**Case Study: Airport Network Upgrade**

**Case Study Scenario:**

In most countries around the world, there are many places that represent the main gates for entrance and exit. Because of the importance of these places, each country takes many necessary measures to provide them with the best technology. Airports are the most sensitive places around the world because they represent these gates. Technology plays many different roles to protect and represent a high quality of services for these places. Computer networking is the most crucial part of modern airports because this new technology takes the most important responsibilities, rather than people doing the tasks as in previous decades.

**Organizational Facts:**

* The majority of the airports around the world have three main departments: the flight management controls, flight service, and arrivals, departures, guests’ department. These departments in airports are connected, and huge amounts of data are transferred between them each and every day.
* Not only is transferring data between these departments important in the project, but saving peoples’ lives is important too. Also, the quality of service in this project is critical because of the difficulty of the networks’ tasks.
* However, in each network, there are many weak points which should be dealt with to avoid many issues that might lead to huge losses in the realms of economy and humanity.
* This project provides a scheme for using two main tools that can help to avoid these common problems: design and implementation.
* The network design offered concentrates on the positions of each element in the network and how these components and capability can solve these issues.

**Current Situation:**

* The airport’s network provides services for different people, including passengers and staff, so there may be some people who cannot be trusted to connect to the inside network. However, there are many techniques to prevent people who are planning terrorist attacks from having access to the sensitive departments in the network.
* The tools that have been used to provide a high security level to the airport’s network are hardware firewalls, an IP access control list, MAC address port security, a DNS server and a proxy server. These techniques have been used to prevent these people from stealing data from the flight management department, the most safety critical department.
* Nevertheless, these techniques must provide a high security level for the network and stop the hackers infiltrating the network because the more the security techniques are increased, the more hackers’ techniques will increase in response. Moreover, the security rules have been designed to prevent any outside hackers sneaking into the network and getting what they want.
* Improving the performance of any network needs a high quality of techniques and services that help to improve the general function of the network. Airport networks need to have a high quality of services that should be presented immediately in order to keep the airport activities on track. In this section the quality of network services has been provided by new techniques to improve the quality of service.
* These techniques are represented by failover firewalls utility, a Pre-boot Execution Environment server (PXE), Dynamic Host Configuration Protocol Server (DHCP), Domain Name System Server (DNS) and cabling. The network includes everything necessary to provide a high quality of service.
* The Internet support for the flight management department needs continuous Internet service, especially the Air Traffic Control system, which manages the aircraft movement in the airport.

**Plans and Requirements**

The aim of this project is to demonstrate an example of an airport’s network design and

Implementation:

* Providing a high security level for the airport’s network
* Providing a high quality of service for the airport’s network
* Maintaining the passengers’ safety in the airport
* Maintaining passengers’ information
* Supporting the flight management system

**Solution:**

**Airport Network Cabling:**

Data cables (also known as transmission media) are responsible for carrying messages back and forth between computers and other devices and as such are the foundation of your network. All other network equipment has to be compatible with your choice of data cable, so this decision constrains or determines many of your other options. While dozens of cable variants are standardized and available for purchase, these variants fall into four main categories:

1. coaxial cable
2. twisted pair cables
3. optical fiber
4. wireless

In the airport’s network, the cable type decision has been made depending on the distance and the type of data that transfers on the wires. In many parts, the security aspect has been taken because some connectivity types cannot be relabeled to transfer the data during the work operations and the quality of transferring these data. Therefore, the airport’s network topology has been taken as the primary consideration for the cabling used in the airport.

**Airport Network Cabling Design:**

* The network cabling design part in the airport network took two aspects of applying the wiring design on the buildings. In the flight management department, the quality and aspects have been considered as the main plane of placing the cables for the airport’s network departments.
* The flight management department has been connected to the primary router with fiber optic (single mode) cable because this department manage the Airport Traffic Control Tower (ATCT) which is usually located in an area that is a long distance from the main building. In this case, the fiber optic has been chosen as a design plane to provide a high speed for transferring the data between the ATCT building, and the management building, this type of cabling can provide the service for long distance. According to McQuerry (2004):
* Single-mode fiber-optic cable allows only one mode (or wavelength) of light to propagate through the fiber. This type of cable is capable of higher band-width and greater distances than multimode and is often used for campus backbones. Single-mode cable uses lasers as the light-generating method and is more expensive than multimode cable. The maximum cable length of single-mode cable is 60+ km (37+ miles).
* As detailed above quote, fiber optic cable provides long distance connectivity with a high quality of transferring the data; this was very critical for the ACTC department because of the importance of the data that transfer between the flight management and the mentioned department. Also, the flight management department, service providers department and arrival, departure and guests’ department have been connected with the main router by fiber optic (multimode) because these departments are not too far from each other. According to McQuerry (2004):
* Multimode fiber-optic cable allows multiple modes of light to propa-gate through the fiber. Multimode cable is often used for workgroup applications, using light emitting diodes (LEDs) as light-generating devices. The maximum length of multimode cable is 2km (1.2 miles).
* As clarified early, these types of cables are appropriate to connect the airport’s departments together as long as they can provide less quality, but this will not affect the network quality in general.



Fig 1: Airport’s Network Cabling Design

**Safety**

**Web Server**

* The main issue is that when you run a Web server on your home PC, you're opening a port on your computer that allows entry from the outside world. Web servers may not be the easiest way to gain access to a computer, but they are a well-known method of intrusion, meaning that you raise your risk of having your computer attacked, your website defaced, and maybe even having your computer taken over completely by unscrupulous individuals.
* Web server can be attacked from outside; this happens when the webserver opens a port on the computer for public uses. In addition, all the information in the computer will be at risk. If there is a database server on the same machine which includes all the users’ information, this could represent a very big problem for any network around the world.
* As it happens in these days, airports are the most targeted placed for terrorist attacks. However, these attacks cannot be just suicide attacks but also could be technical attacks especially in these days.
* All the information could make the way for the terrorist for their criminal operations against the civilians (passengers). Therefore, all the information for the user’s needs to be safe and secure to ensure the safety of passenger’s lives.

**Solution:**

* The other important aspect of saving the website information was locating the web server in a secure place. The setup for the web server took advantages of the security tools which have been configured for the airport’s network.

For this reason, the web server has been placed in this department as shown in the following figure:



Fig 2: Web Server Location Design

* This design has been placed on the local network, which keeps the passengers’ information safe from inside attacks by terrorists who are doing their activity inside the airport. Otherwise, the airport’s network has taken precautions against the outside attacks by placing the firewalls and proxy server in the main internet service providers for the network.
* Nevertheless, providing a protected environment for the web server was more important them protecting the web server itself, this was provided by Internet Information Services (IIS) which is a web server for Microsoft server operating system and can provide a secure environment for the web server.

In this case study, you apply the Cisco Enterprise Architecture to the Airport Network requirements and develop a high-level view of the planned network hierarchy. Complete the following steps:

**Step 1** Consider each of the functional areas of the Cisco Enterprise Architecture:

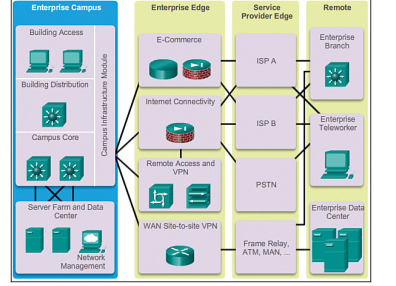


Fig 3. Functional Areas

**• Enterprise Campus:**

Network design experts have developed the hierarchical network design model to help you develop a topology in discrete layers. Each layer can be focused on specific functions, allowing you to choose the right systems and features for the layer. For example, high speed WAN routers can carry traffic across the enterprise WAN backbone, medium speed routers can connect buildings at each campus, and switches can connect user devices and servers within buildings.

A typical hierarchical topology as in Figure 1.1 consists of the following:

* A Core layer of high end routers and switches that are optimized for availability and performance.
* A Distribution layer of routers and switches that implement policies.
* An Access layer that connects users via lower end switches and wireless access points.

Each layer of the hierarchical model has a specific role. The core layer provides optimal transport between sites. The distribution layer connects network services to the access layer, and implements policies regarding security, traffic loading, and routing. In a WAN design, the access layer consists of the routers at the edge of the campus networks. In a campus network, the access layer provides switches or hubs for end user access.

