called **ICS Telecom** from **ATDI**

ICS telecom

ATDI

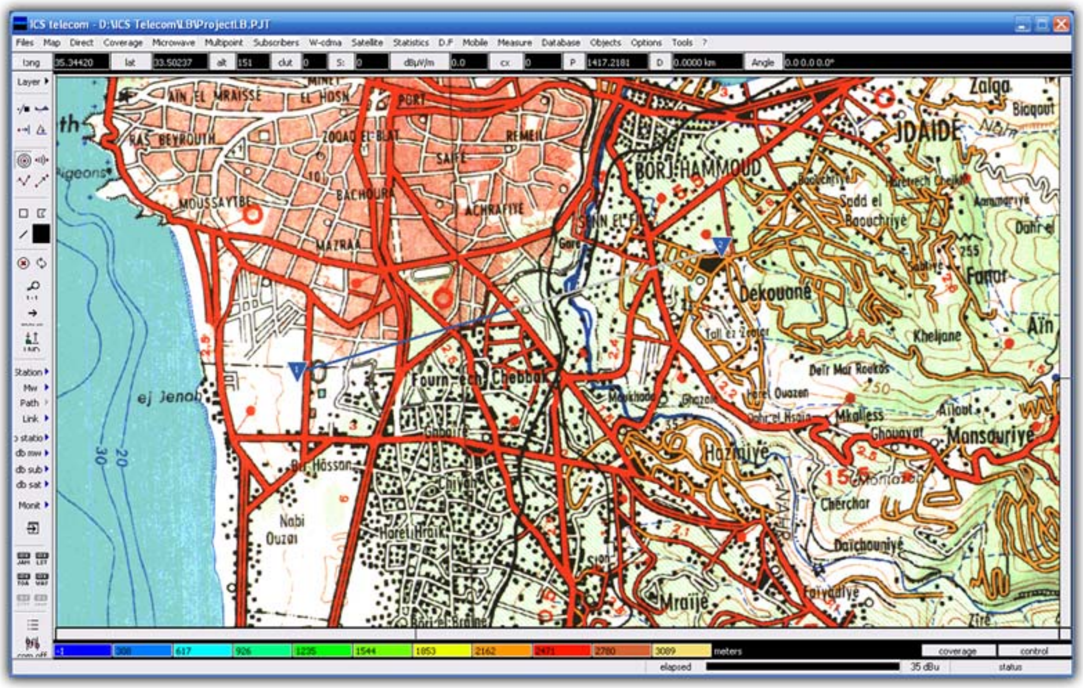
www.atdi.com

(c) ATDI 1991-2002 Authors: P. and D. Missud

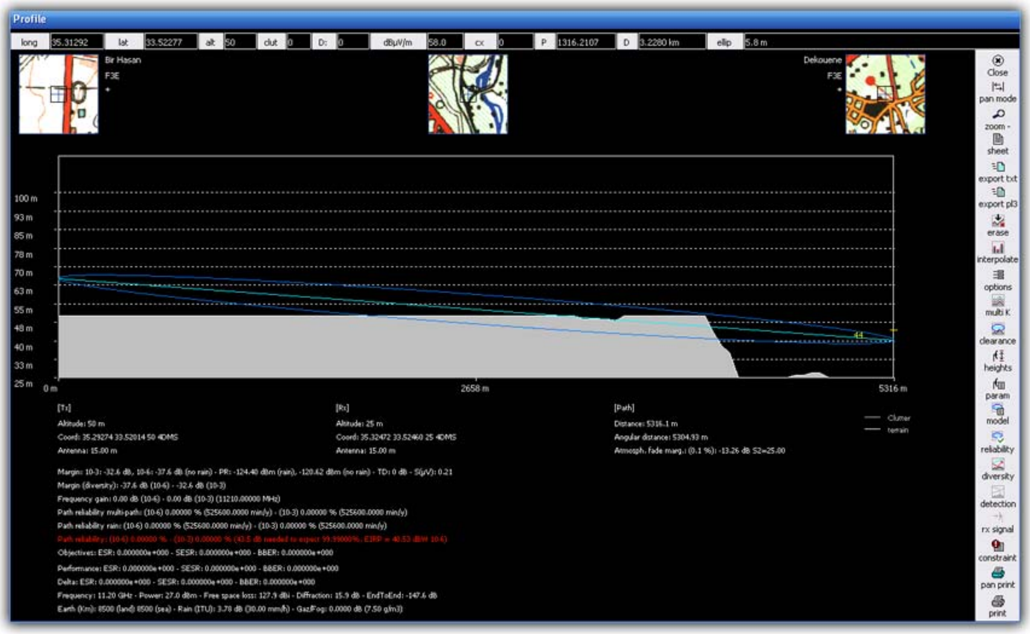
We imported into the ICS Telecom the map of Lebanon which will enable us to have the most accurate results regarding our link, depending on the coordinates brought from Google Earth we have plotted the following points

	Site 1 (Beer Hasan)			Site 2 (Dikoueneh)		
	Degrees	Minutes	Seconds	Degrees	Minutes	Seconds
Latitude	33	52	01	33	52	46
Longitude	53	29	27	35	32	47
Ground Elevation	50 m			32 m		

then we also added the frequency, gains and losses so we had the following result


ICS telecom - D:\ICS Telecom\LB\ProjectLB.PJT
Files Map Direct Coverage Microwave Multipoint Subscribers W-cdma Satellite Statistics D.F Mobile Measure Database Objects Options Tools ?
long 35.34420 lat 33.50237 alt 151 clut 0 S: 0 dBµV/m 0.0 cx 0 P 1417.2181 D 0.0000 km Angle 0.0.0.0.0°
meters
coverage
control
elapsed
35 dBu
status

after checking the link’s profile we have noticed that the different in elevations between the two sites makes it impossible to obtain a clear line of site as show in the following figure.

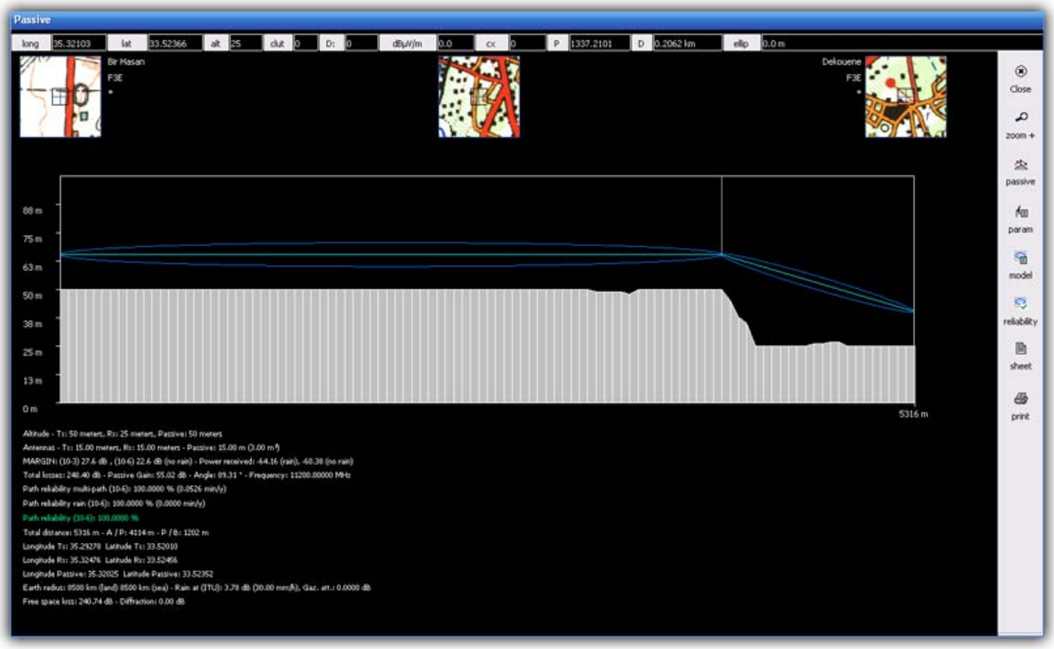


[Tx]
Altitude: 50 m
Coord: 35.29274 33.52014 50 4DMS
Antenna: 15.00 m

[Rx]
Altitude: 25 m
Coord: 35.32472 33.52460 25 4DMS
Antenna: 15.00 m

[Path]
Distance: 5316.1 m
Angular distance: 5304.93 m
Atmosph. fade marg.: (0.1 %): -13.26 dB S2=25.00

```
Margin: 10-3: -32.6 dB, 10-6: -37.6 dB (no rain) - PR: -124.40 dBm (rain), -120.62 dBm (no rain) - TD: 0 dB - S(µV): 0.21
Margin (diversity): -37.6 dB (10-6) - -32.6 dB (10-3)
Frequency gain: 0.00 dB (10-6) - 0.00 dB (10-3) (11210.00000 MHz)
Path reliability multi-path: (10-6) 0.00000 % (525600.0000 min/y) - (10-3) 0.00000 % (525600.0000 min/y)
Path reliability rain: (10-6) 0.00000 % (525600.0000 min/y) - (10-3) 0.00000 % (525600.0000 min/y)
Path reliability: (10-6) 0.00000 % - (10-3) 0.00000 % (43.5 dB needed to expect 99.99000%, EIRP = 40.53 dBW 10-6)
Objectives: ESR: 0.000000e+000 - SESR: 0.000000e+000 - BBER: 0.000000e+000
Performance: ESR: 0.000000e+000 - SESR: 0.000000e+000 - BBER: 0.000000e+000
Delta: ESR: 0.000000e+000 - SESR: 0.000000e+000 - BBER: 0.000000e+000
Frequency: 11.20 GHz - Power: 27.0 dBm - Free space loss: 127.9 dBi - Diffraction: 15.9 dB - EndToEnd: -147.6 dB
Earth (Km): 8500 (land) 8500 (sea) - Rain (ITU): 3.78 dB (30.00 mm/h) - Gaz/Fog: 0.0000 dB (7.50 g/m3)
```



long 35.32103 lat 33.52366 alt 25 clut 0 D: 0 dBµV/m 0.0 cx 0 P 1337.2101 D 0.2062 km ellip 0.0 m

```
Altitude - Tx: 50 meters, Rx: 25 meters, Passive: 50 meters
Antennas - Tx: 15.00 meters, Rx: 15.00 meters - Passive: 15.00 m (3.00 m²)
MARGIN: (10-3) 27.6 dB , (10-6) 22.6 dB (no rain) - Power received: -64.16 (rain), -60.38 (no rain)
Total losses: 248.40 dB - Passive Gain: 55.02 dB - Angle: 89.31 ° - Frequency: 11200.00000 MHz
Path reliability multi-path (10-6): 100.0000 % (0.0526 min/y)
Path reliability rain (10-6): 100.0000 % (0.0000 min/y)
Path reliability (10-6): 100.0000 %
Total distance: 5316 m - A / P: 4114 m - P / B: 1202 m
Longitude Tx: 35.29278  Latitude Tx: 33.52010
Longitude Rx: 35.32476  Latitude Rx: 33.52456
Longitude Passive: 35.32025  Latitude Passive: 33.52352
Earth radius: 8500 km (land) 8500 km (sea) - Rain at (ITU): 3.78 dB (30.00 mm/h), Gaz. att.: 0.0000 dB
Free space loss: 240.74 dB - Diffraction: 0.00 dB
```

Microwave link mirror:

As a result of ICS Telecom program and as shown in the above image we need to implement a mirror between the two points in order to achieve a valid line of site. This mirror will be place on these coordinates x(33/52/35.43) y(35/32/13.49).

