|  |  |
| --- | --- |
| C:\Users\Емил Йорданов\Downloads\logo.png | **ВИСШЕ ВОЕННОМОРСКО УЧИЛИЩЕ „Н. Й. ВАПЦАРОВ“**  ***9002 Варна, ул. „В. Друмев“ 73, тел.052/632-015, факс 052/303-163*** |
| ***“FILII MARIS SUMUS”*** |
|  |  |

**ФАКУЛТЕТ „ИНЖЕНЕРЕН” – КАТЕДРА „ИНФОРМАЦИОННИ ТЕХНОЛОГИИ“**



**КУРСОВ ПРОЕКТ**

**по дисциплина от 4-ти или 5-ти семестър**

**НА ТЕМА:**

„Инзграждане на локална мрежа в малка бизнес сграда в среда на packet tracer”

**Студент:   
Никола Иванов**

**Фак. №12220124**

**Специалност:   
ИКТ**

**2022 г.**

**гр. Варна**

Contents

[1. Хардуерни изисквания: 2](#_Toc131153593)

[2. Адресен план 3](#_Toc131153594)

[3. Конфигуриране на мрежата 5](#_Toc131153595)

[3.1. Комутатори 5](#_Toc131153596)

[3.1.1. L3 Комутатори 5](#_Toc131153597)

[3.1.2. L2 Комутатори 5](#_Toc131153598)

[3.2. HSRP 5](#_Toc131153599)

[3.3. VTP 6](#_Toc131153600)

[3.4. Inter-VLAN routing 7](#_Toc131153601)

[3.5. Сървърна стая 8](#_Toc131153602)

[3.5.1. DHCP server 8](#_Toc131153603)

[3.5.2. Email Server 9](#_Toc131153604)

[3.5.3. WEB server 10](#_Toc131153605)

[3.5.4. DNS server 11](#_Toc131153606)

[3.5.5. FTP и TFTP сървър 12](#_Toc131153607)

[3.5.6. Безжична мрежа 14](#_Toc131153608)

[4. Мерки за сигурност: 15](#_Toc131153609)

[4.1. Запомняне на MAC адреси 15](#_Toc131153610)

[5. IoT 16](#_Toc131153611)

[5.1. Противопожарна система: 16](#_Toc131153612)

[5.2. Система за наблюдение: 16](#_Toc131153613)

[5.3. Възможности за разширение: 16](#_Toc131153614)

[6. Възможности за разширение: 16](#_Toc131153615)

В днешната дигитална ера - добре проектираната мрежа е основата на всеки успешен бизнес. Мрежа, която е надеждна, ефективна и сигурна, може да помогне на една организация да комуникира и да си сътрудничи безпроблемно в различни отдели и етажи. В този курсов проект ще обсъдим дизайна на мрежа на IT компания, която работи на три етажа. Всеки етаж има различни отдели, които трябва да бъдат разделени в отделни виртуални мрежи. Също така ще разгледаме хардуерните изисквания, протоколите за маршрутизиране и мерките за сигурност, които са необходими, за да гарантираме, че мрежата е стабилна и защитена.

Дизайнът на мрежата за тази компания ще се основава на йерархичен модел, състоящ се от три слоя - слой за достъп, слой за разпространение и основен слой. Слоят за достъп отговаря за свързването на устройства като компютри, принтери и сървъри към мрежата. Разпределителният слой отговаря за свързването на слоя за достъп с основния слой, докато основният слой отговаря за маршрутизирането на трафика между различни етажи. В нашия случай основния и разпределителния слой са събрани в едно.

Мрежата ще се състои от L2 комутатори за всяка подмрежа. Всички комутатори L2 ще бъдат свързани към два комутатора L3 - единият от които ще бъде конфигуриран като основен, а другият ще бъде конфигуриран като резервен. Този дизайн ще осигури резервиране и висока достъпност на мрежата. В случай на повреда в един от комутаторите L3, другият комутатор ще поеме основната роля и трафикът ще продължи да тече без прекъсване.