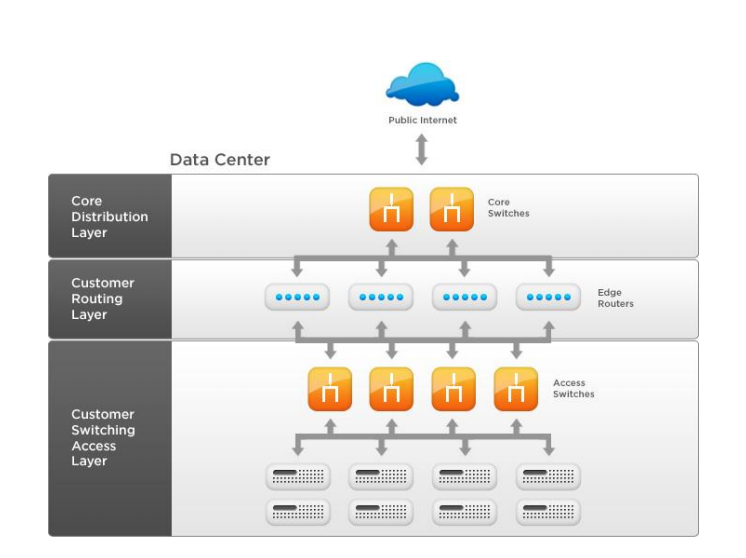


Fig 4: Hierarchial Architecture of the Network

**• Enterprise Edge:**

**DHCP Position in Overall Network**

In the airport’s network as mentioned before each department has been assigned to different IP address classes. However, this service was not provided from one server; there were two central servers which provided the entire network with dynamic IP addresses. The DHCP servers’ design was applied regarding the security policy for each department. The flight management department and the service provider’s departments were provided by two servers which are located in the department as shown in figure

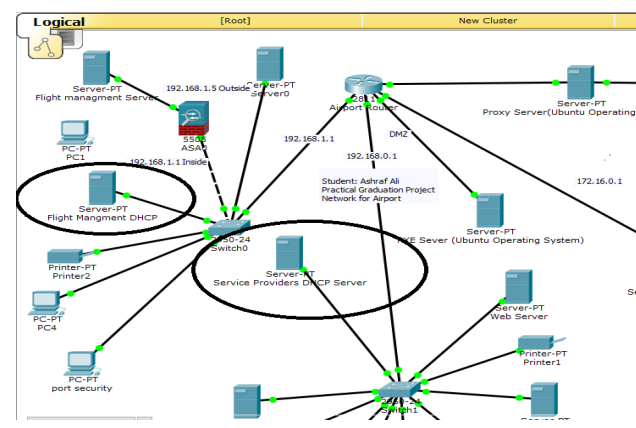
****

Fig 5: DHCP position in overall network

**DHCP & LAN:**

From another aspect, the design of the DHCP server is required to place the arrival, departure, and guests’ department server separately and connected directly with this department without any other connections from the neighboring departments. This was also one of the main requirements of the security policy that was assigned to the airport’s network. In this case, this department has a private server which was supported by different devices with dynamic IP addresses as shown in figure

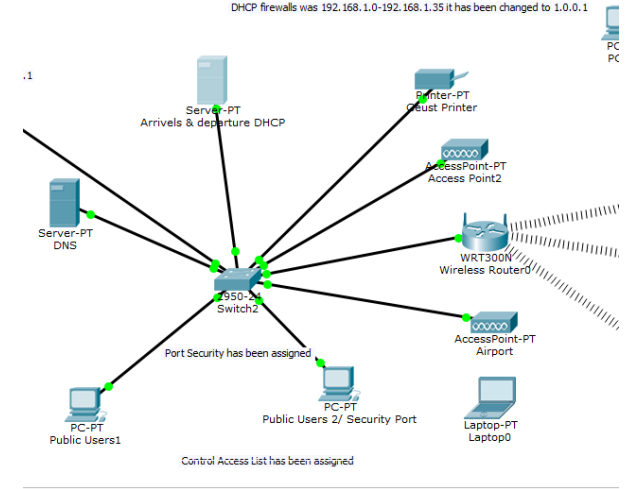


Fig 6: DHCP and LAN connectivity

**Domain Name System (DNS) Server**

The numeric IP address is the mechanism that is used to help establish the communication between devices in the local network and Internet. Also, it is possible to reach the internet websites from the local network by using the IP address and passing them to the outside servers. However, this use of numbers is impractical for users. Therefore, there is a system that can translate a textual name to the numbers, the Domain Name system (DNS). By using it as lookup tool, it is possible to know what the DHS server’s IP address on the network is. For example, the DNS server’s address for Valparaiso University is (152.228.34.1) as shown in figure

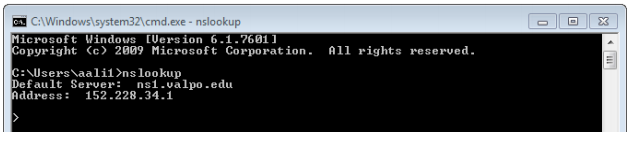
****

Fig 7: DNS Server Example

**DNS Server Network Location**

The DNS server can be located in any positions which should have a high security level. In the airport’s network, the DNS server has been placed in the service provider’s department because the web server has been put in the same department as shown in figure

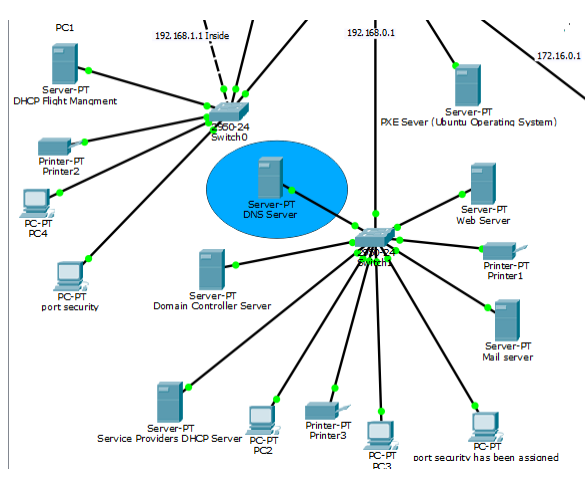


Fig 8: DNS server position in overall network

**• Enterprise Branch**

The other important aspect of saving the website information was locating the web server in a secure place. The setup for the web server took advantages of the security tools which have been configured for the airport’s network. The main beneficial tool for security was the accessed list utility; this tool prevented the unauthorized users from accessing other departments, such as 96 the arrivals, departures, and guests’ department from accessing the service provider’s department. For this reason, the web server has been placed in this department as shown in figure

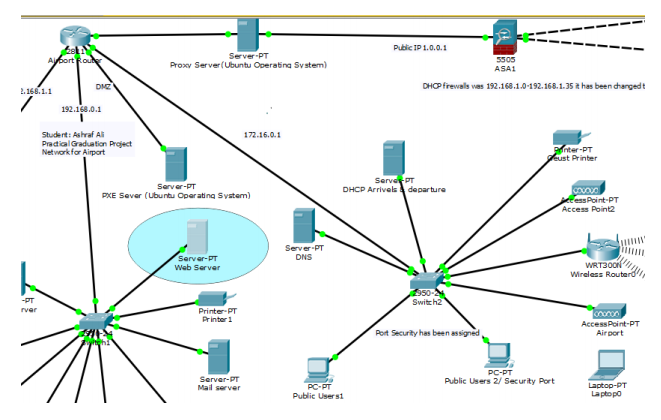


Fig 9: Enterprise Branch

**• Enterprise Data Center**

The **enterprise data center module** is a data center with all of the same functional options as a campus data center, but exists at a remote location. This provides an added layer of security as the offsite data center can provide disaster recovery and business continuance services for the enterprise. High-end switches such as the Cisco Nexus series switch use fast WAN services such as Metro Ethernet (MetroE) to connect the enterprise campus to the remote enterprise data center. Redundant data centers provide backup using synchronous and asynchronous data and application replication. Additionally, the network and devices offer server and application load balancing to maximize performance. This solution allows the enterprise to scale without major changes to the infrastructure.