The Microwave link mirror is in fact a back-to-back antenna with a small radio that does nothing but forwards the signal between the two sites, this radio is TRuePoint from Harris Systems. This radio ensures the reliability we need for our link and almost lossless.

VI-3- Climate Related Data:

The path availability is affected by three climatic factor

- c-Factor:
- Temperature
- Rain Zone

StarLink provides us with maps for average values of c-Factor, temperature and Rain Zone in our region by the corresponding values respectively

We used a program ICS Telecom to plot the two sites on a map using the coordinates obtained from before 4, 21^C, E and all termed by the ITU (International Telecommunication Union).

Frequency Diversity:

Multi-path interference affects mainly lower frequencies below 18GHz this happens when the reflected signal arrive slightly later than the direct signal path. It reduces the ability of the receiver to correctly distinguish the data carried on the signal. Thus we used **Frequency Diversity** protection

Spacing between the two frequencies is 10.00MHz

Received Signal Strength:

Threshold: the receiver threshold considered depends both on the required output performance, i.e., at base- band, and on the type of interference. If the characteristics of the interference resemble AWGN, the relation between the required signal-to-noise ratio at the detector output (SNR) and expressions for z are well known

Received Signal Level is -34.8 dBm while our equipment threshold is -67.0 dBm which is very good because the threshold is higher than the received signal level.

Fade Margin:

Also called the System Operating Margin (SOM) which is the difference (measured in dB) between the nominal signal level received at one end of a radio and the signal level required (Receiver sensitivity) by that radio to assure that a packet of data is decoded without error, in other words, the Fade Margin is the difference between the signal received and the radio's specified receiver's sensitivity.

Multi-path Outage:

Multi-path outage: Multipath propagation occurs when copies of a signal arrive at a receiver at different times as a result of having followed different paths through the atmosphere. If they are out of phase, these signals may cancel at the receiver causing an outage.

Rain Outage:

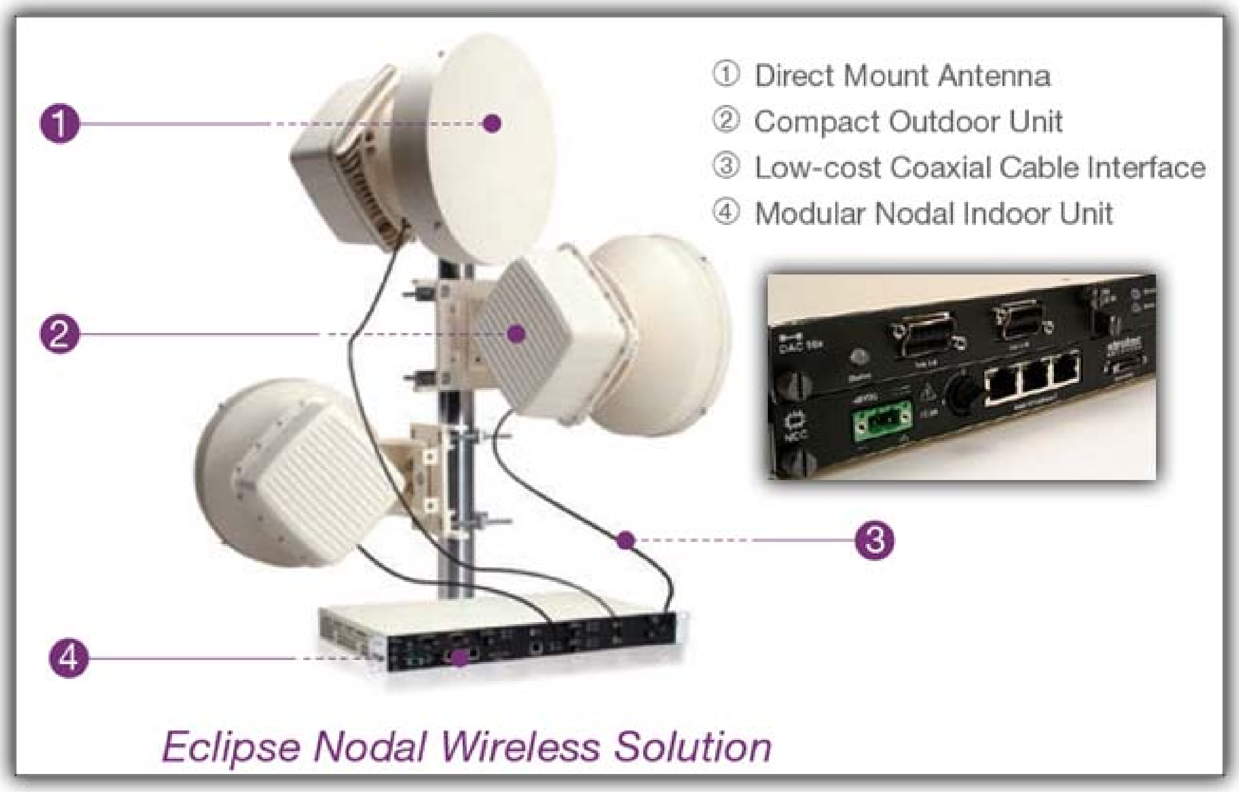
Path loss increase due to high intensity rain is a flat fading (non-frequency selective) phenomenon. It is not improved by diversity reception since both reception branches will experience the same degree of rain-cause fading at the same time. Rain outage is computer relative to the thermal fade margin.

Coordinates:

Bir Hasan: x(35.29274) y(33.52014) l(50)

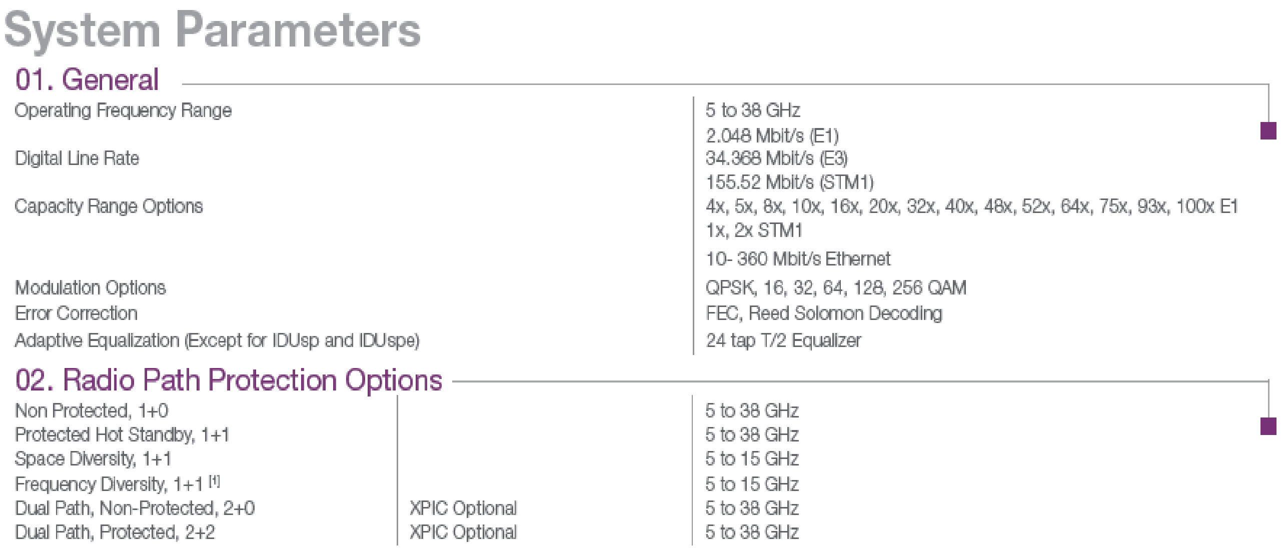
Radio Equipment:

From a vast range of radio types and after contacting with **HARRIS Stratex** support which is located in Melbourne, Florida where we provided them with the characteristics of the connection we are implementing and they suggested that we should use **Eclipse ETSI** as our radio equipment which is capable of enduring the frequency which we need (11.200 GHz) and can support Frequency Diversity protection type.