За симулация на мрежата се използва софтуерът Cisco Packet Tracer

# Хардуерни изисквания:

За проектирането на мрежа за компания, която заема три етажа с отделни отдели, са необходими следните елементи:

Комутатори: Ще бъдат необходими 12 L2 комутатора(по един за всеки VLAN) и 2 L3 комутатора(1 основен и 1 бекъп комутатор за резервност).

Кабелиране: Етернет кабелиране е необходимо за свързване на всички суичове помежду си и свързване на устройства към тях.

Протоколи:

Мрежата ще използва протокола за резервни рутери (HSRP), за да осигури резервност и аварийно възстановяване в случай на отказ на основния L3 комутатор. HSRP е протокол на Cisco, който осигурява резервни рутери, като позволява на два или повече рутери да споделят виртуален IP адрес. Един рутер ще действа като активен и ще препраща трафика, докато другият ще бъде в режим на готовност и ще бъде готов да поеме в случай на отказ.

VTP е прокол, който позволява пренасяне на създадените VLAN-нове между различните комутатори. При VTP избираме комутаторите, които ще действат като сървър и ще изпращат техните VLAN-ове към тези комутатори, които биват настроени като клинети.

За да работи VTP, вссички комутатори ще имат нужда от настроена SSH връзка. SSH позволява отдалечена връзка към устройствата.

# Адресен план

Мрежата е разделена на 9 подмрежи както е изобразено по-долу:

Таблица(1.1 Адресен план на първи етаж)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Първи етаж | | | | |
| VLAN | Име | Gateway | Мрежови адрес | Хост Адреси |
| 10 | Customer Support | 192.168.10.3 | 192.168.10.0 | 192.168.10.4-254 |
| 20 | Sales + Reception | 192.168.20.3 | 192.168.20.0 | 192.168.20.4-254 |

(**Фигура 2.10**) Визуализация на първи етаж

Graphical user interface, diagram

Description automatically generated

(**Таблица 1.2)** Адресен план на втори етаж

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Втори етаж | | | | |
| VLAN | Име | Gateway | Мрежови адрес | Хост Адреси |
| 30 | HR | 192.168.30.3 | 192.168.30.0 | 192.168.30.4-254 |
| 40 | Server Room | 192.168.40.3 | 192.168.40.0 | 192.168.40.4-254 |
| 50 | Tech | 192.168.50.3 | 192.168.50.0 | 192.168.50.4-254 |
| 60 | Devs | 192.168.60.3 | 192.168.60.0 | 192.168.60.4-254 |

(**Фигура 2.11**) Визуализация на втори етаж

Diagram

Description automatically generated

Таблица(1.3 Адресен план на трети етаж)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Трети етаж | | | | |
| VLAN | Име | Gateway | Мрежови адрес | Хост Адреси |
| 70 | Management | 192.168.70.3 | 192.168.70.0 | 192.168.70.4-254 |
| 80 | Finance | 192.168.80.3 | 192.168.80.0 | 192.168.80.4-254 |
| 90 | Data | 192.168.90.3 | 192.168.90.0 | 192.168.90.4-254 |

(**Фигура 2.12**) Визуализация на трети етаж

Diagram

Description automatically generated

За Default Gateway на всяка подмрежа е избран адреса който завършва на 3, тъй като 1 и 2 са използвани за физически адреси на двата Layer 3 комутатора. Адресът .3 е виртуален IP адрес, който е използван за да обозначи устройство  с по-голям приоритет между двата Layer 3 комутатора. Ако основния комутатор бъде изключен, то тогава резервния става главен и приема адреса завършващ на 3. Така позволяваме безпроблемна работа в случай, че първият комутатор бъде изключен.

Това става възможно чрез протокола HSRP(Hot Standby Router Protocol). Конфигурацията му става възможна със следните команди:

# Конфигуриране на мрежата

## Комутатори

Базовата конфигурация на един комутатор се състои от настройка на името, съобщение при опит за вход, пароли при влизане и настройка на конзолна и виртуални линии. Настройката на линиите е изключително важна тъй като всеки, който има данните за вход ще има право да настройва комутатора. Името, банера и паролите се настройват от конфигурационен режим.

