Advanced Diploma of Information Technology - ICT60220

Manuel Sergio Perez Espitia

ICTNWK546 Assessment Task 2: Project Portfolio

Milestones International College, Melbourne/Victoria, Australia February 24th, 2025

Table of Contents

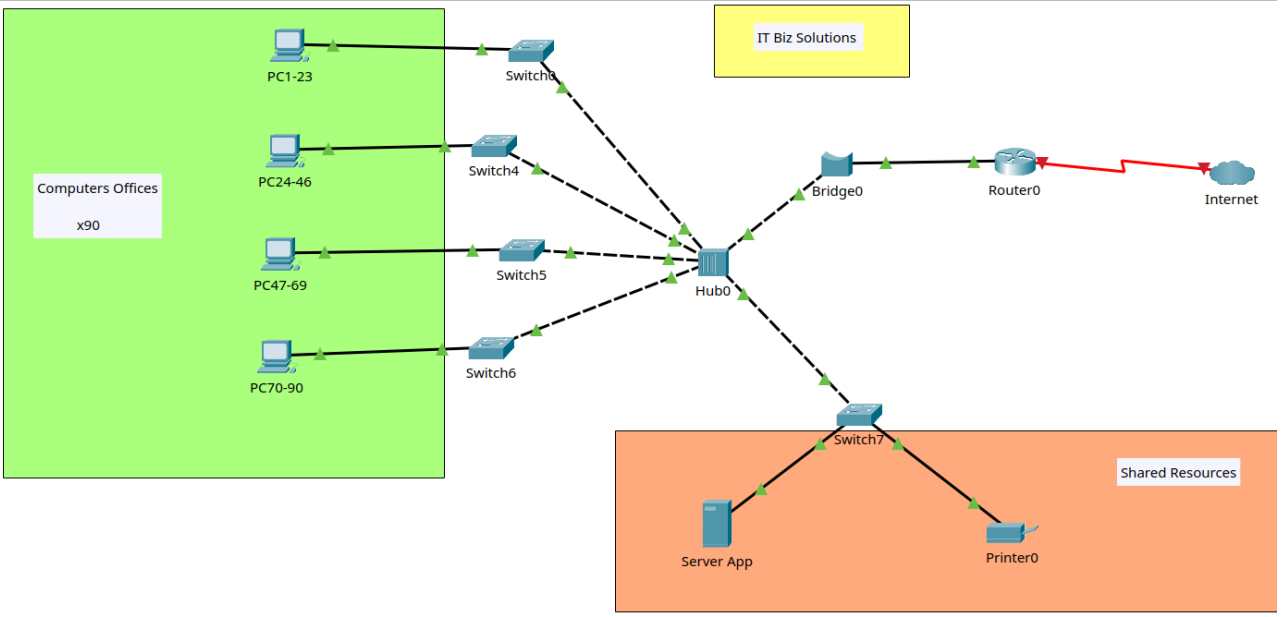
Assessment Task 2: Project Portfolio (Simulation pack, Activities, Project Portfolio Criteria)

security policies and standards:
https://business.gov.au/online/cyber-security/how-to-create-a-cyber-security-policy

Simulation Pack

Case Study – IT Biz Solutions

Current Topology



IT Biz Solutions is a newly formed company offering a wide range of Information and Communication Technology services to businesses of all sizes.

The head office site includes 3 large open plan offices that can accommodate 30 people in each room. (90 PEOPLE)

All computers are connected to the Internet and computers are connected through routers and bridges.

There is a shared printer that is accessible by all computers.

The company has a large number of clients, thus retains client information in its systems. With the number of staff there is a human resources information system containing all confidential staff information.

Information about the company

Company Services

IT Biz Solutions shows clients how to collaboratively transform information technology into business advantages. “We help to translate advanced technology into value for our clients through our range of professional services.”

Managed IT Services

At IT Biz Solutions our Managed IT Services solves all of your technology issues so you can focus on running your business. We do this by giving you all the IT support you need, for a fixed monthly fee.

We are proactive with our support, offering efficient business solutions. We ensure that our clients always know what is planned and what is being implemented when, so there is minimal downtime and all issues are handled before they become problems.

Clients have direct access to our Senior Engineer, who knows how to fix things fast.

The IT Biz Solutions team becomes clients’ outsourced IT team. We continually monitor their system remotely, conducting backups and keeping them updated on what they need to know.
Our clients value not having to deal with IT issues anymore. We handle it all for them.