1
2
3
4
① Direct Mount Antenna
② Compact Outdoor Unit
③ Low-cost Coaxial Cable Interface
④ Modular Nodal Indoor Unit

Eclipse Nodal Wireless Solution

The following is a list of the parameters:



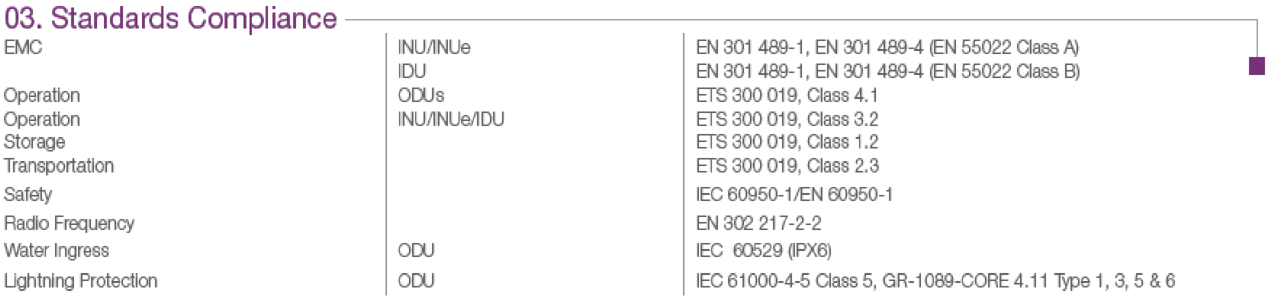
System Parameters

01. General

Operating Frequency Range	5 to 38 GHz
Digital Line Rate	2.048 Mbit/s (E1) 34.368 Mbit/s (E3) 155.52 Mbit/s (STM1)
Capacity Range Options	4x, 5x, 8x, 10x, 16x, 20x, 32x, 40x, 48x, 52x, 64x, 75x, 93x, 100x E1 1x, 2x STM1 10- 360 Mbit/s Ethernet
Modulation Options	QPSK, 16, 32, 64, 128, 256 QAM
Error Correction	FEC, Reed Solomon Decoding
Adaptive Equalization (Except for IDUsp and IDUspe)	24 tap T/2 Equalizer

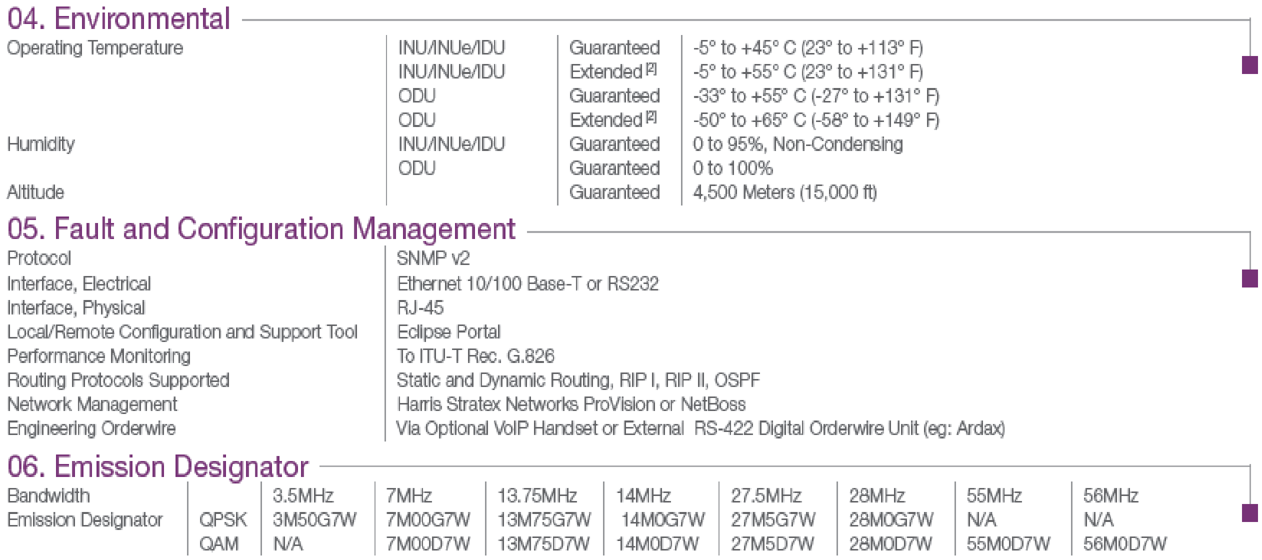
02. Radio Path Protection Options

Non Protected, 1+0		5 to 38 GHz
Protected Hot Standby, 1+1		5 to 38 GHz
Space Diversity, 1+1		5 to 15 GHz
Frequency Diversity, 1+1 [4]		5 to 15 GHz
Dual Path, Non-Protected, 2+0	XPIC Optional	5 to 38 GHz
Dual Path, Protected, 2+2	XPIC Optional	5 to 38 GHz



03. Standards Compliance

EMC	INU/INUe	EN 301 489-1, EN 301 489-4 (EN 55022 Class A)
	IDU	EN 301 489-1, EN 301 489-4 (EN 55022 Class B)
Operation	ODUs	ETS 300 019, Class 4.1
Operation	INU/INUe/IDU	ETS 300 019, Class 3.2
Storage		ETS 300 019, Class 1.2
Transportation		ETS 300 019, Class 2.3
Safety		IEC 60950-1/EN 60950-1
Radio Frequency		EN 302 217-2-2
Water Ingress	ODU	IEC 60529 (IPX6)
Lightning Protection	ODU	IEC 61000-4-5 Class 5, GR-1089-CORE 4.11 Type 1, 3, 5 & 6



04. Environmental

Operating Temperature	INU/INUe/IDU	Guaranteed	-5° to +45° C (23° to +113° F)
	INU/INUe/IDU	Extended [2]	-5° to +55° C (23° to +131° F)
	ODU	Guaranteed	-33° to +55° C (-27° to +131° F)
	ODU	Extended [2]	-50° to +65° C (-58° to +149° F)
Humidity	INU/INUe/IDU	Guaranteed	0 to 95%, Non-Condensing
	ODU	Guaranteed	0 to 100%
Altitude		Guaranteed	4,500 Meters (15,000 ft)

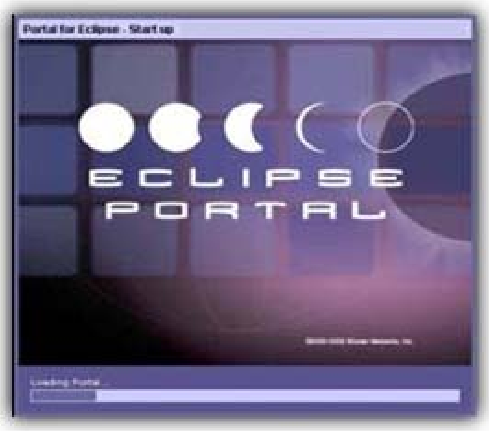
05. Fault and Configuration Management

Protocol	SNMP v2
Interface, Electrical	Ethernet 10/100 Base-T or RS232
Interface, Physical	RJ-45
Local/Remote Configuration and Support Tool	Eclipse Portal
Performance Monitoring	To ITU-T Rec. G.826
Routing Protocols Supported	Static and Dynamic Routing, RIP I, RIP II, OSPF
Network Management	Harris Stratex Networks ProVision or NetBoss
Engineering Orderwire	Via Optional VoIP Handset or External RS-422 Digital Orderwire Unit (eg: Ardax)

06. Emission Designator

Bandwidth		3.5MHz	7MHz	13.75MHz	14MHz	27.5MHz	28MHz	55MHz	56MHz
Emission Designator	QPSK	3M50G7W	7M00G7W	13M75G7W	14M0G7W	27M5G7W	28M0G7W	N/A	N/A
	QAM	N/A	7M00D7W	13M75D7W	14M0D7W	27M5D7W	28M0D7W	55M0D7W	56M0D7W

Radio Configurations:



Eclipse ETSI microwave radio provides a graphical interface for monitoring the microwave link and applying the administrator configurations. This software is the Eclipse Portal

The following is the set of configurations applied to Eclipse radio using Eclipse Portal on both sites (Beer Hasan and Dekouene):

System Configuration:

IP Address: 172.16.64.11

Subnet Mask: 255.255.224.0

Wireless Radio Access Point Configuration:

SSID: IPNET-Link

Frequency: 11.200 GHz

Signal Protection: Frequency Diversity 10 MHz

Signal Encryption: WEP

Data Encryption: 128bits

WEP Mode: HEX

WEP Key: A105FC4A7B

Power: Standard

Console Configuration:

Console Password: 1pN3t*!

Telnet Password: t0k3nr1NG^

HTTP Access: Yes

HTTP Username: controller

HTTP Password: 1Pn3T*!

MAC Address Control: 00 E1 EF 74 4B 3F

VI-4- Antenna:

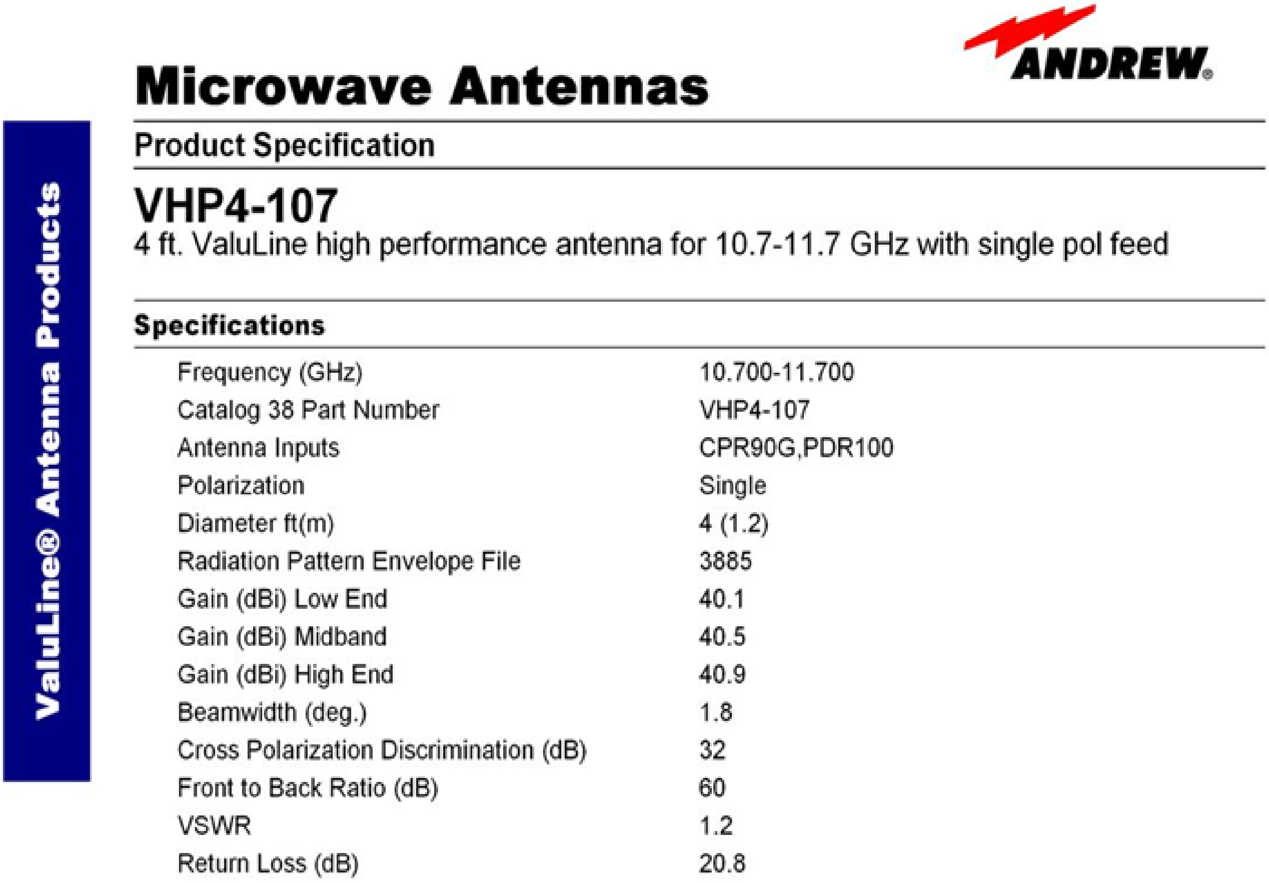
After a detailed study of the availability and reliability of our microwave link by the StarLink Microwave Link Calculator software, we learned that we should use at least 1.2m diameter antenna with gain not less than 40dB, so we decided to use a product from Andrew Company which has a variety of antennas models that suits all kinds of microwave links.