(**Фигура 3.10**) Базова конфигурация на комутатор



Настройването на виртуалните линии не се показва тук, тъй като те ще са нужни за друг протокол.

### L3 Комутатори

Интерфейсите на Layer 3 комутаторите се използват за връзка с Layer 2 комутаторите. Тъй като те осъществяват връзка между различните подмрежи, техните портове се настройват като trunk, за да е възможна комуникация. Ето как се настройват протовете на един Layer 2 комутатор:

(**Фигура 3.11**) Настройка на L3 Комутатор



### L2 Комутатори

Layer 2 комутаторите имат 2 вида интерфейси. Гигабитови и Етернет. Гигабитовите се използват за връзка с Layer 3 Комутаторите, докато етернет интерфейсите се свързват към крайните устройства - компютри, принтери, телефони и тн.

## HSRP

HSRP е протокола, който позволява да имаме резервни и основни устройства с еднакъв виртуален IP адрес, което позволява безпроблемна работа при повреда.

(**Фигура 1.10**) Конфигуриране на HSRP

|  |
| --- |
| int vlan 10 standby version 2 standby 10 ip 192.168.10.3 standby 10 priority 110 standby 10 preempt |

Както е показано на фигурата настройването на този протокол става чрез избиране на нуждната версия, виртуалния IP адрес, който ще се използва, приоритета и накрая дава възможността на устройството да стане основен в случай, че то е работещото устройство с най-голям приоритет. Единствената разлика, която правим при настройката на този протокол на резервния комутатор е, че използваме по-малък приоритет. Тази настройка се повтаря за всяка виртуална подмрежа.

## VTP

За да се опрости настройването на VLAN на всеки комутатор, L3 комутаторите са конфигурирани като VTP сървъри, докато L2 комутаторите ще бъдат конфигурирани като VTP клиенти. Тази конфигурация ще позволи на комутаторите L3 да разпространяват информация за всеки VLAN към L2 комутаторите, което ще намали натоварването от конфигурирането на всеки комутатор поотделно. За да бъде възможно разпространяване на VLAN чрез VTP е нужно настройването на SSH връзка. Това става със следните команди:

(**Фигура 1.20)** Конфигуриране на SSH

|  |
| --- |
| username admin password passwd ip domain-name itmaster.com crypto key generate rsa 1024 line vty 0 15 transport input ssh login local |

След като вече сме настроили виртуалните линии, имаме възможност и за настройка на VTP. Ето какви команди се използват при L3 комутаторите:

**(Фигура 1.30)** Конфигуриране на VTP

|  |
| --- |
| vtp mode server vtp domain itmaster.com vtp password cisco vtp version 2 |

С тези команди L3 комутаторите стават VTP сървъри и могат да разпространяват техните VLAN-ове на всички VTP клиенти. Единствената разлика при конфигуриране на VTP клиентите е в командата mode, където server бива заменено с клиент.

След правилна настройка на VTP сървърите и клиентите, L3 комутаторите ще започнат да изпращат пакети с техните VLAN-нове към клиентите и така всяко устройство в мрежата ще има идентичен VLAN.

## Inter-VLAN routing

За да бъде възможна комуникацията между всяка подмрежа в повечето случаи се използва “Router on a stick”, но тъй като в нашата топология не присъства маршрутизатор, за целта ще използваме двата L3 комутатора. Конфигуриране на  “Router on a stick” е доста сложно. То се състои от енкапсулация и настройка на подинтерфейси за всеки VLAN, но този процес е доста по-лесен при L3 комутаторите. Нужна е само една команда и тя е следната:

(**Фигура 3.13**) Настройване на Inter-VLAN routing

|  |
| --- |
| ip routing |

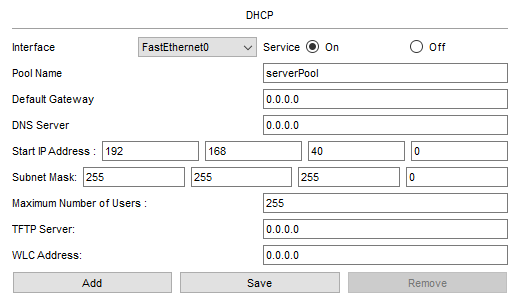
## Сървърна стая

### DHCP server

Различни устройства могат да бъдат настроени като DHCP сървър като при избор на това устройство трябва да се има в предвид бюджета, който е отделила фирмата и нейните нужди. Сървъри могат да бъдат компютри, виртуални машини, сървърни устройства, маршрутизатори и др. Ако една фирма е все още малка и има 30 служителя, тя няма да има нужда от големи сървърни устройства.