Managed Continuity

The IT Biz Solutions Managed Continuity service provides an affordable solution to a range of IT issues faced by businesses, such as:

- Data loss
- Fire or flood damage to IT equipment
- Theft of data, PCs or laptops
- Systems crashing
- Staff unable to work due to server issues
- Email not working
- Virus attacks
- No access to files

Managed continuity provides services which are all designed to protect clients’ business, save them money and help their business to grow.

This service includes training of staff in the new system.

Managed Workstations

The IT Biz Solutions Managed Workstations service keeps PCs and laptops healthy, so you can concentrate on your business.

Advantages include:

- Reducing downtime
- Improving system performance
- Automatic installation of updates and upgrades

Hardware Sales and Maintenance

Instead of shopping for your company's computers and information system hardware yourself, our clients can leave this to IT Biz Solutions. We know the industry very well, so we can get equipment at sale prices and keeps PCs and laptops healthy make bulk purchases that attract generous discounts.

This service can also provide regular, guaranteed maintenance for all computers and information system hardware, whether it has been purchased through us or not.

Managed Email Service

The IT Biz Solutions Managed Email Service helps our clients to keep in constant contact with their customers, suppliers and contractors by email.

With Managed Email, we help you overcome common email issues in a cost-effective and efficient way:

- Virus threats
- Loss of emails
- Server downtime
- Lost email connection
- Junk mail filling your inbox
- Genuine emails getting blocked
- Running out of server space
- Unable to locate important emails

It takes about six weeks to set the system up as it involves research into the company's current and future email usage as well as extensive programming. Once it is in place, however, it will function for the life of the company.

Managed Security Services

Every company's confidential information should be comprehensively protected against hacker attacks.

The IT Biz Solutions Managed Security service protects clients' data against internal and external breaches through a cost-effective, affordable solutions.

It helps keep clients safe from:

- Attacks on your email
- Data theft
- Virus attacks
- Unauthorised access to systems
- Downtime

This service takes about two months to put in place, depending on the size of the company's data base, number of users and the complexity of jobs being performed.

Digital Marketing Services

IT Biz Solutions are committed to looking for ways to help our clients grow their business.

We do this by offering a full suite of digital marketing services that deliver specialist support to help our clients do business better in the digital age.

We help with:

- Website design
- SEO
- Social Media
- E-marketing
- Strategy & Planning
- Content development
- Graphic Design
- Training

Website design

In this digital age, a company's website should be at the centre of all the marketing that they do.

Every company absolutely needs a professional-looking website with great content that will inspire the viewer, with inbuilt systems that deliver new leads regularly.

Smart businesses understand the power of the passive income that an online shop can provide.

There are many reasons why a great website is a must for every competitive business:

- Every competitor has a website
- It gives access to millions of potential customers worldwide
- People will look online for products and services
- It helps to future-proof a business
- It represents affordable marketing
- It can be a platform for great advertising
- It provides passive income opportunities
- It is open 24/7
- Can improve customer service
- Provides a portal to share information about your business

Great websites do more than provide information: they can be a portal of communication between customers, employees, suppliers and consultants, and each of these can be maintained securely and personably.

This does not mean that all good websites are complex, but that complex websites offer a greater capacity for effective communication between all stakeholders.

Depending on the website's complexity, it can take up to three months to set up. There should also be some ongoing website maintenance to ensure that the website is always up-to-date.

Training

IT Biz solutions can provide a wide range of training for clients' staff.

Whether it be in website maintenance, email server configuration, or workplace set up, clients staff can be trained to take over these roles through planned courses that include theory and hands-on training.

IT Biz Solutions Fee schedule

For internal use only.

Fees	Details
Managed IT Services	$500 per month
Managed Continuity	$750 per month
Managed Workstations	$150 per workstation per month
Hardware Sales and Maintenance	$200 per month
Managed Email Services	$1,600 set up and staff training $200 per month
Managed security Services	$1,000 annual fee
Digital Marketing Services	$75 per hour
Simple website construction	$5,000
Complex website construction	$8,000
Website maintenance and support	$400 per month
Disaster recovery support	$200 per hour
Staff training for initial website	$1,500

Activities

1. Security Design (Preparing for the security design)

You are required to prepare for the network security design process, as well as identify and analyse threats and risks. This involves:

- Defining processes that needs to be followed in order to plan, build and manage network security. (Network security planning)
- Researching and reporting on major threats to any network security, as well as their origins. (Threat modelling)
- Researching and reporting on network vulnerabilities.
- Determining current risks to the network and developing a risk management plan. (Risk management plan)
- Listing the assets that need to be protected, as well as categorising them according to their value. (ICT assets)

2. Security Design and Security Policies (Create a security design and security policies)

You are to create a security design to protect the network for your chosen organisation. You are also to develop and document relevant security policies which is also to include the auditing of the network, as well as how to respond to incidents. Detailed instructions are included in your Portfolio.