The best choice was the ValuLine family antenna VHP4-107 made by Andrew Company, this antenna is the best choice for the frequency we will transmit the data on, with the minimal loss in signal.

ValuLine High Performance Shielded Antennas (VHP Series):

ValuLine VHP Series standard performance unshielded antennas provide a cost-effective solution for all terrestrial microwave systems operating at frequencies between 7 GHz and 60 GHz. These antennas are available in both single and dual polarized configurations and sized from 1 ft (0.3 m) to 6 ft (1.8 m) in diameter.

A software from Andrew “ANTDES” from Andrew PowerTools, helped us in a detailed and complete specifications of the chosen product, in addition to internet WebPages.



ValuLine® Antenna Products

ANDREW.

Microwave Antennas

Product Specification

VHP4-107

4 ft. ValuLine high performance antenna for 10.7-11.7 GHz with single pol feed

Specifications

Frequency (GHz)	10.700-11.700
Catalog 38 Part Number	VHP4-107
Antenna Inputs	CPR90G,PDR100
Polarization	Single
Diameter ft(m)	4 (1.2)
Radiation Pattern Envelope File	3885
Gain (dBi) Low End	40.1
Gain (dBi) Midband	40.5
Gain (dBi) High End	40.9
Beamwidth (deg.)	1.8
Cross Polarization Discrimination (dB)	32
Front to Back Ratio (dB)	60
VSWR	1.2
Return Loss (dB)	20.8

The following is the technical characteristics of the microwave antenna chosen:

Adjustment:

Fine Adjustments degrees:

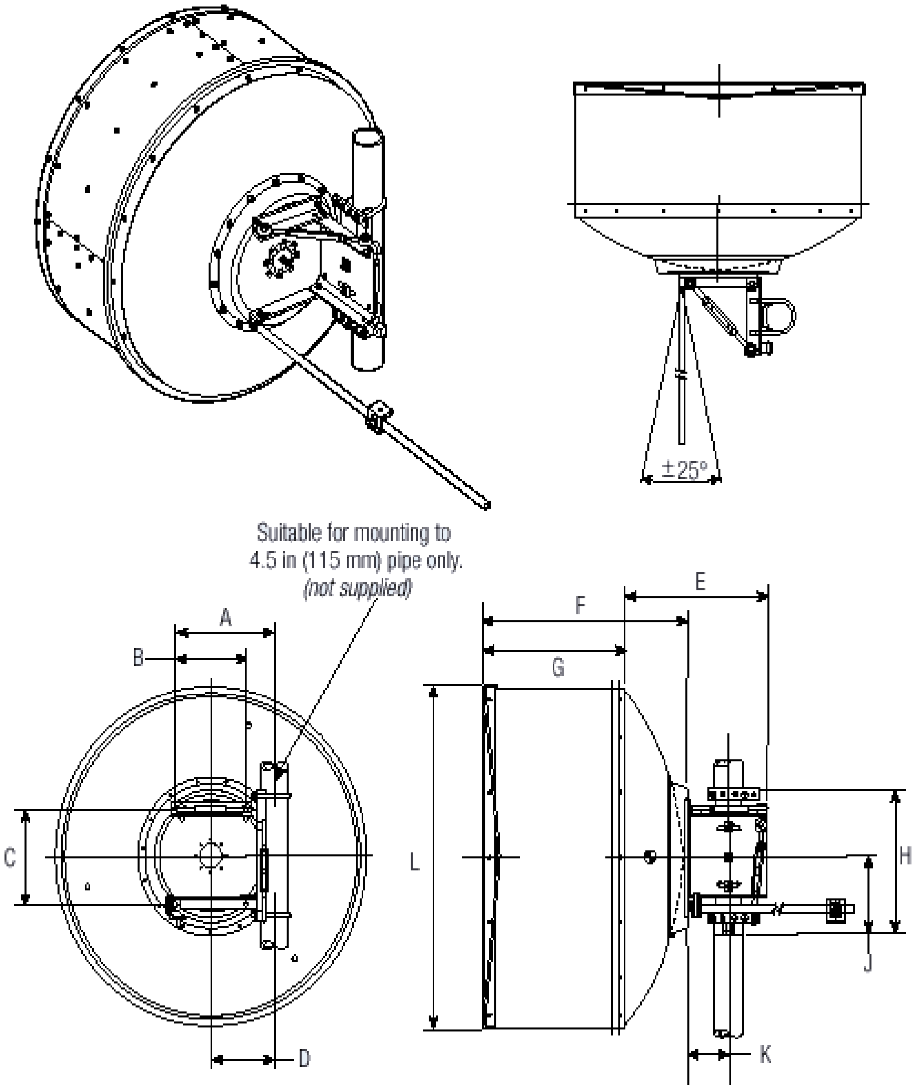
Azimuth: ±15

Elevation: ± 20

Survival Wind Speed: 200km/h

Net Weight: 57.0 kg

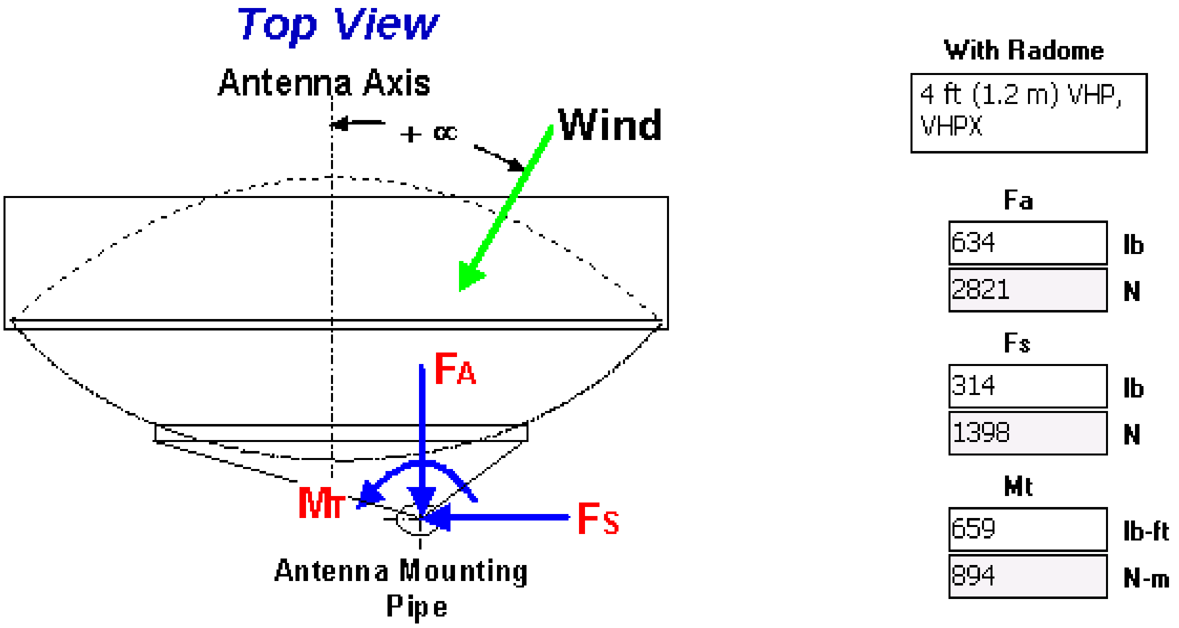
Antenna Dimensions:



Suitable for mounting to 4.5 in (115 mm) pipe only. *(not supplied)*

	in (mm)
A	16.2 (411)
B	11.6 (295)
C	14.2 (361)
D	10.4 (264)
E	21.4 (544)
F	23.4 (594)
G	14.7 (373)
H	20.8 (528)
I	
J	11.1 (288)
K	6.5 (165)
L	49.1 (1247)

Wind force is an important factor to study while planning to deploy the antenna, because any movement in millimeters could interrupt the microwave link. Therefore we had to make a complete research about the wind force on the chosen antenna depending on its dimensions and size.



With Radome

4 ft (1.2 m) VHP, VHPX

Fa

634	lb
2821	N

Fs

314	lb
1398	N

Mt

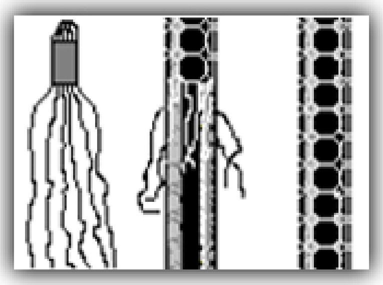
659	lb-ft
894	N-m

Those calculations were made on a Wind Force speed of 200km/h which is the maximum wind speed the region of our microwave link can reach.

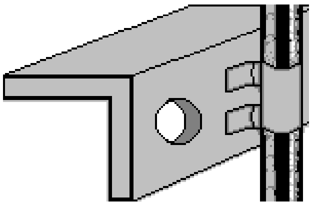
VI-5-Antenna Construction Tools:

The Antenna we are deploying is a roof top antenna, therefore we've chosen the tools which will help us fix the antenna in a precise way to face wind forces and other factors.