• **Enterprise Teleworker**

This airport’s network domain as planed to provide two services: security and storage. The services took advantages of the distinctive computer network design in the two departments of the airport’s local network, as shown in figure

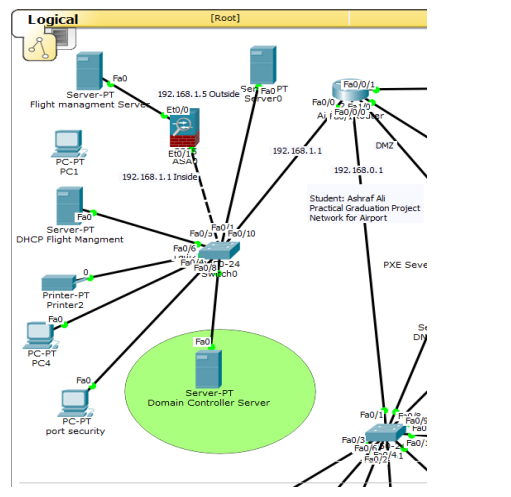


Fig 10: Network Design

The storage service contains a physical device which has been placed in the flight management department and connected directly to the domain controller server. This can help each user in the network to have his own partion when he logged in to the domain. Also, these services are contacted under specific security rules. The service provider’s department employees can access the domain service. However, the domain active directory placed security policy for each user depending on her/his position in the airport’s network. For example, the services provider’s department employees can read only from the data storage server which is placed in the flight management department. Also, the service flight management department’s employees have all permissions in the data storage server like read, write and execute. Otherwise, some of the information technology department’s employees have all permissions for all computers in the airport’s local network. They can remove, install, configure, maintain and set up programs on the all connected computers. Moreover, each employee must have his unique username and password to join to the domain for accessing the machine which will has an available storage portions spaces. On the other hand, the arrivals, departures, and guests’ department cannot access to the domain controller server and the domain storage service. The domain controller server are hosted in secure placed which provide high security level for the network as a general. The reason for that is, the arrivals, departures, and guests’ department has been designed and configured to provide internet service and some computers for public use only. As mentioned before arrivals, departures, guest’s department cannot access to the other two departments because of the airport’s network security policy, so the service in this department configured for limited purposes.

**Step 2** List some key considerations or functions for each of the modules in the Cisco Enterprise Architecture. Indicate whether each module is used in the Airport Network Upgrade.

**Solution:**

■ Enterprise Campus Building Access layer:

* Whether you have an Ethernet connection to each end station or a remote access server, if the device allows users to connect to the network, it's considered an Access layer device.
* Typically, these devices are hubs, multistation access units (MAUs), or switches deployed in wiring closets on each floor of a building.
* Users' network cables are then terminated into such an Access layer device, where they are connected to each user on the local network.
* Typically, virtual LANs (VLANs) are implemented to separate broadcast domains on the Access layer.

■ Enterprise Campus Building Distribution layer:

* From the OSI model Physical layer perspective, the main function of the Distribution level is to provide the Access layer with connectivity to the Core layer.
* The Distribution layer connects each Access layer device so that the Access devices can route between themselves and to the Core layer.
* If VLANs are used to separate traffic in the Access layer, the Distribution layer can route between the VLANs.

■ Campus Core layer of the Enterprise Campus:

* Campus networks that contain two or more switch blocks require a Core layer to connect each switch block to other switch blocks.
* The most important consideration at the Core layer is speed, because devices at the Core layer must perform switching between the switch blocks at very high speeds.
* Since speed is important, the Core layer is not where network policies, firewalls, or any type of filtering should be performed.

■ Enterprise Campus Server Farm module:

* A server farm is a set of many servers interconnected together and housed within the same physical facility.
* A server farm provides the combined computing power of many servers by simultaneously executing one or more applications or services.
* A server farm is generally a part of an enterprise data center or a component of supercomputer.

■ Enterprise Edge modules:

* The **enterprise edge module** provides connectivity for voice, video, and data services outside the enterprise. This module often functions as a liaison between the enterprise campus module and the other modules.
* This module supports traditional, circuit-switched, and more advanced media. All Cisco devices that support these WAN technologies, in addition to routing, access control, and QoS mechanisms, can be used in this module.
* Although security is not as critical when all links are enterprise-owned, it should be considered in the network design

■ Service Provider modules:

* The SP edge module spans across large geographic areas in a cost effective manner
* It converges voice, video, and data services over a single IP communications network
* It supports QoS and service level agreements
* It supports security using VPNs (IPsec / MPLS) over Layer 2 and Layer 3 WANs

■ Enterprise Data Center:

* The **enterprise data center module** is a data center with all of the same functional options as a campus data center, but exists at a remote location.
* This provides an added layer of security as the offsite data center can provide disaster recovery and business continuance services for the enterprise.
* High-end switches such as the Cisco Nexus series switch use fast WAN services such as Metro Ethernet (MetroE) to connect the enterprise campus to the remote enterprise data center. Redundant data centers provide backup using synchronous and asynchronous data and application replication.
* Additionally, the network and devices offer server and application load balancing to maximize performance. This solution allows the enterprise to scale without major changes to the infrastructure.

■ Enterprise Teleworker:

* The **enterprise teleworker module** is responsible for providing connectivity for workers who operate out of different geographically dispersed locations, including home offices, hotels, or customer/client sites.
* The teleworker module recommends that mobile users connect to the Internet using the services of a local ISP, such as cable modem or DSL. VPN services can then be used to secure communications between the mobile worker and central campus.
* Integrated security- and identity-based networking services enable the enterprise to extend campus security policies to the teleworker.
* Staff can securely log in to the network over the VPN and gain access to authorized applications and services from a single cost-effective platform.

■ Enterprise Branch:

* T he **enterprise branch module** includes remote branches that allow employees to work at noncampus locations.
* These locations are typically responsible for providing security, telephony, and mobility options to employees, as well as general connectivity into the campus network and the different components located inside the enterprise campus. The enterprise branch module allows enterprises to extend head-office applications and services, such as security, Cisco Unified Communications, and advanced application performance, to the remote branches.
* The edge device connecting the remote site to the central site varies depending on the needs and size of the site. Large remote sites may use high-end Cisco Catalyst switches, while smaller sites may use an ISR G2 router. These remote sites rely on the SP edge to provide services and applications from the main site.

**Step 3** Since the time initial discussions with the organization occurred, the following additional requirements have surfaced:

• Providing a high security level for the airport’s network

• Providing a high quality of service for the airport’s network

• Maintaining the passengers’ safety in the airport

• Maintaining passengers’ information

• Supporting the flight management systemHow does this new information change the design? Incorporate the changes into your high-level design, and update the list of modules and considerations.

**Solution:** An Internet Connectivity module, an E-commerce module, a Remote Access and VPN module, and a possibly an Enterprise Teleworker module will be added to the network design.

The following figure shows the addition of these modules.

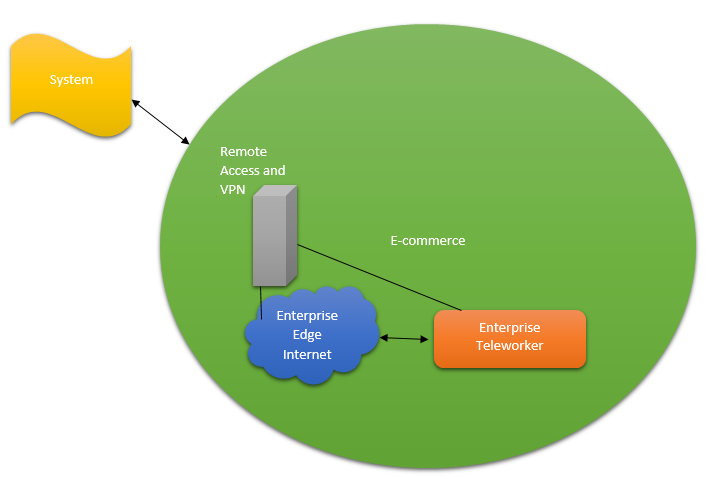


Fig 11:

The following are some considerations for each of these modules.