You are also to prepare a short presentation about the work that you have completed that can be presented to a team for feedback. If you are completing this in your RTO, this will be to a small group of students organised by your assessor. If you are completing this based on your own business, it can be a presentation to your team at work or you can also present it to a small group of students.

Further, include the costs of the equipment/software you have identified and document them here.

3. Presentation (Security design presentation)

Provide your presentation to your team about the security design you have developed. Make sure you provide your team the opportunity to provide feedback. Following the presentation, you will document the feedback in your Portfolio, as well as your response.

During the presentation, you are to use oral communication skills including:

- speaking clearly and concisely
- asking questions to idresponding to questionComprus as reqresponding to questions as requiredresponding to questions as requiredresponding to questions as requiredresponding to questions as requireduired entify required information
- responding to questions as required
- using active listening techniques to confirm understanding
- observational techniques to ensure that everyone is participating so that you can gain a range of different perspectives.

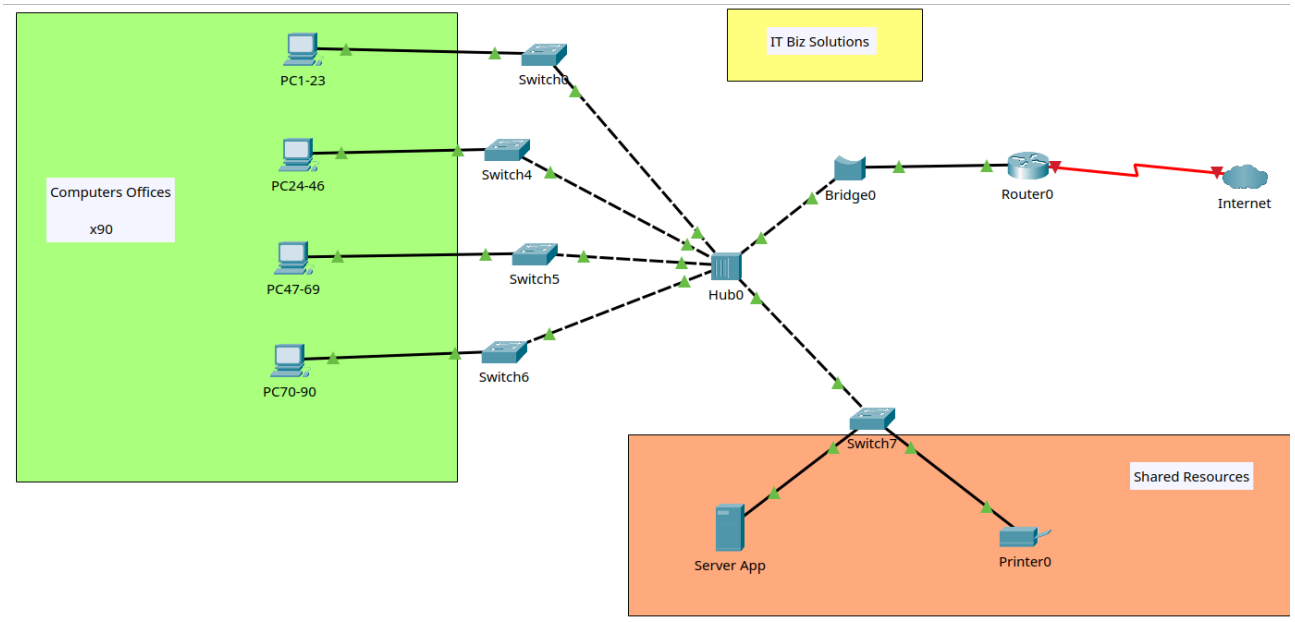
This can either be viewed in person by your assessor or you may like to video record the session for your assessor to watch later. Your assessor can provide you with more details at this step. Make sure you follow the instructions above and meet the timeframes allocated.

Following the presentation, include the feedback you received in Section 1 of your Portfolio and make amendments to your quality management plan to include the corrective action. Further report on the skills of staff, confirming their ability to meet quality standards or otherwise.