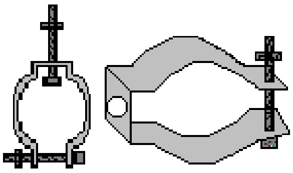
Standard Hoisting Grip:



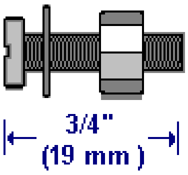
Type of Mount: Angle/Pre-Punched Steel:



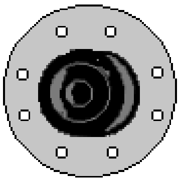
Cable Attachment: Standard Hanger Kit:



Mounting Hardware: Standard Hanger Attachment Hardware 3/4 long:



As we have to put the radio transmitter inside a small room (closet) in both sites.So we have to use an Entrance Plate so we used a Single Entrance Wall/Roof Feed Thru Assembly:



Then we used a grounding toolkit to provide a ground line for the antenna as following:

Standard Grounding Kit with wire length of 600 Inches and a factory attached One-Hole lug:

VI-6-Cable and Feeder:

After Choosing the Antenna we move to the link (Cable and feeder) between the antenna and the Radio transmitter device. We also chosen Andrew company to provide us with the suitable product depending also on the frequency used the margin of loss (dB) we can take.

There are three types of cables can be used between antenna and the radio device:

Air Coax	Foam Coax	Elliptical Waveguide

Air Coaxial Cable

The rigid coaxial line consists of a central, insulated wire (inner conductor) mounted inside a tubular outer conductor. In some applications, the inner conductor is also tubular. The inner conductor is insulated from the outer conductor by insulating spacers or beads at regular intervals. The spacers are made of Pyrex, polystyrene, or some other material that has good insulating characteristics and low dielectric losses at high frequencies.

The chief advantage of the rigid line is its ability to minimize radiation losses. The electric and magnetic fields in a two-wire parallel line extend into space for relatively great distances and radiation losses occur. However, in a coaxial line no electric or magnetic fields extend outside of the outer conductor. The fields are confined to the space between the two conductors, resulting in a perfectly shielded coaxial line. Another advantage is that interference from other lines is reduced. The rigid line has the following disadvantages:

1) It is expensive to construct
2) It must be kept dry to prevent excessive leakage between the two conductors;
3) Although high-frequency losses are somewhat less than in previously mentioned lines, they are still excessive enough to limit the practical length of the line.

Leakage caused by the condensation of moisture is prevented in some rigid line applications by the use of an inert gas, such as nitrogen, helium, or argon. It is pumped into the dielectric space of the line at a pressure that can vary from 3 to 35 pounds per square inch. The inert gas is used to dry the line when it is first installed and pressure is maintained to ensure that no moisture enters the line. Flexible coaxial lines are made with an inner conductor that consists of flexible wire insulated from the outer conductor by a solid, continuous insulating material. The outer conductor is made of metal braid, which gives the line flexibility. Early attempts at gaining flexibility involved using rubber insulators between the two conductors. However, the rubber insulators caused excessive losses at high frequencies.

In our link it is possible to use any of the cables but in the case of the Elliptical ones we would then have to add a special module to the radio to support an Elliptical feeder which will increase the cost, on the other hand using the Foam Coaxial cable would decrease the insertion loss (dB) where as our preferable solution is the Air Coaxial cable which has a higher rate of insertion loss knowing that our link can endure such a loss. Thus we used the Air Coaxial cable of part number HST1-50 from Andrew company with the following characteristics:

Air Coaxial Cable Characteristics					
Part Number	**Frequency Band(MHz)**	**Insertion Loss (dB)**	**Efficiency (%)**	**Peak Power (kW)**	**Average Power (kW)**
HST1-50	0.5 – 18000	5.31	29.43	6.4	0.15

<u>Foam Coaxial Cable</u>

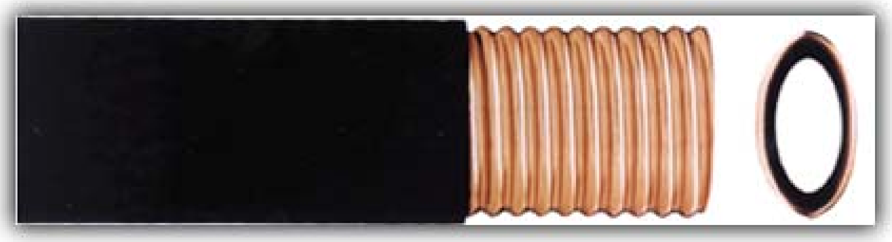
Foam dielectric cables combine a remarkable flexibility with high strength and superior electrical performance. The cable construction allows easy handling and easy preparation for attachment of connectors together with high resistance to connector pull-off.

Foam dielectric cables have the following characteristics:

- High flexibility
- High crush resistance
- Low attenuation
- High power rating
- Longitudinal uniformity
- Small reflection factor
- High screening effectiveness
- Resistant to hostile environments

Elliptical Waveguide

Radio Frequency Systems is the originator and designer of continuous seam welded corrugated transmission lines. FLEXWELL® is RFS's brand name for the highest quality, best performing, and most reliable elliptical waveguide in the industry. FLEXWELL® designs are constantly proven successful in thousands of installations throughout the world. FLEXWELL® elliptical waveguide is the ideal choice for microwave antenna systems and offers quality and reliability that you can depend on.



FLEXWELL® waveguides are available in a wide selection of frequency bands throughout the 3 GHz to 40 GHz microwave bands. The waveguides are equivalent in sizes to rectangular waveguide R32 (WR284) through R320 (WR28).

Pricing:

Microwave Link Equipment				
	ITI Building	**Dikoueneh Building**	**Qty.**	**Price**
Eclipse ETS Microwave Radio	✓	✓	**2**	2400$
Eclipse 2Years Warranty	✓	✓	**2**	150$
Andrew VHP4-107 Microwave Antenna	✓	✓	**2**	800$
Harris TRuePoint Mirror + 2 Antennas	✓	✓	**1**	1300$
Elliptical Waveguide + Feeder	✓	✓	**2**	130$
Grounding Kit	✓	✓	**2**	90$
Weather proofing kit	✓	✓	**2**	40$
Cable Entry Wall Feed-Thru Assembly	✓	✓	**2**	36$
Standard Hangers	✓	✓	**2**	25$
Wall mounted rack	✓	✓	**2**	260$
Totals				**5231$**

Wi-Fi Equipment			
	ITI Building	**Qty**	**Price**
3Com Wireless 8760 Access Point	✓	**1**	370$
3Com 8dBi Dual-Band Omni Antenna	✓	**1**	170$
Totals			**540$**

Switches			
	ITI Building	**Qty.**	**Price**
3Com 4400 24 ports	✓	**8**	1580$
3Com 4400 48 ports	✓	**1**	3200$
3Com 2126-G 24 ports	✓	**5**	94$
3Com 2126-G 48 ports	✓	**4**	123$
3Com 5500 26 ports	✓	**2**	7000$
1000Base-SX Module	✓	**16**	490$
1000Base-SX SFP Module	✓	**2**	330$
Totals			**12817$**

Cables				
	ITI Building	**Qty. in meters**	**Unit Price /m**	**Price**
UTP Cables	✓	5000	0.3305$	1652.5$
STP Cables	✓	430	0.55$	236.5$
Single-Mode Fiber Optic Cables	✓	74	33$	2442$
Multi-Mode Fiber Optic Cables	✓	139	27$	3753$
UTP/STP/in-building Fiber Raceways	✓	820	0.18$	147.5$
Underground Fiber Optic Raceways	✓	70	8$	560$
Outlets	✓	300 outlet	6$	1800$
Totals				**10592$**

Servers Hardware			
	ITI Building	**Qty**	**Price**
Server Box	✓	**5**	23725$
Monitor/Keyboard/Mouse	✓	**2**	1000$
KVM	✓	**1**	70$
Totals			**24795$**

Servers Software			
	ITI Building	**Qty**	**Price**
Microsoft Windows Server 2008	✓	**1**	1000$
Microsoft ISA Server 2006	✓	**1**	170$
Symantec Antivirus Corporate Edition	✓	**1**	400$
Totals			**1570$**

Hardware Firewall and Router			
	ITI Building	**Qty**	**Price**
3Com TippingPoint 50 Firewall	✓	**1**	2900$
3Com 3000 HDSL Router	✓	**1**	330$
Totals			**3230$**

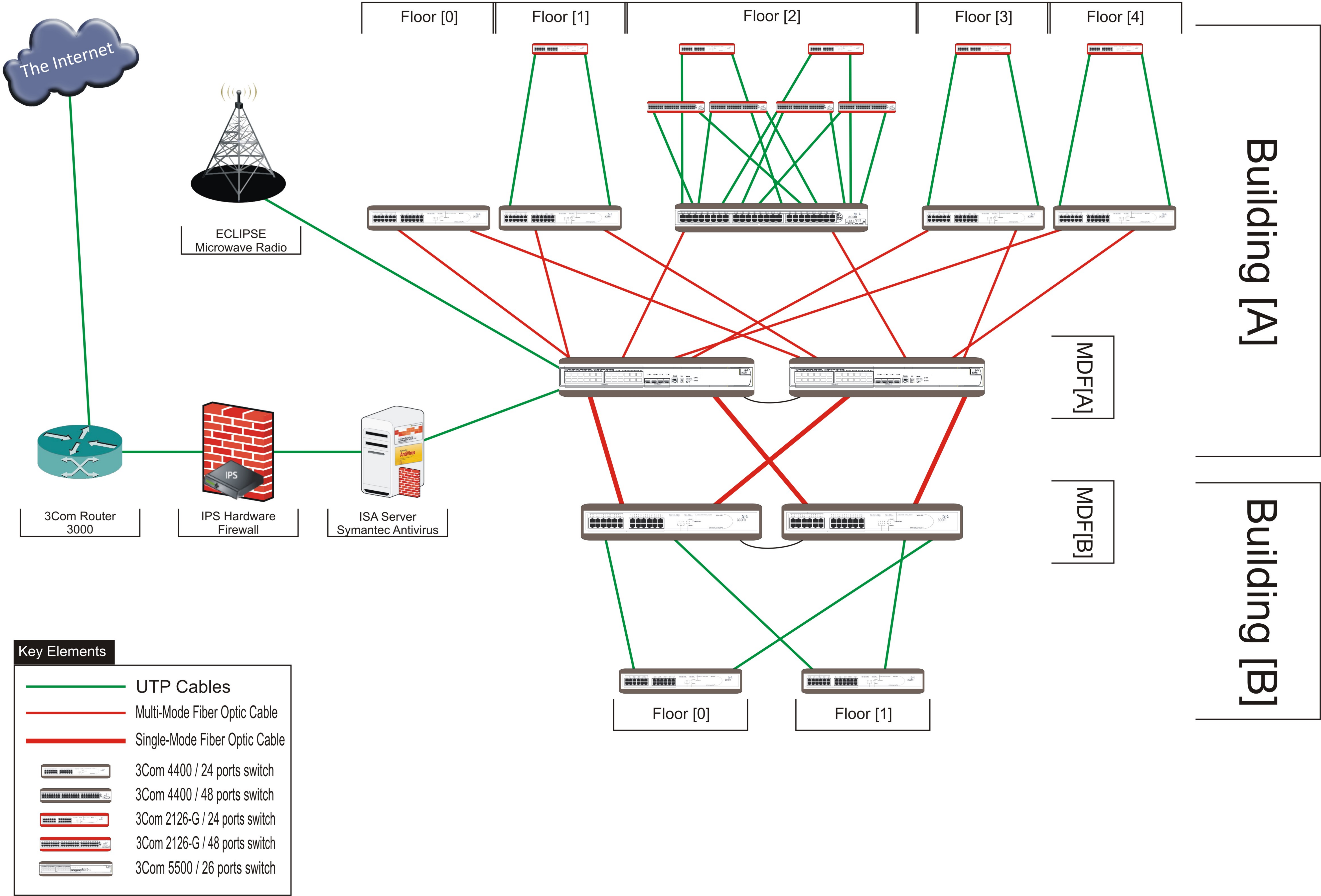
Patch Panels and Racks			
	ITI Building	**Qty**	**Price**
Wall-mounted Rack	✓	**10**	1300$
Tower Cabinet Rack	✓	**9**	1710$
UTP/STP Patch Panel 24-ports	✓	**12**	480$
UTP/STP Patch Panel 48-ports	✓	**5**	200$
Fiber Optic Patch Panel 8-ports	✓	**8**	880$
Fiber Optic Patch Panel 24-ports	✓	**1**	140$
Totals			**4710$**