При настройката на DHCP сървър може да се използва графичен и команден интерфейс. В симулацията се използва сървърно устройство което се намира в сървърната стая(VLAN 40) по този начин:

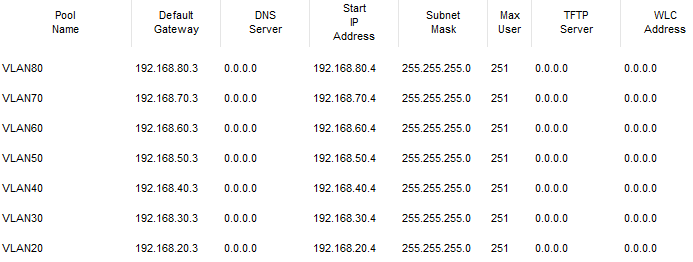
(**Фигура 3.24**)Конфигуриране на DHCP



След като изберем услугата DHCP в полето с услуги, ние имаме възможност да изберем име на адресното поле, неговия default gateway, начален и краен адрес и др.

Ето как изглеждат адресните полета на нашата мрежа:

(**Фигура 3.25**) Адресни полета



Тъй като DHCP сървърът е в отделен VLAN, нито един компютър няма да има възможност да го намери. Единственият начин е да информираме L3 комутаторите за съществуването на този сървър, за да може да препраща пакетите към този адрес. Това става възможно със следната команда:

(**Фигура 3.25**) Добавяне на помощен адрес

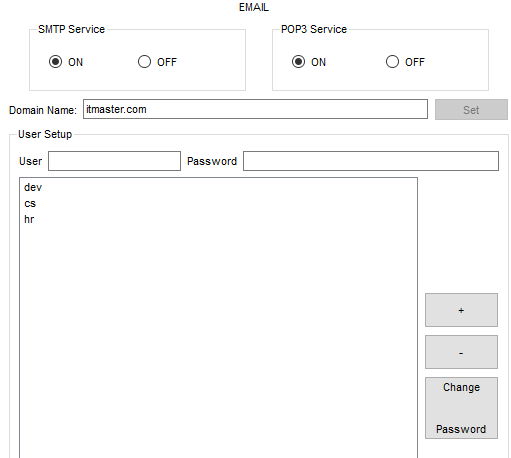
|  |
| --- |
| int vlan 10 ip helper-address 192.168.40.7 |

Тъй като имаме отделни подмрежи, ще бъде необходимо да настроим всяка една от тях за правилно функциониране.

### Email Server

Настройката на mail сървър е проста, но важна в една мрежа. Тя ще позволи комуникация между служителите във всеки отдел както и обявяване на новини и промени във фирмата. Чрез mail сървъра ние създаваме потребители и парола, които служителите могат да използват, за да изпращат съобщения към техните колеги. Настройката му става от следното поле:

(**Фигура 3.26**)Настройка на Email server

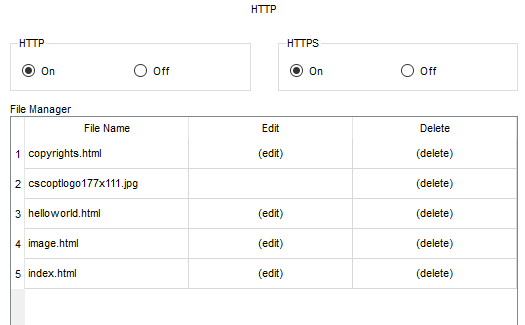


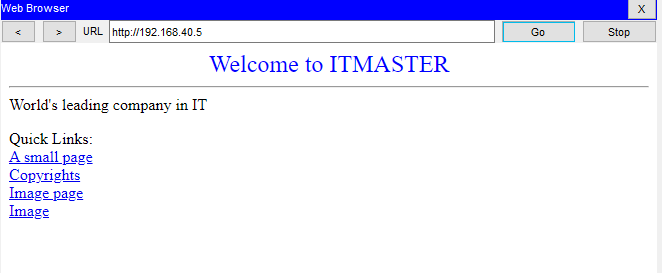
### WEB server

В зависимост от това какви услуга предлага една фирма, трябва да се направи решение дали те ще имат сайт. Ако бъде направено решението да се направи фирмен сайт тогава трябва да се има на предвид създаването на web server както и наемане на персонал за поддръжката му, или купуване на тази услуга от друга фирма, която я предлага.

Настройката на сървъра в нашата симулация е доста лесна. Използвайки графичния интерфейс на Cisco Packet Tracer. Методът е следния: избираме услугата http/https и след като я включим, добавяме файловете, които ще се заредят:

(**Фигура 3.27**) Настройка на уеб сървър



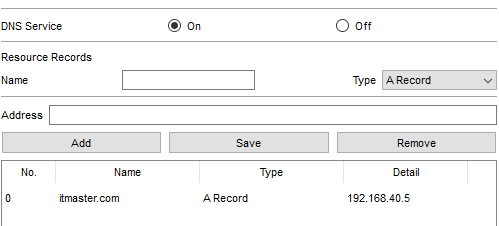
За да може се достъпи този сайт е нужно клиентите или служители да достъпят IP адреса на този сървър чрез техния браузър, както е показано на фигурата:  
  
(**Фигура 3.28**) Достъпване на уеб сайт  


В този случай обаче възниква един проблем. Тъй като никой не използва IP адреси за достъп до такъв сайт.

### DNS server

DNS ще ни е нужен,за да постави, домейн който съответства, за да може да се достъпва и запомня лесно. В симулационната среда, настройката на DNS сървъра става след като включим DNS услугата и изберем домейн, който да съответства на IP адреса ни.

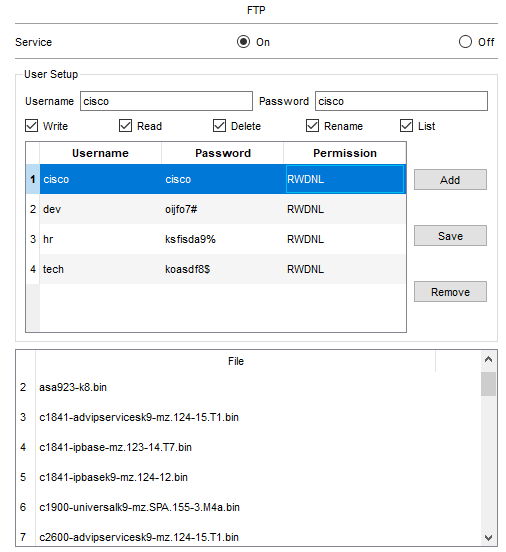
(**Фигура 3.29**) Настройка на DNS сървър



### FTP и TFTP сървър

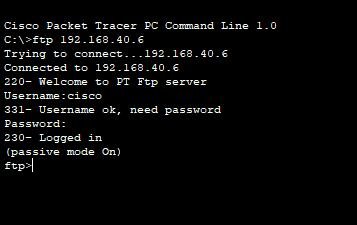
FTP сървъра е нужен за безпроблемно изпращане и запазване на файлове. Настройката му в симулационна среда става чрез създаване на потребители, които да могат да достъпят файловете на сървъра и определяне на техните права(read,write,list,delete,rename).

(**Фигура 3.30**)Настройка на FTP



След настройване на FTP сървъра, ние вече ще можем да го достъпим през всяко едно друго устройство използвайки терминала.