Title of my presentation: MIC -- Manuel Perez - Security Design for IT Biz Solutions 2025

Planning for network security design

Current design



Network details

Type: LAN (Local Area Network)
Topology: Star

Network Nodes

Type	Quantity
PC	90
Switch	5
Hub	1
Bridge	1
Router	1
ISP Connection	1
Server App	1
Printer	1

Identified Issue

1. The bandwidth is being occupied by the additional traffic caused by the hub and the bridge.
2. Poor Segmentation. The network segmentation provided by the bridge is poor as it sends all packets to all nodes regardless of the segment.
3. There are no security features to protect against DDoS attacks
4. There are no backup servers or methods to maintain information redundancy.
5. The application server and the storage server are the same

Work details

Scope

- Evaluate current network performance and identify traffic congestion issues
- Develop and implement solutions to optimise traffic flow
- Monitor the implemented changes and adjust configurations as needed
- Ensure network security and improve user experience

Complaints

Users report slow internal speeds and delays in accessing local storage.

Identified Issue

High network congestion in working hours.

Planned Network Strategy

- Segment the network by creating VLANs.
- Implement Quality of Service (QoS) policies to prioritise critical applications.
- Re-design network to improve bandwidth.
- Enhance network security by introducing a firewall, access controls and authentication measures

Planned Design

1. Replace hubs and bridges with switches.
2. Segment the network with VLANs
3. Balance the number of devices connected to the switches
4. Add at least one firewall
5. Add a backup server with disk in RAID

Advantages of the new network design

1. Unnecessary network traffic will be eliminated by reducing noise across all nodes by using hubs and bridges.
2. Network security will be increased with segmentation, and traffic will remain within the same segment.
3. Switch performance can be increased by lower network traffic, so switches can respond better to sudden increases in traffic.
4. Bandwidth will be used in the best way by eliminating all unnecessary traffic.
5. Adding a firewall to the network helps the company prepare for DDoS attacks
6. With a backup server the company can have a copy of all the data, and by using the disks in RAID we can recover the information in case parts are destroyed.

Budget Available

The project must present a cost report to evaluate for stakeholders.

Site Access Arrangements & Timelines

All access credentials will are removed for simulated network management tools.

Implementation

The methodology chosen for planning and implementing network security design is project management body of knowledge (PMBOK). The planning will be divided into 5 steps:Legislative context:

1. Initiating: Gathering information about the security design, objectives, risks, needs, assets and current policies to align with project objectives, legislative context and governance. Responsibilities. This information will be used to define best practices for the adoption of PMBOX, this decision would be made by the stakeholders and the PMBOK work team.
2. Planning: Individual work teams will be created for each area of the company. These teams will be responsible for planning the integration based on their responsibilities and the company's policies and principles as well as the allocation of resources.
3. Executing: The project will be executed according to the company's principles and objectives, based on the resources allocated for each task. The objective of this step is to align the company with the objectives defined in the PMBOK for this project.
4. Control:Changes will be controlled and monitored to ensure compliance with PMBOK quality standards. I would emphasize efforts on network security to detect potential security breaches and failures in security systems.
5. Closure: Cessation of activities and delivery of the performance report

List of tasks

1. Get the current network diagram
    a. Threats and risks
2. Get a list of ICT assets and data to be protected
3. Develop network security policies
4. Develop a risk management plan
5. Propose a network diagram
    a. Technical specs for network nodes
    b. Network segmentation
    c. Develop monitoring plan

ICT assets

Based on the current topology, this is the list of assets:

Category	Description	Total Price	Importance
Human Resources	Human Resources	Not Calculated	High
Data	Customer Information	Not Calculated	High
	Providers Information	Not Calculated	High
Hardware	PCs	$90,000	Medium
	Switches	$7,500	Medium
	Server Application	$2,000	Medium
	Printer	$1,500	Low
	Hub	$30	Low
	Bridge	$25	Low
	Router	$1,070	Medium
	HardDisks	$500	Low
	Uninterruptible Power Supply (UPS)	Not Calculated	Medium
	Backup & Redundancy Server (NAS)	$5,000	Medium
Software	Operating System Licenses	$9,000	Medium
	CRM System	$5,000	High
	Enterprise Cybersecurity Suite	$10,000	Medium
	Enterprise Data Recovery Tools	$10,000	Medium
	Enterprise Monitoring Tools	$10,000	Medium
	Enterprise Digital Resources	$30,000	Medium
	Enterprise Graphic Design Suite	$10,000	Low
	Knowledge Base	Not Calculated	Medium
Services	Training Material	Not Calculated	Low
	International Certifications	Not Calculated	Low
Professional Talent	Professional Talent	Not Calculated	High

Threat modelling

Based on statistics, the greatest risks for a company, regardless of its size, are ransomware, social engineering attacks and DDoS attacks.