■ Enterprise Edge E-commerce module:

— This module provides scalability, security, and high availability within the overall e-commerce network design. Devices in this module include various servers (Web, application, database), firewalls or firewall routers, NIDS appliances, and multilayer switches with IDS modules.

■ Enterprise Edge Internet Connectivity module:

— This module provides internal users with Internet connectivity and access to information published on the enterprise’s public servers, such as HTTP and FTP servers.

— This module accepts VPN traffic from remote users and forwards it to the Remote Access and VPN module, where VPN termination takes place.

— Devices in this module include SMTP mail servers, DNS servers, public servers (FTP and HTTP), firewalls or firewall routers, and edge routers.

■ Enterprise Edge Remote Access and VPN module:

— This module terminates VPN and dial-in and uses the Internet Connectivity module

to initiate VPN connections to remote sites.

— Devices in this module include dial-in access concentrators, ASAs, firewalls, and NIDS appliances.

■ Enterprise Teleworker:

— This module provides people in geographically dispersed locations, such as home offices or hotels, with highly secure access to central-site applications and network services.

**Step 4**

Which of the following infrastructure or network services are immediately

applicable to your design?

• Security services

• Voice services

• Wireless

• Network management

• High availability

• QoS

• Multicast

Are there specific locations or modules where some of these services are

particularly relevant?

Solution:

**Infrastructure and Network Services applicable in an Airport Network**

* Security Services :-

Security services supporting support the Internet Connectivity for the functionality of various systems in an airport network and the security of the same, E-commerce for flight bookings and various other needs and Remote Access and VPN modules.

* Firewalls and intrusion detection systems.

Any outside to inside activity in the network should be inspected. Compare the firewalls’ configuration with each other to ensure the similarity in the Policy rules. Inspect for the activation of each firewall in the same network.

Check the impact of a port compromise to interface for the firewall. Assuring the policy configuration setups for the firewalls to meet the organization requirements. Making sure of disabling the unused open ports especially the closes one from the used ports. Depending on the organization’s equipment the used ports should be mentioned as a part of the policy rules. The firewall policy rules, which should be trusted on every update.

Position of the System:-

The ASA1 firewall position design takes a very important location because it works as police check point on the bridge. With this strategy, no data can be exchanged without it passing through the firewalls. For the most network designs, network engineers take prominent role for the design of the network before anything. This step represents the first step in establishing an integrated any deploy system as well as the all practical work that benefits the design, especially the overall technology.

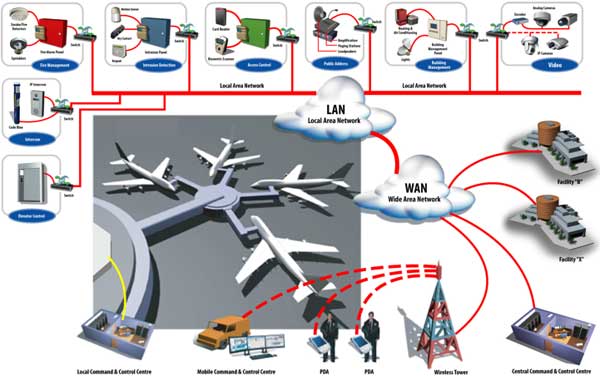


Fig 12: Infrastructure and Network Services

* Voice Services & Wireless Services :-

More and more, employers are providing tools such as wireless-enabled laptops, personal digital assistants (PDAs), and VPN access to corporate networks to help employees work more efficiently at home and on the road. Corporate travellers now take more than 280 million business trips each year, and Cahners In-Stat estimates that 80 percent of all business travellers use VPN technology.

Business travelers equipped with these tools want to use the time they spend in airports as productively as possible. An airport that provides high-speed Internet access through a wireless LAN (WLAN) can transform boarding gates, lounges, and food courts into practical, value-added working environments for business travelers. In hub airports where passengers may spend several hours waiting for a connecting flight, this offering is particularly attractive. As more mobile professionals and their employers consider public access Internet capability when choosing airlines and transit routes, the investment in wireless Internet access can translate into higher customer volumes.

* Network Management :- Software for centralized management of the entire airport network for bandwidth allocation, switching and routing , traffic control and firewall policy architecture is mandatory for day to day operations to be conducted in a network.
* High Availability is needed for critical time depended air operations including Air Traffic Management, Communications, Gate Allocations, Taxi Ways, etc all depend only if high network availability is there.
* QoS: Quality of service (QoS) refers to any technology that manages data traffic to reduce packet loss, latency and jitter on the network. QoS controls and manages network resources by setting priorities for specific types of data on the network. A second offbeat that is need is reliability; accordingly, this design incorporates looks for failover. Failover utility is very powerful and was used to provide constant communication service during the network operations. This utility was located in the Cisco firewalls and routers network’s devices. Usually, this configuration is used when the network has two outside connections to one device. Each link connection has a special task, the main link connection (ISP1) named primary as a default and the second named as a secondary link connection
* Muticast: The industry leader in IP Multicast for more than ten years, develops value-added features that enable Enterprise customers to deploy IP Multicast within the network core. Cisco provides a depth of functionality that allows Enterprise customers to select a solution customized for their particular needs. Multicast Source Discovery Protocol (MSDP), for example, is a traditional Service Provider protocol that has been updated for use within highly available Enterprise networks that use a MDP / Anycast design.

**Step 5:** Indicate where redundancy should be supported in the design.

**Solution:**

**Redundancy in Airport Network**

* A network-level redundancy involves the use of both redundant links as well as network equipment, such as routers and switches. The concept is similar to a physical-level redundancy should your main communication path go down, your servers can use your backup links to maintain availability and keep your business online.

In layman’s terms, consider your network redundancy like directions you’d get from your car’s GPS. If you are driving down the highway and there is an accident, your navigation system will divert you to a route that’s less crowded. It may not be the shortest route in distance, but it ends up being the quickest to your destination. Of course, your network-level redundancy won’t have unlimited paths from which to choose like your car GPS. It will only work with paths that you’ve already established as your backups.

* The AirPort Extreme (802.11n) and Time Capsule work with most disks that are not software RAID volumes (no more than one volume per physical disk). If the disk is a self-contained RAID that presents itself to a computer as a single volume requiring no software support, then it may be supported.

Perhaps something like the Netgear [ReadyNAS Duo](http://www.readynas.com/?cat=3), if someone wants to get a ready-made solution. One can also buy NAS enclosures with two or more bays, a couple of bare drives, and roll their own. Note that one would typically connect NAS to the Airport via Ethernet (though some NAS enclosures allows to connect via USB, which was the original plan), but since the limiting speed is the Airport wireless speed, that wouldn’t be a problem.

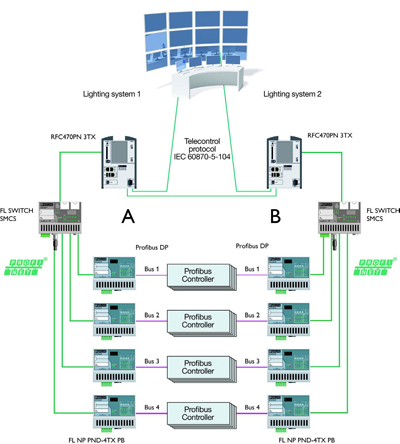


Fig 13: Redundancy in the network

**Case Study Additional Information**

The project is to design a proposal for setting up a network in an airport. The airport has three departments.

1.Airport authority

2. Flight service providers

3. Guests.

The airport authority maintains a server which handles the flight management controls. The flight service providers should have access only to the specific server in the airport authority network and not to any other systems. The guest users should have wireless access to a high speed internet connection, which should be shared among all the users in all the departments.

The wireless access should be using a common password. The guest users should not have access to the other two departments. The users should obtain IP addresses automatically. The airport authority has 20 users, the flight service providers have 40 users and the maximum numbers of guests are estimated to be 100.

**Networking Requirement.**

1.The active networking components (Routers, switches, wireless access points etc) with quantity.

2. The IP network design for each department.

3. Creating and mapping IP networks with vlans.

4. Analysis, identification and explanation of methodologies to use for access restriction and internet sharing.

5. Dynamic IP addressing design for all the networks.

6. Identify the configuration and features, wherever appropriate, which is required on the active components to setup the network.