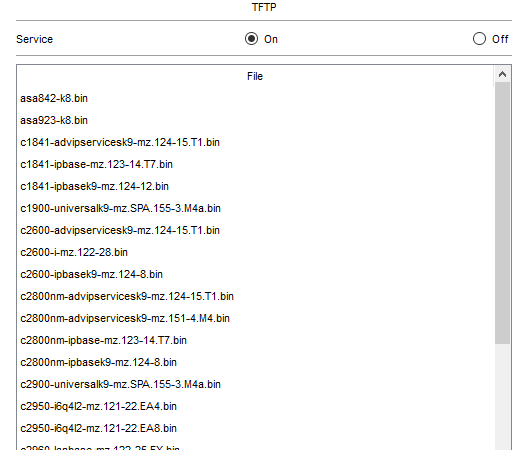
(**Фигура 3.31**)Пример за достъп до FTP сървър



На фигурата е показано как използваме командния интерфейс на един от компютрите, за да достъпим FTP сървъра, след което влизаме с единия от потребителите. Следващите действия, които можем да предприемем зависят от правата на потребителя с който сме влезли.

При TFTP сървъра не се използват име и парола, защото той главно се използва за съхранение и изпращане на конфигурационни файлове на мрежови устройства. В симулационната среда се настройва лесно чрез включване на услугата.

(**Фигура 3.32**) TFTP server



### Безжична мрежа

Във всеки един отдел е добавена точка за достъп, чрез която служителите могат да свързват техните безжични устройства - лаптопи, телефони и тн. Тъй като устройствата с директно свързани към комутаторите - те директно раздават IP адреси на безжичните устройства както Layer 2 комутаторите.

# Мерки за сигурност:

Мрежата ще прилага няколко мерки за сигурност, за да се предпази от неразрешен достъп и атаки. Някои от мерките включват:

Разделяне на VLAN: Всеки отдел ще бъде присвоен отделен VLAN, което ще гарантира, че трафикът е изолиран между отделите и етажите.

## Запомняне на MAC адреси

Комутаторите имат възможност да запомнят физическия адрес на устройствата свързани на всеки порт. По този начин ние можем да настроим всеки интерфейс да работи единствено ако от другата страна е устройство чийто физически адрес съответства на този запомнен от комутатора. Това става възможно със следните команди:

(**Фигура 4.10**) Port-security

|  |
| --- |
| switchport port-security switchport port-security maximum 1 switchport port-security mac-address sticky |

На фигурата по-горе е показано как на избрания интерфейс се настройва максимума на възможните адреси, който в случая е само един. По този начин ограничаваме интерфейсите на комутатора, за да няма възможност за свързване на друго устройство към мрежата. Следващата команда обозначава физическия адрес който ще отговаря на този интерфейс. За улеснение използваме командата sticky вместо да пишем самия адрес за всеки интерфейс. След като въведем тези команда - комутатора следи кое е следващото устройство от което получава сигнал на този интерфейс и запомня неговия физически адрес.

## Ненужни портове на комутаторите

Тъй като не всеки порт на комутаторите се използва, всеки, който има достъп до комутаторите ще има възможността да се свърже към свободните портове и да получи достъп до мрежата. По тази причина е добра идея да променим настройките на свободните портове.

Първо използваме L3 комутаторите, за да създадем нов VLAN 100, където ще изпращаме всеки свободен порт. След което влизаме във всеки L2 и L3 комутатор и настройваме всеки свободен порт да бъде в този vlan и да е в режим access. По този начин някой се свърже към този порт, той няма да може да комуникира нито с устройствата в същата мрежа, нито с тези извън нея. Ето как бяха настроени портовете не L3 комутаторите:

(**Фиугра 4.20**) Портове на L3 комутатор



# Възможности за разширение:

Мрежата е проектирана, за да може да се разширява при необходимост. Сървърната стая може да бъде разширена или да бъде добавен допълнителен сървър в зависимост от бизнес нуждите. Може да се добавят още L3 комутатори(основни и резервни) в случай на нужда от увеличаване на отделите. Още L2 комутатори биха били добър избор при увеличаване на персонала.

## IoT

В случай, че бъде нарпавено решение да се добяват допълнителни smart технологии, които подпомогнат работната обсатовка, имаме много опции:

### Противопожарна система:

В слуай на пожар, ще ни бъдат нужни сензор за дим и сирена. Сензори и сирени трябва да бъдат поставени във всеки отдел. При засичане на пожар, прозорците се отварят и всички сирени се активират. Тази симулация може да стане възможна в Cisco Packet Tracer.