Ransomware

This is a malware that encrypts data, this is known as data kidnapping. Usually the attacker demands money to release the data.

The most common form of infection is through emails, downloading files from the Internet, and it could also happen that a vulnerability is exploited. Once the malware has encrypted the data, it displays a message with instructions for its release.

In the event of a ransomware attack, the company would lose one of its most important assets. Because it would lose access to critical information such as customer information, the knowledge base, client information, and accounting information.

Possible consequences

- Loss of critical information
- Financial costs
- Information leaks on the Internet
- Loss of trust

Possible System vulnerabilities

- Outdated systems
- Poor backup management
- Poor staff training

Social Engineering Attacks

This involves the manipulation of employees, which consists of tricking them into stealing sensitive information such as access credentials.

The most common form of attack is through phishing, which takes advantage of trust to make people make mistakes.

If such an attack were to occur, it could allow unauthorised access to the company's computer systems, where it can steal computer resources, financial information or customer information.

Possible consequences

- Credential theft
- Financial fraud
- Information leak on the Internet
- Loss of trust

Possible system vulnerabilities

- Poor staff training
- Poor access control to computer systems
- Poor password security policy

DDoS Attack

This is an attack that tries to generate traffic to overload a company's servers.

Attackers can use almost any device with Internet access. These devices are known as botnets. Botnets send large amounts of requests in a short period of time that saturate the company's infrastructure, causing failures. For example, the website, servers and applications stop working.

Possible consequences

- Loss of services
- Economic losses
- Loss of trust and reputation

Possible system vulnerabilities

- Poor protection against malicious traffic
- Network infrastructure unable to scale
- Poor network monitoring

Risk management plan

Threat	Likelihood	Impact	Risk Level	Risk Control Measure
Ransomware	**High**	**High**	**High**	• Implement regular data backups • Keep systems up to date • Use endpoint protection • Employee regular training on recognising phishing
Social Engineering Attacks	**High**	**Medium**	**Medium**	• Enforce multi-factor authentication • Employee regular training on cybersecurity awareness • Implement email filtering to detect phishing attempts • Implement policies for confidentiality information • Implement verification procedures before sharing sensitive information.
DDoS Attacks	**Medium**	**High**	**High**	• Use cloud-based traffic filtering • Implement firewalls and intrusion prevention systems • Move to a scalable network infrastructure

General Security policies

Legislation

Workplace Health and Safety Act 2011 code

As part of the IT team, I am required to follow legal guidelines for the management of electronic equipment and networks such as cabling and racks. As part of my duties, I must maintain and make modifications to the physical infrastructure of the IT Biz Solution’s network.

Code of conduct

Telecommunications Code of Practice 2018

As a service provider to IT Biz Solutions, I will ensure that I provide accurate, detailed information and fair pricing.

Regulations

Workplace Health and Safety Regulations 2021

As a service provider to IT Biz Solutions, I will ensure that I attend to the client's safety training as well as comply with the Incident Reporting policy. In particular, my regular duties involve following Electrical Safety regulations.

Standards

Customer service standards

As a service provider of IT Biz Solutions, I will ensure that I offer the highest standard of service as well as follow the same quality standard in after-sales services.

Proposed Security Policies

Based on the services provided by the company, I consider it necessary to include additional security policies to accompany and guarantee the protection of the information base on the network security design.

So I'm going to focus on protecting the company against malware (ransomware) and phishing attacks.

Legislation

GDPR - General Data Protection Regulation

Protect people data privacy in the European Union.

Purpose

- Ensuring that people's data is protected
- penalises companies that do not comply with the legislation

Key procedures

- Protection of information: Role-based access control, in addition to using multi-factor access controls
- Data protection: Encrypt data and audit access to information
- Audits: Periodic audits, in case of detecting vulnerabilities, require companies to report the incident within 72 hours

NIST Cybersecurity Framework

It was designed in the US to improve the cybersecurity of companies

Purpose

- Helps a company understand, identify, protect, detect, respond to and recover from an attack
- Helps reduce the impact of attacks such as ransomware and phishing

Key procedures

- Helps reduce the impact of attacks such as ransomware and phishing
- Threat Control: Detects potential threats and executes automatic procedures to respond to incidents
- Audit: Periodic audit in search of vulnerabilities in the company's systems

California Consumer Privacy Act – CCPA

Designed to protect people's personal information.