7. Network topology diagram.

**Selecting Network Devices:**

After the customer requirements have been analysed, the design staff recommends the appropriate network devices to connect and support the new network functionality. Modern networks use a variety of devices for connectivity. Each device has certain capabilities to control the flow of data across a network. A general rule is that the higher the device is in the OSI model, the more intelligent it is. This means that a higher-level device can better analyze the data traffic and forward it based on information not available at lower layers. For example, a Layer 1 hub can only forward data out all ports, a Layer 2 switch can filter the data and only send it out the port connected to the destination based on MAC address, and a Layer 3 router can decide which traffic to forward or block based on the logical address. As switches and routers evolve, the distinction between them becomes blurred. One simple distinction remains: LAN switches provide connectivity within an organization’s LAN, whereas routers are needed to interconnect local networks or to form a wide-area network (WAN) environment. In addition to switches and routers, other connectivity options are available for LANs. Wireless access points allow computers and other devices, such as handheld Internet Protocol (IP) phones, to wirelessly connect to the network or share broadband connectivity. Firewalls guard against network threats and provide application security, network control and containment, and secure connectivity technologies. ISRs combine the functionality of switches, routers, access points, and firewalls in the same networking device.

**Selecting LAN Devices:**

Although both a hub and a switch can provide connectivity at the access layer of a network, switches should be chosen for connecting devices to a LAN. Switches generally are more expensive than hubs, but the enhanced performance makes them cost-effective. A hub generally is chosen as a networking device within a very small LAN, within a LAN that requires low throughput requirements, or when finances are limited. A hub may also be installed in a network when all network traffic is to be monitored. Hubs forward all traffic out all ports, whereas switches microsegment the network. Connecting a network monitoring device to a hub allows the monitoring device to see all network traffic on that segment. Some switches do provide the ability to monitor all network traffic through a special port, but this is not a universal feature.

**Selecting Internetworking Devices :**

After the LAN switches have been selected, it is time to determine which router is appropriate for the customer. A router is a Layer 3 device. It performs all tasks of devices in lower layers and selects the best route to the destination network based on Layer 3 information. Routers are the primary devices used to interconnect networks. Each port on a router connects to a different network and routes packets between the networks. Routers can break up broadcast domains and collision domains. 64 Working at a Small-to-Medium Business or ISP, CCNA Discovery. Learning Guide Packet Tracer Activity 04\_2109\_ch03.qxd 4/8/08 3:31 PM You must consider a number of factors when selecting a router.

**Core Layer Design Configurations:**

The Cisco three-layer hierarchal model is composed of the core layer, distribution layer, and access layer. Of the three layers, the core layer is responsible for transporting large amounts of data quickly and reliably. The designer must ensure that the core layer is designed with fault tolerance, especially because all users in the network can be affected by a failure. The ability to avoid unnecessary delays in network traffic quickly becomes a top priority for the network designer.

The core layer is sometimes called the network backbone. Routers and switches at the core layer provide high-speed connectivity. In an enterprise LAN, the core layer, may connect multiple buildings or multiple sites, and may provide connectivity to the server farm. The core layer includes one or more links to the devices at the enterprise edge to support Internet, virtual private networks (VPN), extranet, and WAN access.

Core Layer Technologies:

Technologies used at the core layer include the following:

* Routers or multilayer switches that combine routing and switching in the same device
* Redundancy and load balancing
* High-speed and aggregate links
* Routing protocols that scale well and converge quickly, such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) Protocol

Implementing redundant links at the core layer ensures that network devices can find alternate paths to send data in the event of a failure. When Layer 3 devices are placed at the core layer, these redundant links can be used for load balancing in addition to providing backup. In a flat, Layer 2 network design, Spanning Tree Protocol (STP) disables redundant links unless a primary link fails. This STP behaviour prevents load balancing over the redundant links.

Most core layers in a network are wired in either a full-mesh or partial-mesh topology. A full-mesh topology is one in which every device has a connection to every other device.

Although full-mesh topologies provide the benefit of a fully redundant network, they can be difficult to wire and manage and are more costly. For larger installations, a modified partial-mesh topology is used. In a partial-mesh topology, each device is connected to at least two others, creating sufficient redundancy without the complexity of a full mesh.

**Distribution Layer Design Configurations:**

The next layer of the Cisco hierarchical model is the distribution layer. This layer is associated with routing, filtering, and is the communication point between the core layer and the access layer. A network designer must create a distribution layer design that complements the needs of the other two layers.

The distribution layer represents a routing boundary between the access layer and the core layer. It also serves as a connection point between remote sites and the core layer.

Distribution Layer Routing:

The access layer is commonly built using Layer 2 switching technology. The distribution layer (see Figure 1-10) is built using Layer 3 devices. Routers or multilayer switches, located at the distribution layer, provide many functions critical for meeting the goals of the network design, including the following:

* Filtering and managing traffic flows
* Enforcing access control policies
* Summarizing routes before advertising the routes to the Core
* Isolating the core from access layer failures or disruptions
* Routing between access layer VLANs

Distribution layer devices are also used to manage queues and prioritize traffic before transmission through the campus core.

Trunks:

Trunk links are often configured between access and distribution layer networking devices. Trunks are used to carry traffic that belongs to multiple VLANs between devices over the same link. The network designer considers the overall VLAN strategy and network traffic patterns when designing the trunk links.

Redundant Links:

When redundant links exist between devices in the distribution layer, the devices can be configured to load balance the traffic across the links. Figure 1-11 shows the redundant links at the distribution layer. Load balancing is another option that increases the bandwidth available for applications.

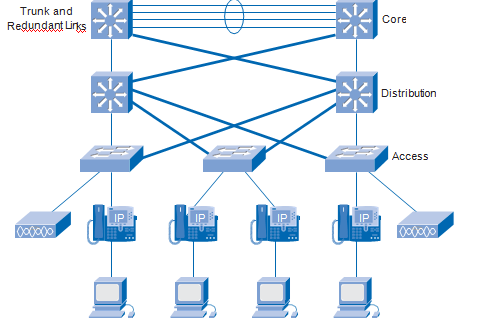


Fig 14: Distribution Layer Design

**Access Layer Design Configurations:**

The modern computer network consists of more than just personal computers and printers connecting to the access layer. Many different devices, can connect to an IP network, including the following:

1. IP telephones
2. Video cameras
3. Videoconferencing systems

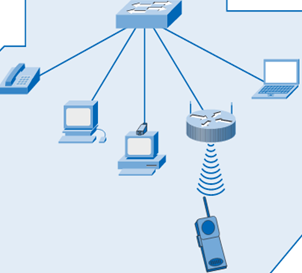


Fig 15: Access Layer Connections

All of these services can be converged onto a single physical access layer infrastructure. However, the logical network design to support them becomes more complex because of considerations such as quality of service (QoS), traffic segregation, and filtering. These new types of end devices, and the associated applications and services, change the requirements for scalability, availability, security, and manageability at the access layer.

In addition to providing basic connectivity at the access layer, the designer needs to consider the following:

* Naming structures
* VLAN architecture
* Traffic patterns
* Prioritization strategies

Following good design principles improves the manageability and ongoing support of the network by

* Ensuring that the network does not become too complex
* Allowing easy troubleshooting when a problem occurs
* Making it easier to add new features and services in the future

Most recent Ethernet networks use a star topology, which is sometimes called a hub-and-spoke topology. In a star topology, each end device has a direct connection to a single networking device. This single networking device is usually a Layer 2 or multilayer switch. A wired star topology in the access layer typically has no redundancy from individual end devices to the switch. For many businesses, the cost of additional wiring to create redundancy is usually too high. However, if costs are not a factor, the network can be configured as a full-mesh topology to ensure redundancy.

Using VLANs and IP subnets is the most common method for segregating user groups and traffic within the access layer network:

Today, VLANs are used to separate and classify traffic streams and to control broadcast traffic within a single wiring closet or building. Figure 1-20 shows VLANs segregating traffic within a network. Although large VLANs that span entire networks are no longer recommended, they may be required to support special applications, such as wireless roaming and wireless IP phones.