(**Фигура 5.10**) Визуализация на противопожарна система

Diagram

Description automatically generated

### Система за наблюдение:

Може да бъде настроеа система за наблюядение във всички офиси. В Packet Tracer е възможно активирането на наблюдателните устройства при засичане на движение чрез сензор за движение.

(**Фигура 5.11**) Визуализация на наблюдателна система

Diagram

Description automatically generated

### Настойка:

За да се настроят тези технологии е нужен IoT сървър към който да се свъзват устройствата и да се правят уловия за работа

### Още възможности:

Възможни са много други устройства, които да подобрят работната обстановка в офиса и да увеличат сигурността, удобството и продуктивността на служителите като smart климатици, вентилатори и гаражни врати. Ето как изглеждат устройствата в един IoT сървър:

(**Фигура 5.12**) Визуализация на IoT сървър:

Graphical user interface, text, application, email

Description automatically generated

При нужда от увеличаване на скоростта е възможно настройване на Ether-Channel. Технологията позволявава свързване между 2 устройства с повече от един интерфейс и действието им като един общ. Настройката на този протокол ства по следния начин:

Първо ни е нужно да свържем двете устройства с еднакви кабели(протоколът няма да работи ако искаме да го настроим между 1 Гигабит и 1 Етернет порт). След това трябва да сложим интерфейсите в една channel група. Следващите стъпки ще зависят от това кой протокол бихме искали да изпозлваме. Имаме избор между LACP и PAgP. LACP може да се използва за всякакви устройства, докато PAgP е настроен единствено за Cisco устройства. Ето как биха изглеждали командите ако искаме да изпозваме PAgP.

(**Фигура 5.13**) Настройка на PAgP

|  |
| --- |
| int range g0/1-2  channel-group 1 mode desirable |

Важно е да се отбележи, че трябва се настрои един и същ протокол и на двете устройства, които ще се звързват с Ether-channel.

# Заключение:

Добре проектираната мрежа е от съществено значение за ефективното функциониране на бизнеса. Проектирането на мрежата трябва да включва мерки за сигурност, аварийно възстановяване и възможности за разширение.

Какво е необходимо да се вземе предвид при проектирането на мрежата:

При проектирането на мрежата трябва да се вземат предвид някои фактори, които да гарантират ефективността и сигурността на мрежата. Някои от тези фактори са:

Брой на служителите: Броят на служителите определя броя на устройствата, които ще се свързват към мрежата. Трябва да се осигури достатъчно капацитет за всички устройства.

Интернет доставчик: Наличието на два или повече интернет доставчика може да осигури по-голяма резервност на мрежата и да гарантира, че бизнесът ще продължи да функционира дори при проблеми с единия доставчик.

Сигурност: VLAN-ите могат да бъдат използвани за разделение на мрежата и за ограничаване на достъпа до определени устройства.

Аварийно възстановяване: HSRP може да бъде използван за аварийно възстановяване на мрежата в случай на отказ на основния L3 суич. Също така, да се осигурят бекъп устройства за всички критични компоненти на мрежата.

Възможности за разширение: Мрежата трябва да бъде проектирана със скалируемост в предвид. Трябва да се предоставят възможности за добавяне на допълнителни устройства и VLAN-и, ако е необходимо.

В заключение, успешното проектиране на мрежата може да доведе до значително повишаване на ефективността на бизнеса. Трябва да се има впредвид сигурността и възможностите за разширение при проектирането на мрежата. Използването на отделни VLAN-и за всеки отдел може да бъде полезно за ограничаване на достъпа до определени устройства в мрежата. Това ще помогне за подобряване на сигурността и ефективността на мрежата, като същевременно осигурява по-голяма гъвкавост и контрол върху мрежовите ресурси.Трябва да се вземат под внимание и други аспекти, като маршрутизация, мрежова скорост, брой на портовете на суичовете и брой на устройствата, които ще бъдат свързани към мрежата. Тези фактори могат да повлияят на производителността на мрежата и следователно трябва да бъдат взети впредвид при проектирането й.