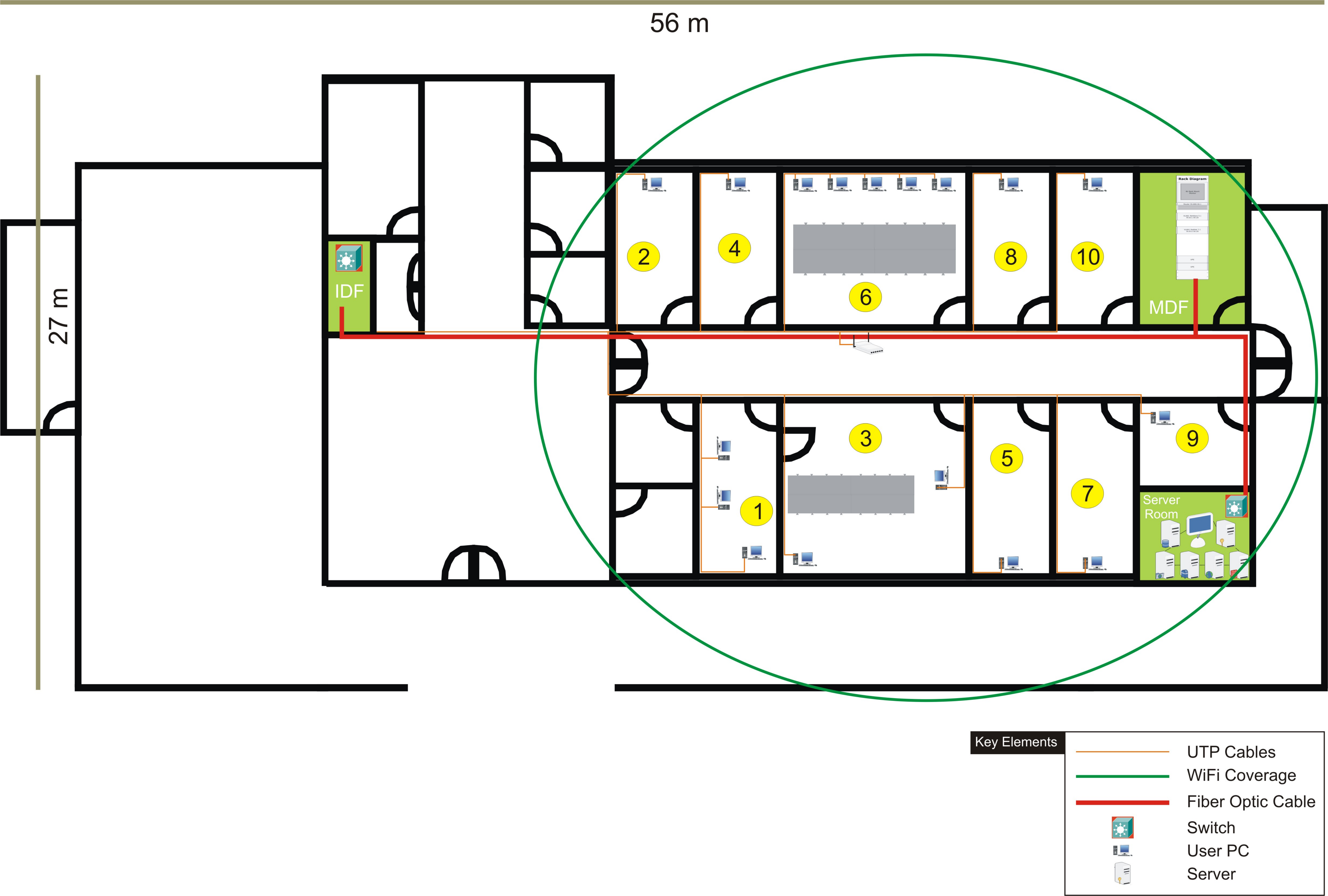
Uninterruptable Power Supply – UPS			
	ITI Building	**Qty**	**Price**
APC 650VA	✓	**17**	680$
APC 750VA	✓	**3**	180$
APC 1000VA	✓	**5**	1560$
Totals			**2420$**

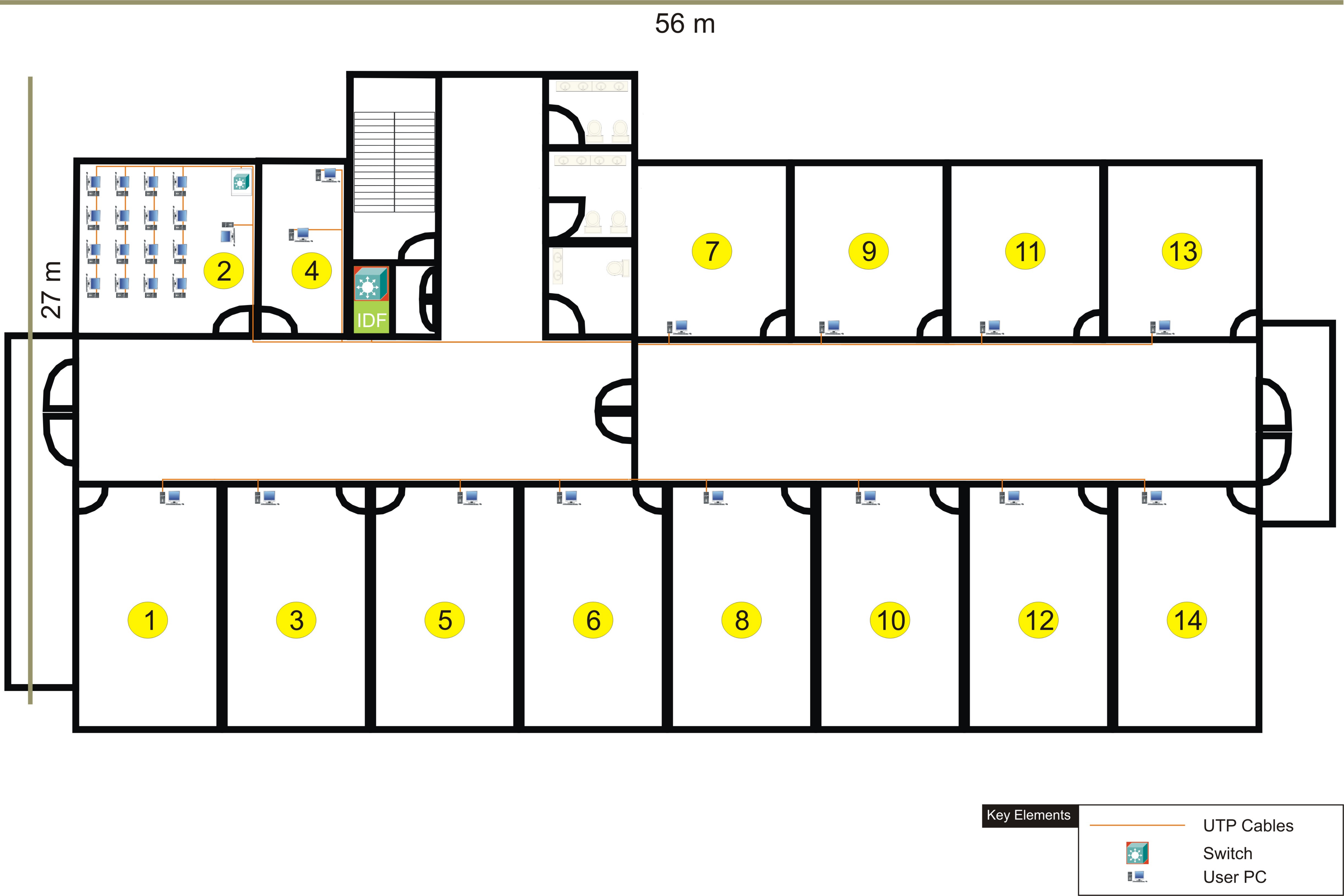
Total Project	
Microwave Link Equipment	**5231$**
Wi-Fi Equipment	**540$**
Switches	**12817$**
Cables	**10592$**
Servers Hardware	**24795$**
Servers Software	**1570$**
Hardware Firewall and Router	**3230$**
Patch Panels and Racks	**4710$**
Uninterruptable Power Supply – UPS	**2420$**
Totals	**65509$**