Purpose

- Provides control actions to users of computer systems
- Seeks to guarantee the security of information against theft and fraud

Key procedures

- Access control: Adds strict authentication controls to access personal data
- Threat control: Implements firewalls to prevent intrusions into systems
- Audit: Periodic audits of access logs in search of anomalies

ISO/IEC 27001 (Information Security Management)

International standard for implementing an Information Security Management System (ISMS).

Purpose

- Access control: Protect information from unauthorised access and attacks.
- Integrity control: Ensure confidentiality, integrity and availability of data.

Key procedures

- Access control: Secure password policies and multi-factor authentication.
- Threat control: Add perimeter security with firewalls and malware detection.
- Authorship: Periodic audits for risks and internal procedures

Standards

Center for Internet Security - CIS Controls

A set of 20 security procedures designed to mitigate threats.

Purpose

- Establish a security framework to reduce ransomware and phishing risks.
- Improve incident response capacity.

Key procedures

- Access control: Includes the implementation of access policies by levels.
- Threat control: Requires monitoring of logs and detection of suspicious activity.
- Audit: Regular audits based on risk metrics.

Payment Card Industry Data Security Standard - PCI DSS

Mandatory standard for processing card payments.

Purpose

- Protect credit card data from fraud and cyberattacks
- Prevent phishing targeting customers and employees.

Key procedures

- Authentication control: Use of multi-factor authentication for system access.
- Threat control: Data encryption and monitoring of suspicious transactions.
- Audit: Periodic audits for PCI compliance failures.

MITRE ATT&CK Framework

Adoption of knowledge bases of tactics and techniques used by cyber attackers.

Purpose

Help companies understand attack methods, to develop effective strategies against ransomware and phishing attacks.

Key procedures

- Access control: Alert system and monitoring of access attempts, focused on unauthorised access
- Threat control: Performing attack simulations to evaluate the effectiveness of the company's countermeasures
- Audit: Regular audits to update tactics based on the most recent techniques found

Codes of Conduct

OECD Code of Good Practice

Set of countries OECD standards, guidelines and procedures on digital security.

Purpose

- Help the company create effective cybersecurity policies
- Reduce the impact of cyberattacks on critical infrastructures

Key procedures

- Access control: Role-based access control and permission segmentation
- Threat control: Threat control with the use of specialized tools to detect attacks
- Audit: Periodic audits on the analysis of the company's vulnerabilities

ISACA Code of Conduct

Set of ethical standards and practices for information security professionals.

Purpose

- Helps the company to emphasise risk management
- Seeks to ensure the protection of sensitive data

Key procedures

- Access control: Implementation of controls for the strict validation of user credentials
- Threat control: Creation and implementation of contingency actions against ransomware
- Audit: Periodic audits on logs and security events to create detailed reports

Code of Ethics - ISC

Set of standards aimed at professionals, which establishes ethical standards of behaviour.

Purpose

- Promote good practices in cybersecurity
- Protect user information and privacy

Key procedures

- Access control: Restricted access based on minimum privilege policies
- Threat control: Regular penetration testing
- Audit: Periodic audits that focus on compliance with standards