**Hardware and Software inventory list**

|  |  |  |
| --- | --- | --- |
| **Item** | **Model** | **Quantity** |
| **Router** | Cisco 2600 Series 2621 ROUTER with high speed interface for internet connection | 1 |
| **Switches** | Cisco 2950 Catalyst Switch | 3 |
| **Access Points** | Cisco Aironet 1200 Access Point | 3 |
| **Server** | IBM/DELL | 1 |
| **Operating System** | Windows 2008 | 1 license |
| **PC** | IBM/DELL | As per requirement |

**Designing Server Farm for Airport System**

The Airport Server is the machine that protects the airport database. Whereas most firewalls protect internal clients, this machine protects an internal server and therefore needs to be more secure than a firewall and have very strong assurances that it cannot be compromised.

The Airport Server uses system integrity to determine if any of the system files changed. System files can change either through system administration, or, in a worst case as part of a disk failure. The system integrity tools are run periodically by the Security Officer.

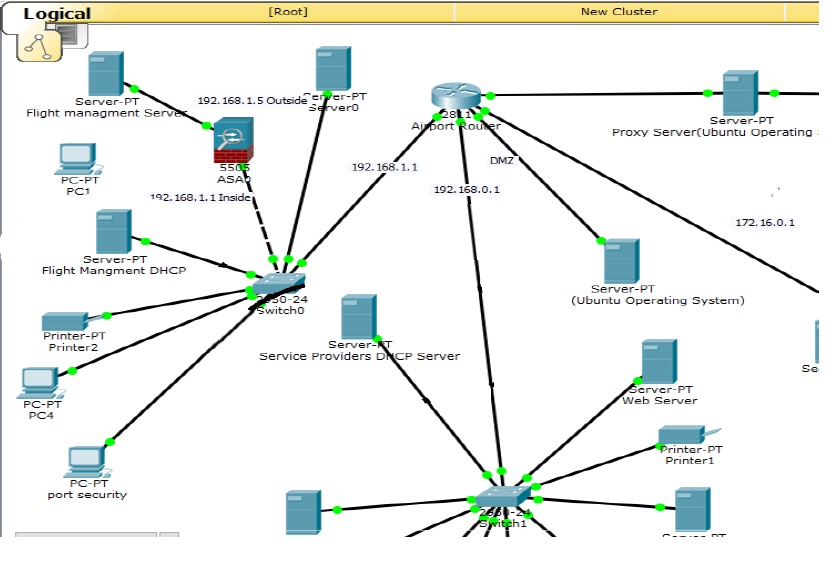


Fig 16: Server Farm

Multiple servers are managed in the server farms. These servers need to be handled carefully since the operations and transactions that takes place highly rely on these servers.

The above diagram is a representation of how servers are associated with the backbone and core of the entire network.

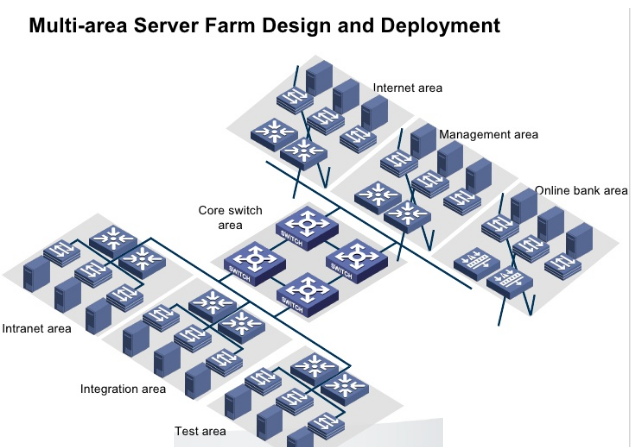


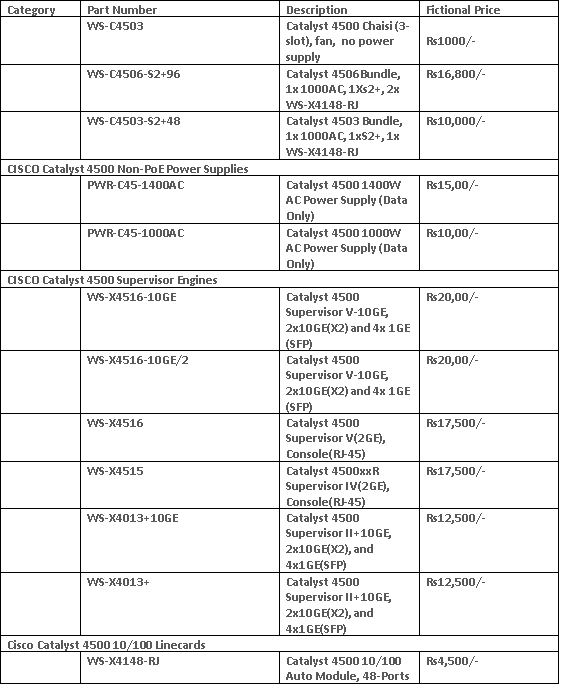
Fig 17: Multi-area Sever Farm Design and Deployement

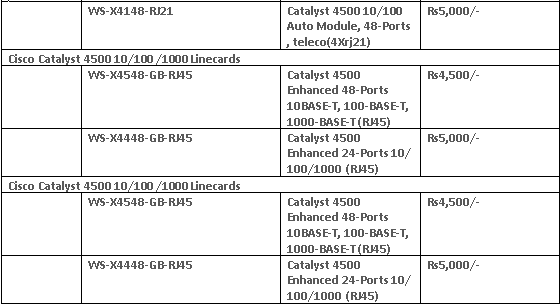
The entire point of organizing a server farm is to make their managing task more easier as they are located in a centralized manner.

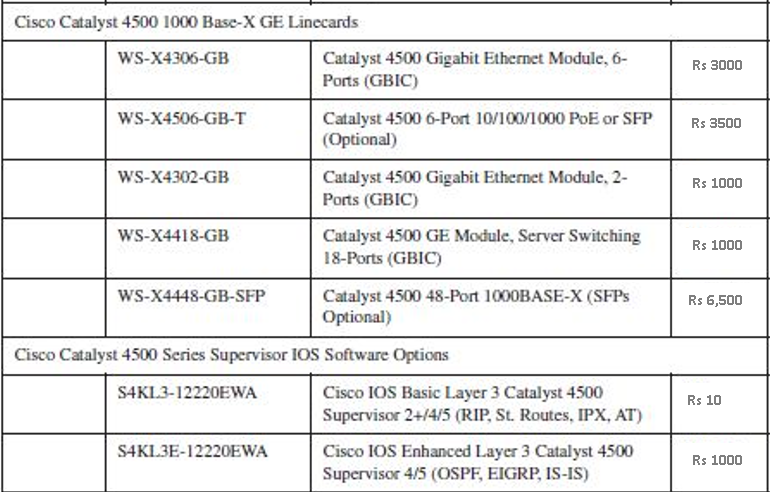
The above diagram is a possible architecture of an airport that can be followed to organize and maintain a server farm.

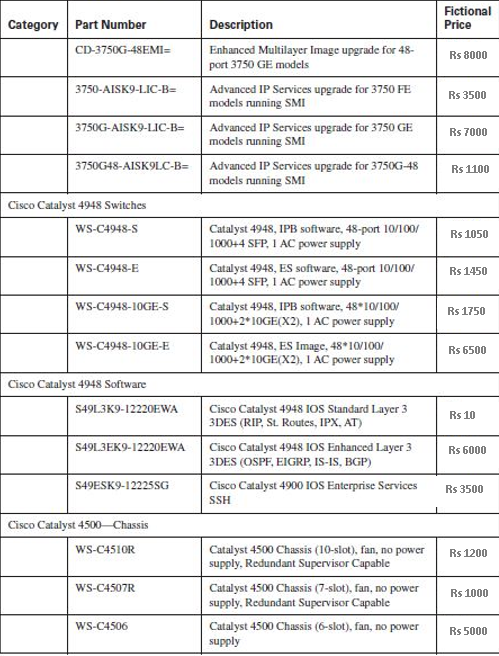
***Develop a bill of materials listing switch models, numbers, prices, and total price.***

BOM for creating an Airport network design are listed below in tables:







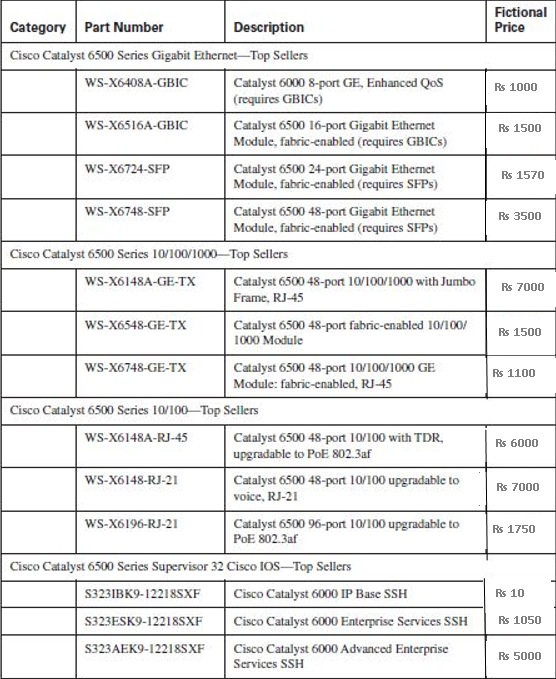


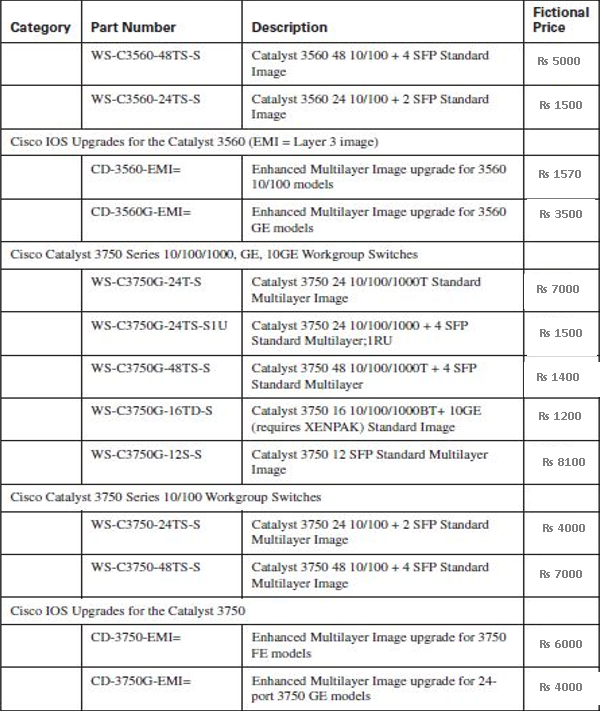
**Rs 3500**

**Rs 1200**

**Rs 1450**

**Rs 1000**





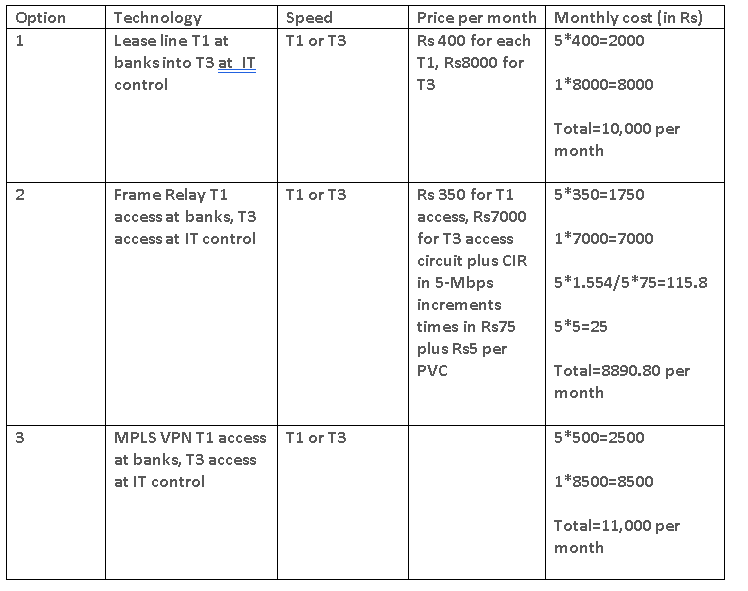
Develop a list of relevant information that should be provided in the Airport WAN Request for Proposal (RFP).

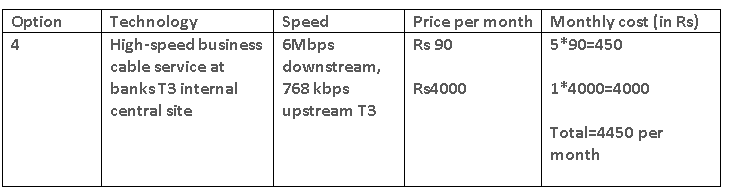
The RFP should include the following items:

■ The number of sites and the minimum bandwidth required to each site

* The service level that should be guaranteed (that the provider will deliver) under the SLA
* The mean time to repair (MTTR) that is acceptable under the SLA
* The level of packet loss, latency, and jitter that is acceptable under the SLA
* How the SLA parameters will be measured
* Any penalties for SLA noncompliance

**Step 2** Airport put out an RFP specifying that it requires at least T1 bandwidth at the remote clinics. The responses to the RFP, indicating the technologies currently available to the airport.





**Network Design strategy**

VLAN technology would be used to create the networks associated with different departments. Every department would be associated with an IP network and mapped with a specific vlan. Appropriate restrictions would be provided between the departments using access control lists. A DHCP server would used for providing dynamic IP addresses to the users on the network.

**VLAN and IP Network Design**

VLAN’s are created and mapped with each department.

1. VLAN 2 – Airport Authority

2. VLAN 3 – Flight service providers

3. VLAN 4 – Guests

IP networks are created for each VLAN and mapped with the same. The IP address range for users and systems which can be used on the specific department is also included.

|  |  |  |
| --- | --- | --- |
| **VLAN** | **IP Network Address** | **IP Address Range** |
| VLAN2 | 192.168.2.0/24 | 192.168.2.1-192.168.2.254 |
| VLAN3 | 192.168.3.0/24 | 192.168.3.1-192.168.3.254 |
| VLAN4 | 192.168.4.0/24 | 192.168.4.1-192.168.3.1/24 |

**Requirement analysis of Active Networking Components** .

**Switches –**

The airport authority has 20 users, the flight service providers have 40 users and the maximum numbers of guests are estimated to be 100. The total number of LAN users is 60, which includes the airport authority and flight service providers. As the guests are on the wireless networks, 3 access points are proposed for accommodating the 100 users. This would require 60 ports for the LAN users, 3 ports for the access points, 1 port for the airport authority server and 1 port for the DHCP server. So a total of 65 ports are required. Switches are available as 24 or 48 port capacity. So 3 nos of 24 port switches, which support vlans are proposed.

**Routers –**

A router which supports high speed internet connection, with the appropriate interface is required. The router also requires an interface which supports 802.1q, which would be used for routing between vlans and access restriction between the vlans. 1 nos router is required.

**Access points –**

As the estimated number of guest users are 100, a total of 3 access points are proposed. This is proposed based on the load which can be shared on the access points.

**DHCP Server –**

A DHCP server is required for assigning dynamic IP addresses to users on the network. The DHCP server service on Windows 2008 is leveraged for the purpose.

**ROUTING PROTOCOL**

A routing protocol is used by routers to dynamically find all the networks in the internet work and to ensure that all routers have the routing table. Basically, a routing protocol determines the path of a packet through an internet work. Examples of routing protocols are Static, RIP, EIGRP, and OSPF.

**Types of routing**

**1. STATIC ROUTING ALGORITHMS:**

Table mappings established by the network administrator before the beginning of routing. These mappings do not change unless the network administrator alters them. Algorithms that use static routes are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple.

**2. DYNAMIC ROUTING ALGORITHMS:**

This algorithm adjusts to changing network circumstances by analysing incoming routing update messages. If the message indicates that a network change has occurred, the routing software recalculates routes and sends out new routing update messages. These messages permeate the network, stimulating routers to rerun their algorithms and change their routing tables accordingly.