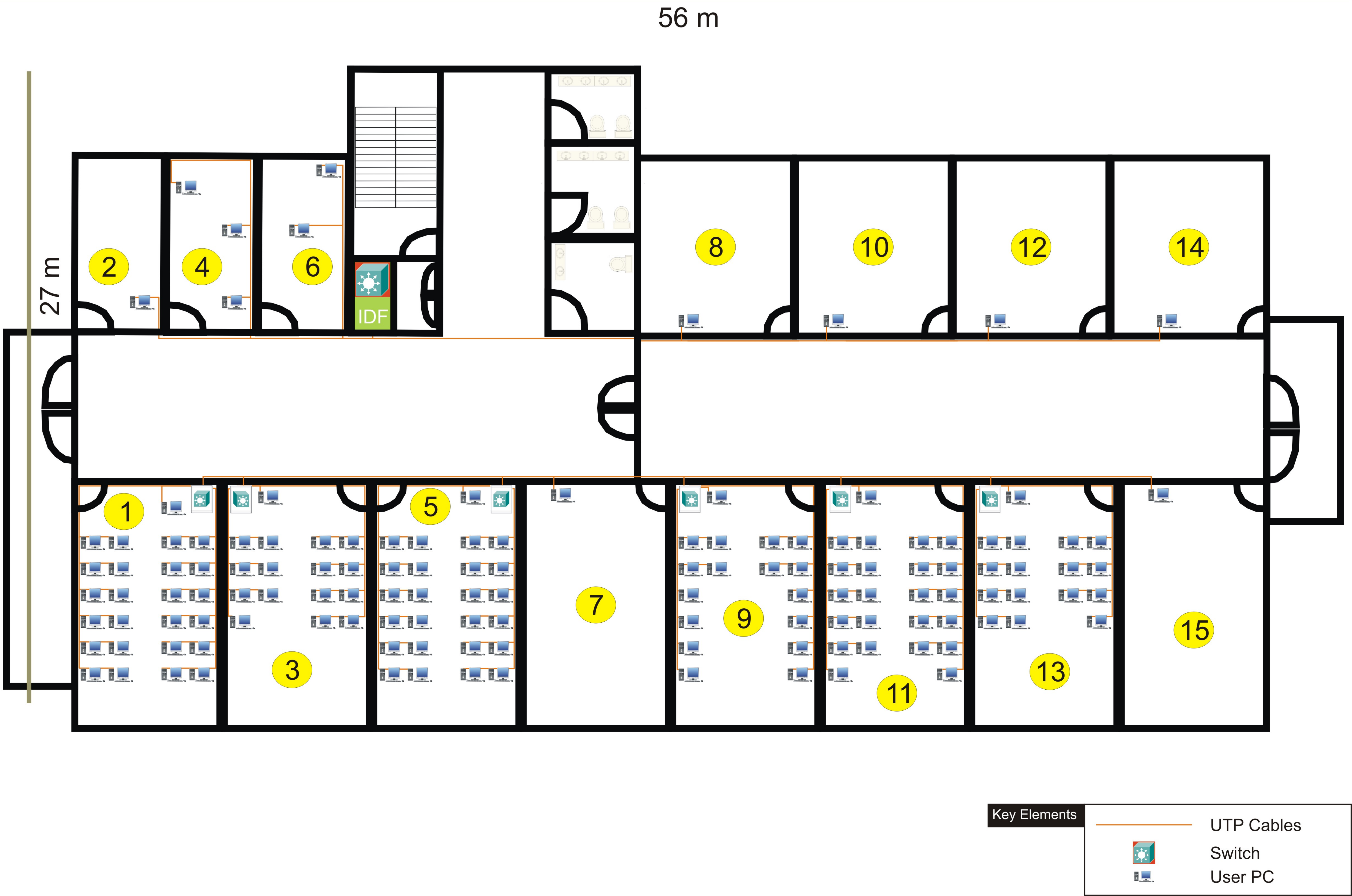
Conclusion

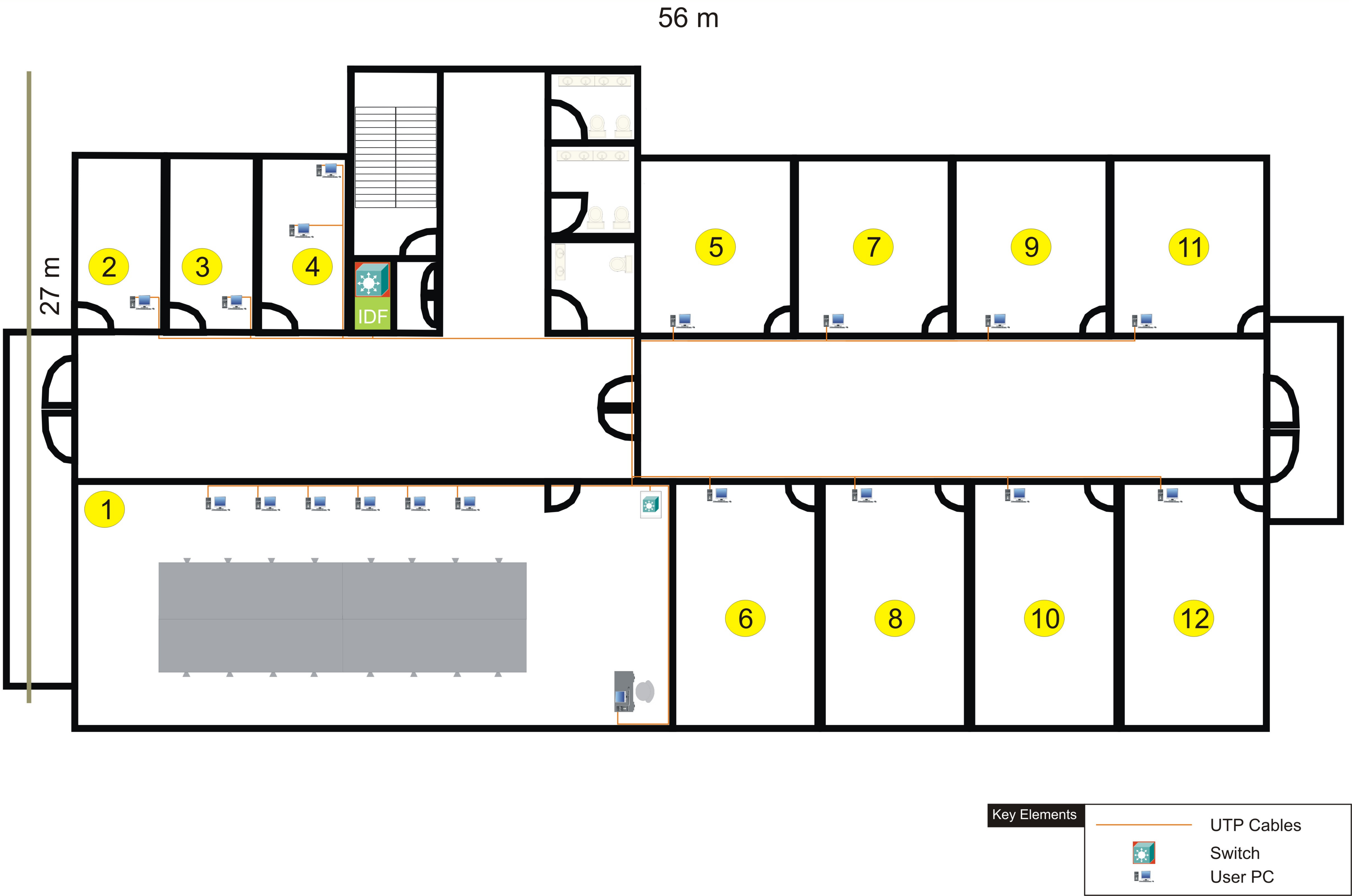
Finally, we would like to mention a few points that could have been done in the previous study and was not applicable because of cost-effective policies, but in our point of view and planning we would have replaced the Layer 2 switches with Layer 3 ones, and we would have divided the IP address into more subnets in such a way that each lab would be on a segment of it own which will enable us to excessively use VLANs to pump up the local security. We also would have wanted to bring WiFi coverage for the whole institute, on the hopes that this case study would be a reality one day because from our point of view it is up to the challenge and it deserves to be bid on.