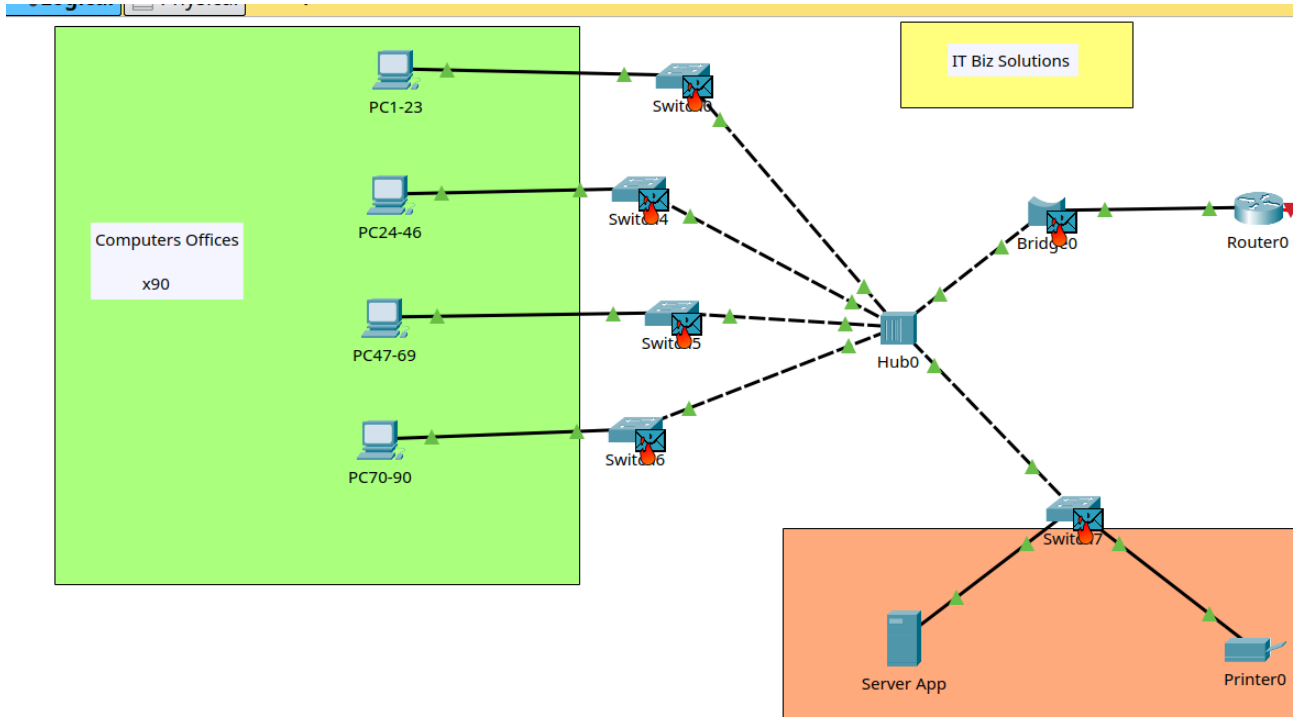
Network monitoring software

- Wireshark – for packet analysis
- Cisco Packet Tracer – for network simulations

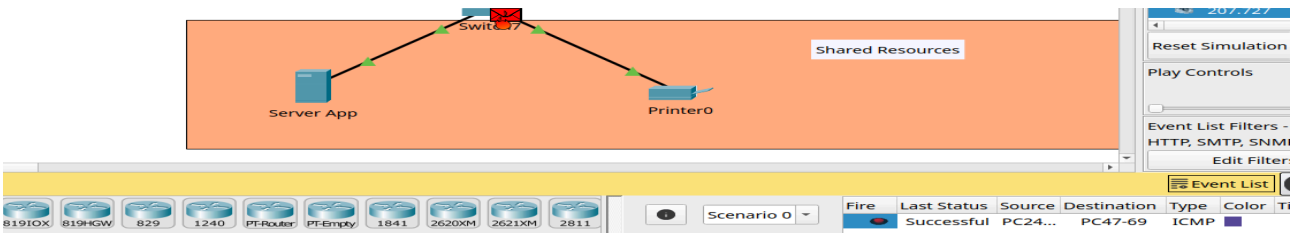
Network capacity and traffic congestion evaluation

Example of send a package from PC01 to any other PC.

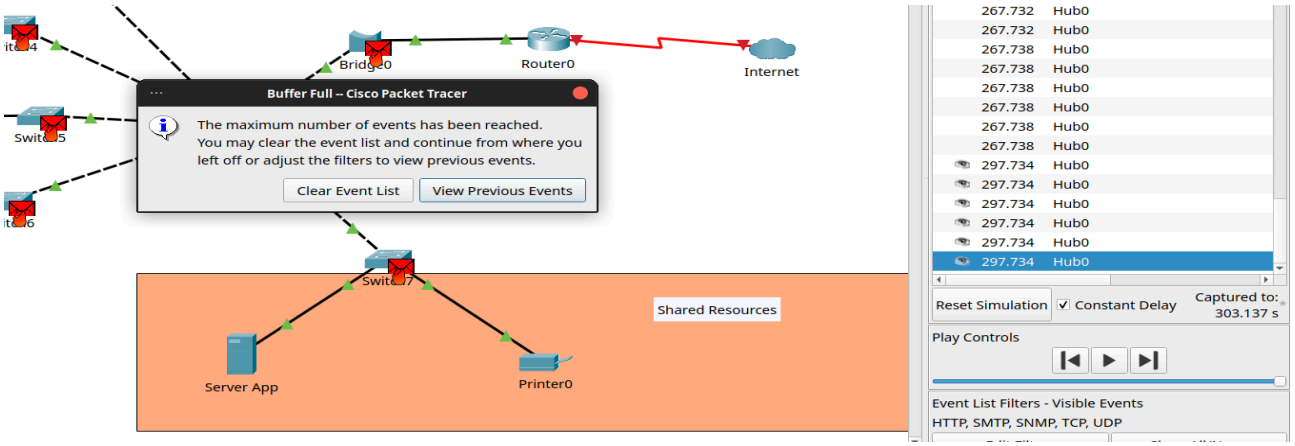
The packet is forwarded to all nodes in the network by the Hub. When the Bridge receives the packet, it replicates the packet and these packets are forwarded.