**ADMINISTRATIVE DISTANCES**

Administrative distance is the feature used by routers to select the best path when there are two or more different routers to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol.

**CLASSIFICATION OF DYNAMIC ROUTING PROTOCOL.**

Dynamic routing protocols do not change how routing is done. They just allow for dynamic altering of routing tables. There are two classifications of protocols:

***1. Interior Gateway Protocols (IGPs)*** exchanges routing information within a single autonomous system. Common examples include.

***2. Exterior Gateway Protocols (EGPs)*** route between separate autonomous systems. EGPs include. • EGP (The original exterior gateway protocol used to connect to the former internet backbone network ~ now obsolete). • BDP (Border Gateway Protocol: current version, BGPv4m, was adopted around 1995).

***3. RIP Routing Updates*** RIP sends routing-update messages at regular intervals and when

the network lope changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new router. The metric value for the path is increased by I, and the sender is indicated as the next hop. After updating its routing table, the router immediately beings transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates the RIP routers send.

*1. RIP Configuration*

The command syntax is as follows: Router (config)

#router rip Router (config-router)

#network network-number net-mask

*2. IGRP Configuration:*

To configure the IGRP routing process use the router igrp configuration command. The command syntax is as follows.

Router A (config) #router igrp as-number Router A (config) #network network-number net-mask There as number identifies the IGRP process. To specify a list of networks for IGRP routing process, se the network router configuration command. To remove an entry, use the no form of the command.

*3. EIGRP*

Features and Operation EIGRP is sometimes referred to as a hybrid routing protocol because it has characteristics of both distancevector and link-state protocols. For example, EIGRP doesn‟t send link-state packets as OSPF does; instead, it sends traditional distance-vector updates containing information about networks plus the cost of reaching them from the perspective of the advertising router. This makes EIGRP suitable for very large networks. EIGRP has a maximum hop count of 255.There are a number of powerful features that make EIGRP a real standout from IGRP and other protocols. The main ones are listed here. • Support for IP , IPX, and Apple Talk via protocol-dependent modules • Considered classless (same as RIPv2 and OSPF) • Support for VLMS/CIDR • Support for summaries and discontinuous networks networks • Efficient neighbor discovery • Communication via Reliable Transport Protocol (RTP) • Best path selection via Diffusing Update Algorithm (DUAL)

*EIGRP Configuration*

EIGRP is an ideal choice for large, multi-protocol networks built primary on Cisco routers. RouterA(Config)#router eigrp as-number RouterA(Config)#network network-number net-mask.

*4. OSPF Features and Operation OSPF*

configuration requires that he OSPF routing process be enabled on the router with network addresses and area information specified. Network addresses are configured with a wildcard mask and not a subnet mask. The wildcard mask represents the links or host addresses that can be present in this segment. Area IDs can be written as a whole number or doted decimal notation

OSPF provides the following features [8]; • Consists of areas and autonomous systems • Minimizes routing update traffic • Allows scalability Supports VLSM/CIDR • Has unlimited hop count • Allows multi-vendor deployment (open standard) Is supposed to be designed in a hierarchical fashion, which basically means that you can separate the larger internetwork into smaller internetworks called areas.This is the best design for OSPF. American Journal of Engineering Research (AJER) 2015 w w w . a j e r . o r g Page 87 4.10.1

*OSPF Configuration*

To enable OSPF routing, use the global configuration command syntax: Router (configure) #router ospf process-id Router (configure-router) #network address wildcard-mask area area-id.

Now discuss and simulate the RIP Protocol. Routing Information Protocol (RIP) is a true Distance-Vector routing protocol. It sends the complete routing table out to all active interfaces every 30 seconds. RIP only uses hop count to determine the best way to a remote network, but it has a maximum allowable hop count of 15, meaning that 16 is deemed unreachable. Network structure: Banking system in Bangladesh all banks has an IT department. IT department solution all type of IT problem and serve the core network. IT creates a core network diagram. This diagram involves all type of useable network mechanism (Switch, Router, Firewall, Server) etc. Simulation is the most important of any system. An accurate system design, accurate performance and accurate Simulation give best performance of a system.

***Usable Protocol:***

In banking network system data transfer for router configuration using two types of routing protocol.

• RIP (Version 2)

• OSPF OSPF protocol uses the following bank

• HSBC

• Standard Chartered RIP (Version 2)

• NCC bank

• BRAC bank

Project Structure:

Now we discuss and simulate the OSPF protocol. Open Shortest Path First (OSPF) is a routing protocol developed for Internet Protocol (IP) networks by the interior gateway protocol (IGP) working group of the Internet Engineering Task Force.

Now discuss and simulate the RIP Protocol.

Routing Information Protocol (RIP) is a true Distance-Vector routing protocol. It sends the complete routing table out to all active interfaces every 30 seconds. RIP only uses hop count to determine the best way to a remote network, but it has a maximum allowable hop count of 15, meaning that 16 is deemed unreachable.

**Network Implementation Plan**

Ports on the switches are made members of respective vlans. The computers belonging to the respective departments are connected to the respective ports. Intervlan routing is setup on the router, where appropriate access control lists are provided for restricting communication as per the project requirement. The access points are connected to the ports which are on VLAN 4 on the switch as it is used for guest vlan. The DHCP server is setup on VLAN 2, the airport authority vlan, Copyright 2013 @ projectsinnetworking.com and configured with multiple DHCP scopes to provide IP addresses from respective vlans to the users on the network. IP Helper-address feature is configured on the router for users belonging to the flight services provider and guest network to receive dynamic IP addresses from the DHCP server residing on the airport authority network.

**Network Topology Diagram**

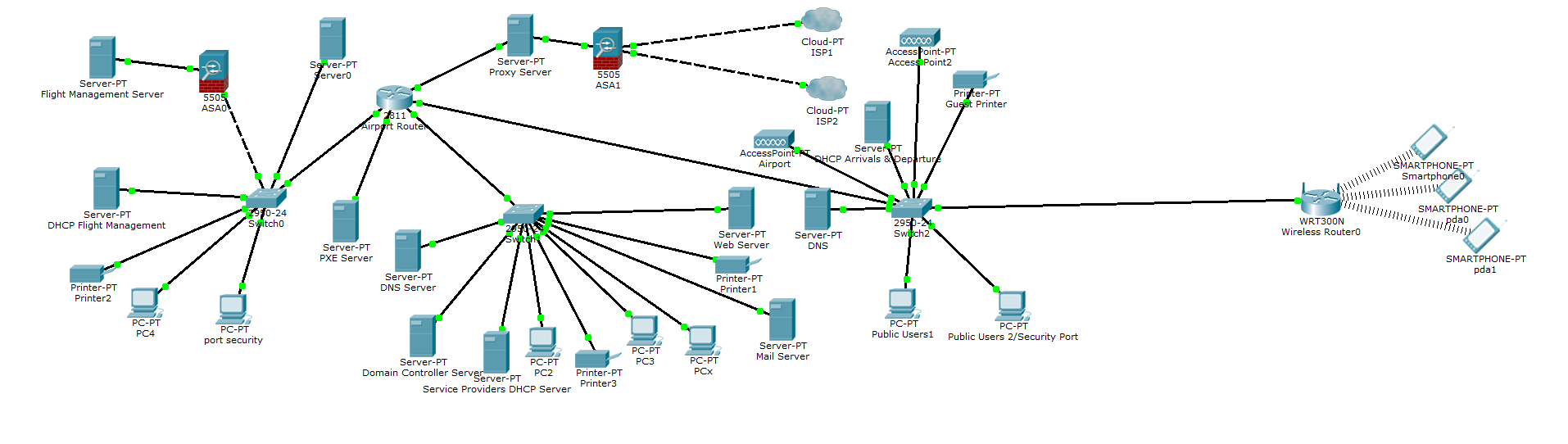
****

Fig 18: Network Topology Diagram

The network topology diagram is as shown above. The DHCP server and the airport authority server are connected to ports on the switch, which are members of VLAN 2, the airport authority VLAN. The respective PC’s belonging to the departments are connected to the appropriate ports on the switch. The access points are connected to ports on the switches, which are members of VLAN 4, which is associated with the guest VLAN. The guest users connect to the access points and are assigned IP address in the appropriate VLAN range.