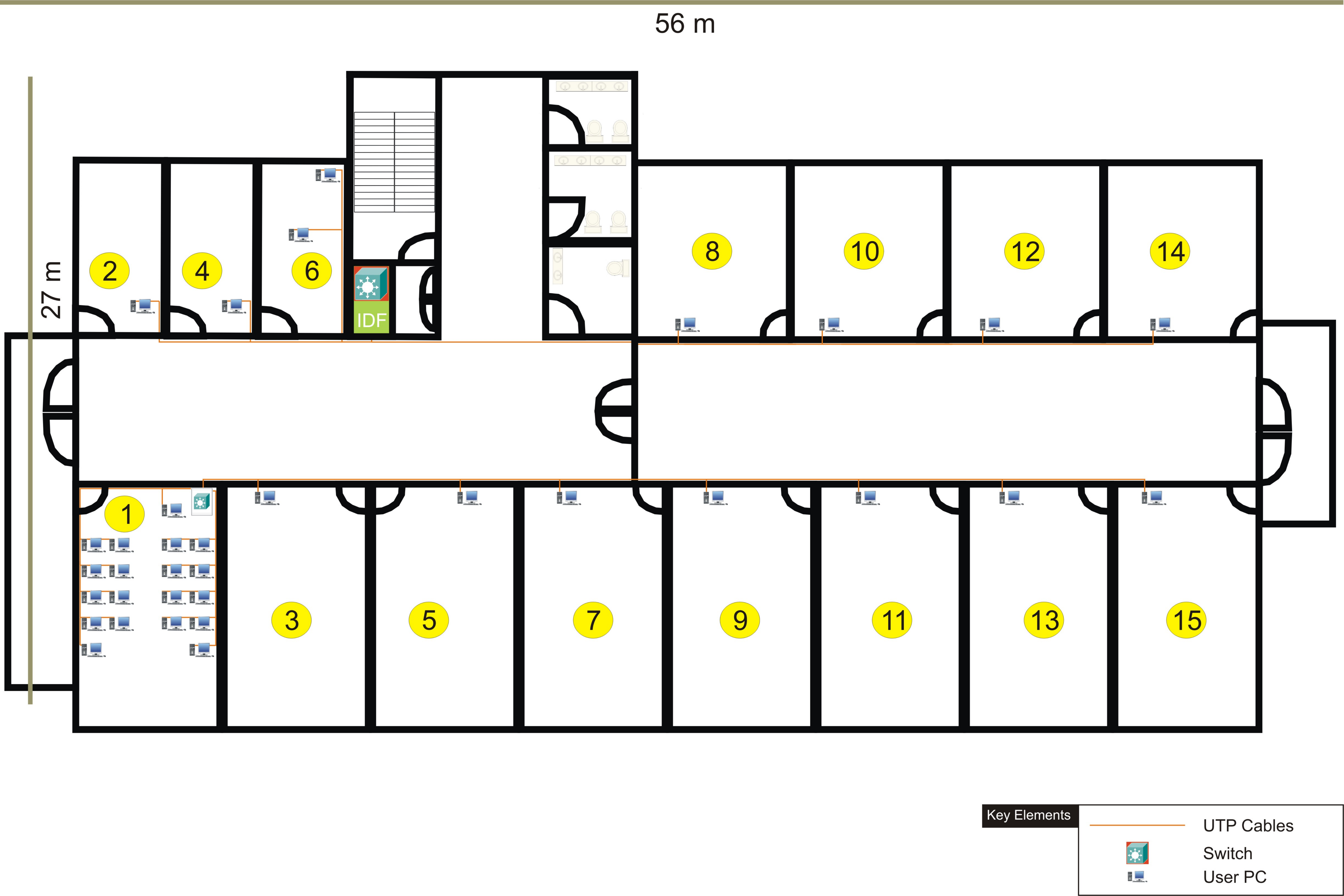

The Internet
ECLIPSE Microwave Radio
Floor [0]
Floor [1]
Floor [2]
Floor [3]
Floor [4]
Building [A]
MDF[A]
MDF[B]
Building [B]
3Com Router 3000
IPS Hardware Firewall
IPS
ISA Server Symantec Antivirus
AntiVirus
Floor [0]
Floor [1]
Key Elements
UTP Cables
Multi-Mode Fiber Optic Cable
Single-Mode Fiber Optic Cable
3Com 4400 / 24 ports switch
3Com 4400 / 48 ports switch
3Com 2126-G / 24 ports switch
3Com 2126-G / 48 ports switch
3Com 5500 / 26 ports switch

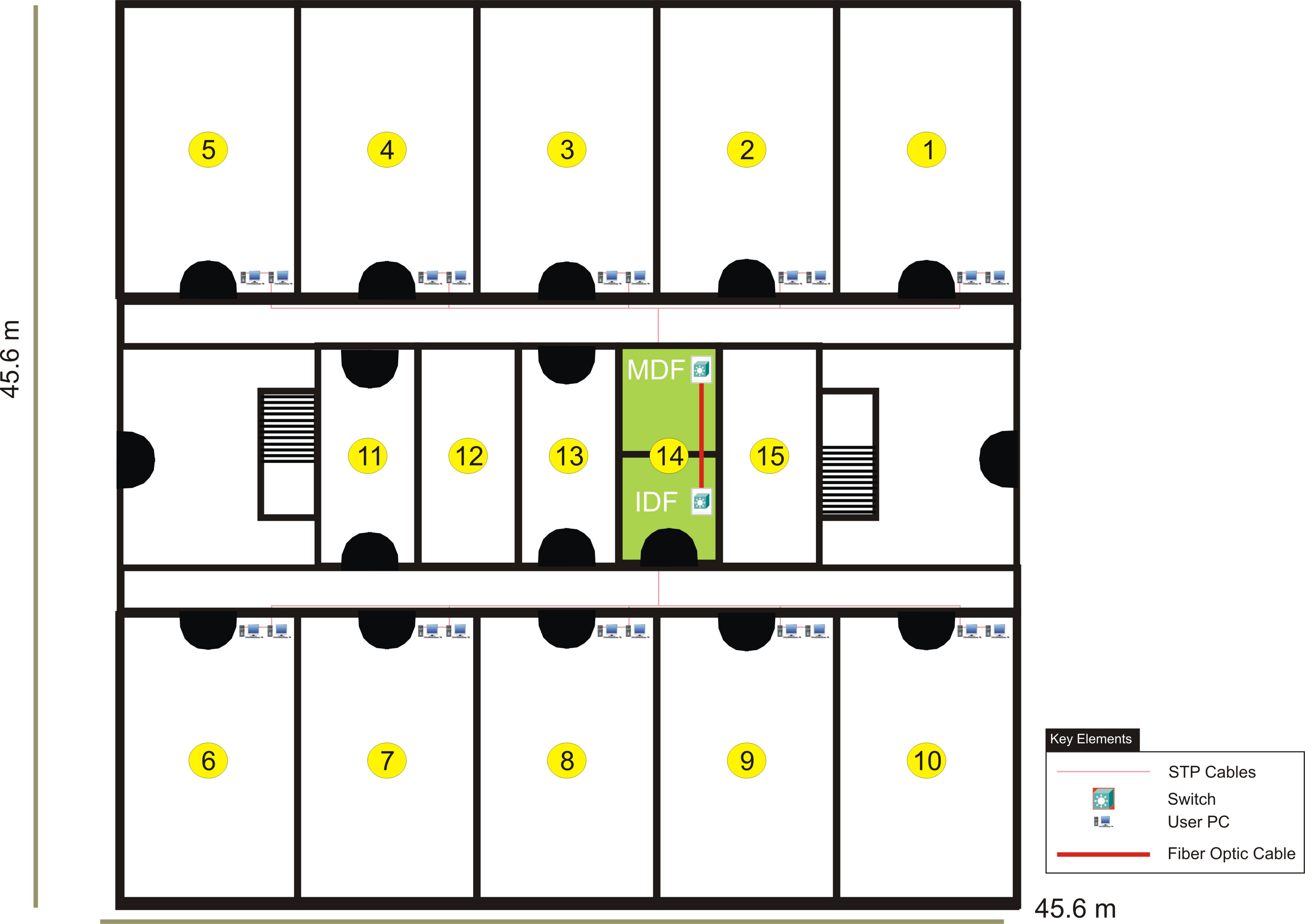

56 m
27 m
IDF
2
4
6
8
10
Rack Diagram
MDF
3
1
5
7
9
Server Room
Key Elements
UTP Cables
WiFi Coverage
Fiber Optic Cable
Switch
User PC
Server

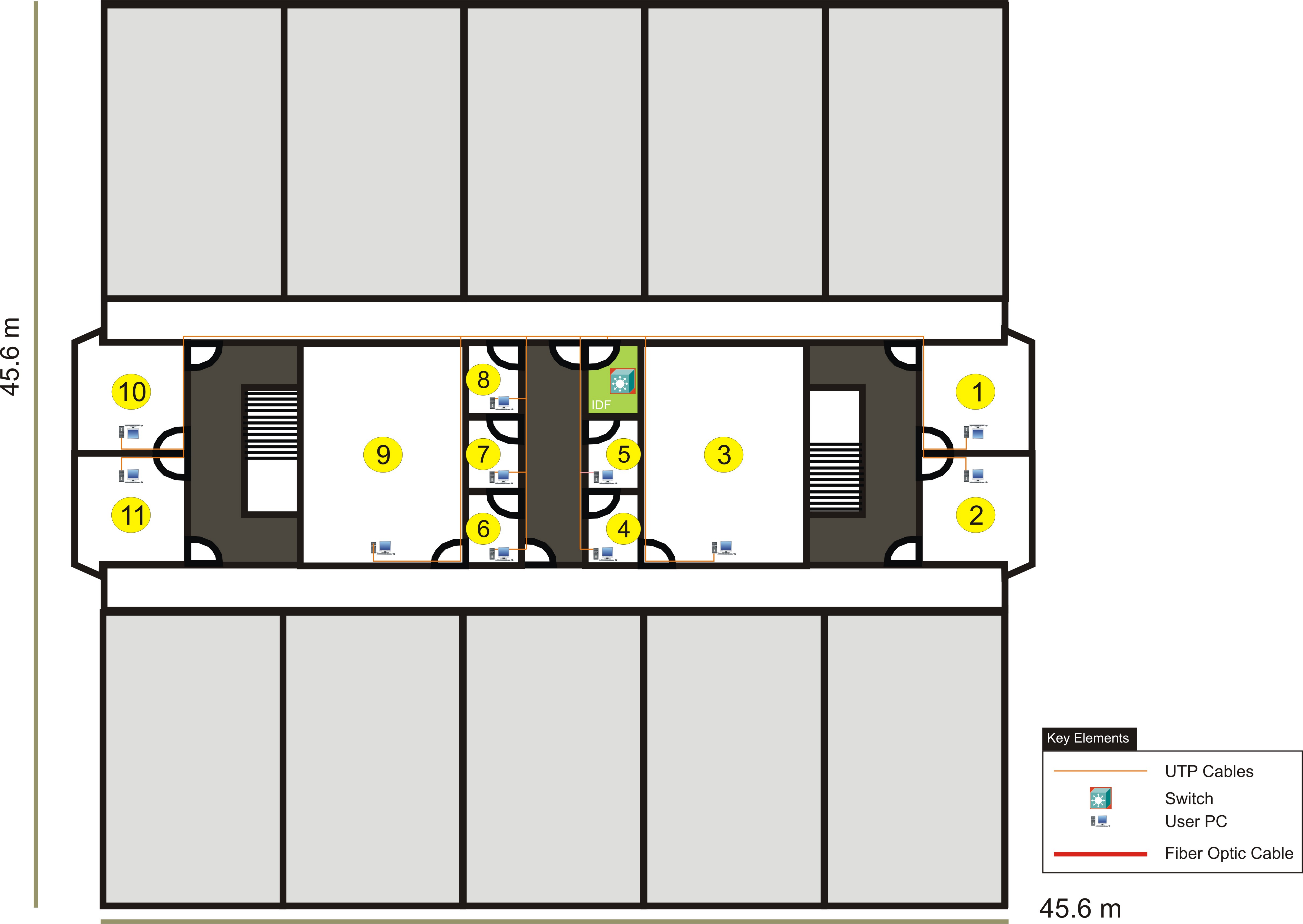

56 m
27 m
2
4
IDF
7
9
11
13
1
3
5
6
8
10
12
14
Key Elements
UTP Cables
Switch
User PC


56 m
27 m
IDF
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Key Elements
UTP Cables
Switch
User PC


56 m
27 m
2
3
4
IDF
5
7
9
11
1
6
8
10
12
Key Elements
UTP Cables
Switch
User PC


56 m
27 m
2
4
6
IDF
8
10
12
14
1
3
5
7
9
11
13
15
Key Elements
UTP Cables
Switch
User PC


45.6 m
5
4
3
2
1
MDF
IDF
11
12
13
14
15
6
7
8
9
10
Key Elements
STP Cables
Switch
User PC
Fiber Optic Cable
45.6 m


45.6 m
10
11
9
8
7
6
IDF
5
4
3
1
2
Key Elements
UTP Cables
Switch
User PC
Fiber Optic Cable
45.6 m