Even though the packet has already arrived at its destination, the network is still saturated with replicated packets.



Eventually the network becomes saturated, causing delays. In this capture, it can be seen that the simulator exhausted the event queue due to the large number generated by a single packet.



Projected Costs

Based on Planned Network Strategy and Security policies, The costs for hardware, software and additional services are:

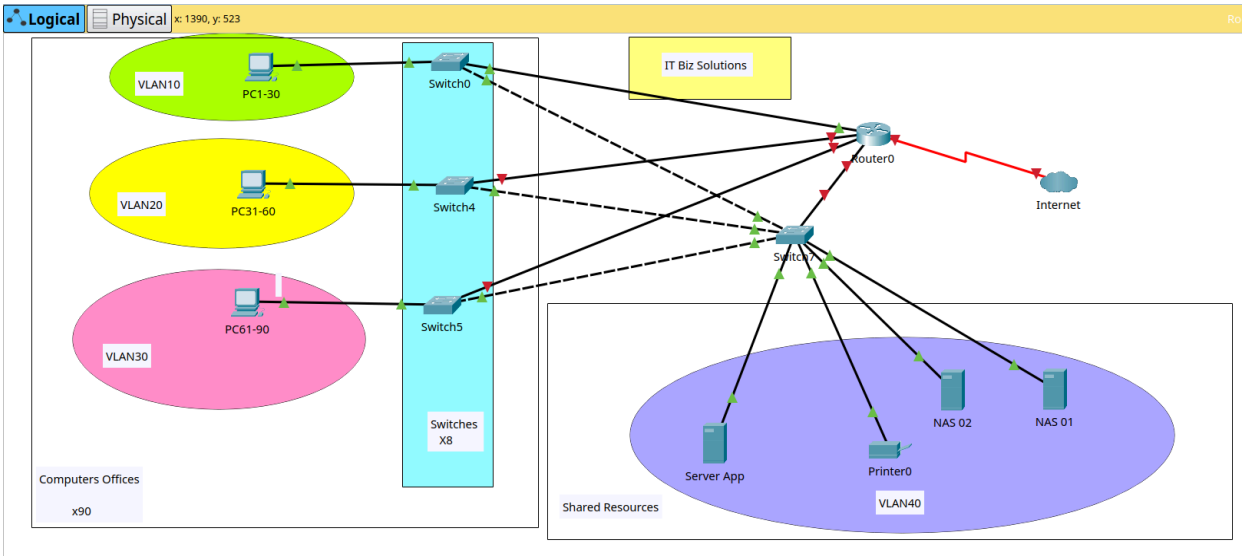
Given the advantage of being a company specialising in technology services, the cost of their own services was taken as a reference.

The project would last 3 months, during which the network would be redesigned, employees would be trained in how to avoid cyber attacks from the Internet (ransomware and phishing) and a NAS server with a mirror backup would be created. The current application server will no longer be used as a data backup; these functions will be managed by the NAS.

Item	Quantity	Unit Cost	Total Cost
Hardware			
Switches	4	-	$6,000
Firewalls	2	-	$2,000
Router	1	$1,070	$1,070
NAS	2	-	$4,000
Disks (200TB)	20	270	$5,400
Monthly Services			
Managed IT Services	3 months	$500	$1,500
Managed Continuity	3 months	$750	$2,250
Human Resources Training	3 months	$1,500	$4,500
Total Project Cost			**$26,720**

Proposal Network Design

For simplicity of design, PCs and switches are grouped together.



Network details

Type: LAN (Local Area Network)
Topology: Extended star

Network Nodes

Type	Quantity
PC	90
Switch	9
Router	1
ISP Connection	1
Server App	1
NAS	2
Printer	1

PRESENTATION

Title of my presentation: MIC -- Manuel Perez - Security Design for IT Biz Solutions 2025

Feedback

I showed my presentation to some friends with experience in the technology sector, and they shared their opinions. In summary it is as follows:

The proposed solutions are only focused on local solutions, and do not contemplate the use of hybrid technologies that are more effective against DDoS attacks. Nor is the possibility of using cloud technologies to facilitate network scalability and the adoption of technologies to help against ransomware and phishing attacks.