***פרויקט תקשורת נתונים ואבטחת מידע***

***כיתה: ב 1***

***שמות ו ת"ז מגישים:***

***חטיב יזן : 207733585***

***זערורה סאלח : 211918461***

***נושה הפרויקט: חברת KSP***

***מספר סניפים: 2***

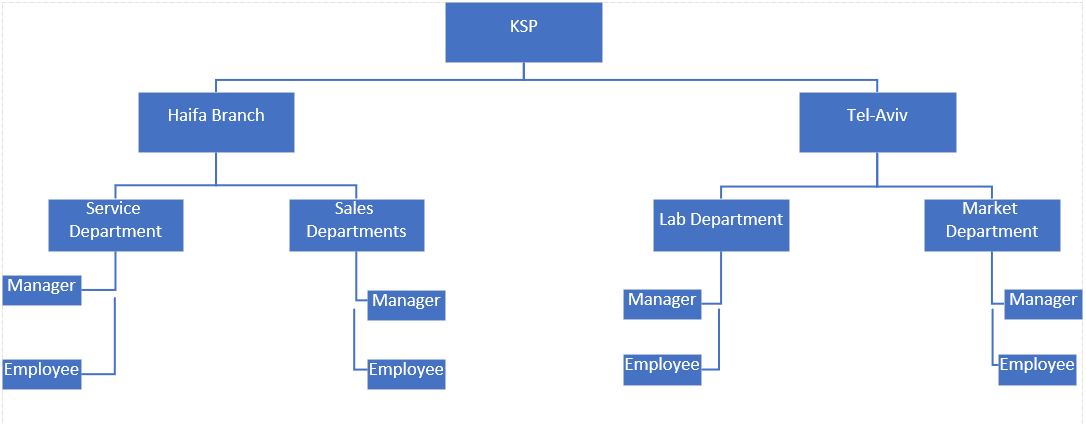
***ספר פרויקט :***

חברת למכירת מוצרי מחשבים (KSP )

הפרויקט הוא חברת למכירה מוצרי מחשבים שיש לה שני סניפים אחד בתל-אביב הוא אחראי על שירות לקוחות ועל ניהול חשבונות לחברה .והסניף השני שנמצה בחיפה והוא אחרי על מכירת מוצרים וגם יכיל מעבדה.  
ובכל סניף יש שתי מחלקות.  
  
  
1.הסניף הראשון הנמצא באזור תל-אביב מחולק לשתי מחלקות:  
-מחלקה של שירות לקוחות

-מחלקה לניהול חשבונות .

2.הסניף השני באזור צפון מחולק לשני מחלקות :  
-מחלקה למכירת מוצרים .  
-מחלקה מכילה מעבדה



סניף חיפה

בסניף חיפה יש לנו שתי מחלקות , מחלקת שירות ו מחלקת מכירות , וכל מחלקה יש לה מתג ו VLAN משלה מחובר ל ROUTER .

יש בסניף חיפה 3 שרתים :  
DHCP  
DNS  
MAIL

***שרת DHCP :***   
הוא שרת שמחלק כתובות למחלקות, השרת מחלק כתובות לעובדים ולכל רכיב חדש שמתחבר.

ה Vlan לכל אחד מהבריכות שונה.  
\*\* הבקודות בהמשך

|  |  |
| --- | --- |
| IP | Server |
| 192.168.1.2 | DHCP |

בשירת DHCP יש שתי בריכת כתובות, בריכה שמחלקת כתובות למחלקת עובדים, ובריכה שניה שמחלקת כתובות למחלקת שירות מנהלים.

הגדרת הבריכות בשרת DHCP:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VLAN | Max number of user | DNS | Starting IP | Default gateway | Pool name |
| 20 | 50 | 192.168.30.3 | 192.168.20.10 | 192.168.20.1 | Employees |
| 30 | 50 | 192.168.30.3 | 192.168.30.10 | 192.168.30.1 | Managers |

***שרת DNS:***  
 שמאפשר גישה לאתר שלנו דרך שם דומיין.  
 שם הדומיין: ksp.com  
כתובת ה DNS היא משותפת לכל סניף.

|  |  |
| --- | --- |
| IP | Server |
| 192.168.30.3 | DNS |

***שרת EMAIL :***  
הוא שרת שמאפשר שליחת מייל בין המחלקות ובין הסניפים , לפי ההגדרה בשרת :  
שם הדומיין   
שם משתמש ו סיסמה

|  |  |
| --- | --- |
| IP | Server |
| 192.168.30.30 | E-mail |

הגדרת משתמשים לשרת MAIL :

|  |  |  |
| --- | --- | --- |
| E-mail | Password | User |
| serviceman@ksp.com | 123 | serviceMan |
| serviceemp@ksp.com | 123 | serviceEmp |
| salesman@ksp.com | 123 | salesMan |
| salesemp@ksp.com | 123 | salesEmp |
| labman@ksp.com | 123 | labMan |
| labwor@ksp.com | 123 | labWor |
| marketman@ksp.com | 123 | marketMan |
| marketwor@ksp.com | 123 | marketWor |

***מחלקת עובדים:***

היא מחלקת שאחראית לטיפול בשירות לקוחות ויש בה מחשב מנהל , מדפסת מנהל ו מחשב עובד ו כל אחד כתובת ומקבל Vlan 20 .  
  
מחשב מנהל מקבל כתובת ip שלו כ Static .

מחשב עובד מקבל כתובת ip שלו כ Static .

מדפסת מקבלת כתובות דרך שרת DHCP .

כל רכיב נוסף מקבל כתובות דרך שרת DHCP .

|  |  |
| --- | --- |
| IP | Component |
| 192.168.20.10 | SalesEmployeePc | |
| 192.168.20.12 | ServiceEmployeePc | |
| DHCP | EmployeePrinter | |
| DHCP | Other component | |

***מחלקת מנהלים :***

היא מחלקת שאחראית על כל חשבונות ומכירות לחברה ויש בה שני מחשב מנהל ,ושני מדפסת מנהל כל אחד כתובת ומקבל Vlan 30 .  
  
מחשב מנהל מקבל כתובת ip שלו כ Static .

מחשב מנהל מקבל כתובת ip שלו כ Static .

מדפסת מקבלת כתובות דרך שרת DHCP .

כל רכיב נוסף מקבל כתובות דרך שרת DHCP .

|  |  |
| --- | --- |
| IP | Component |
| 192.168.30.10 | ManagerSalesPc | |
| 192.168.20.12 | ManagerServicePc | |
| DHCP | ManagerPrinter | |
| DHCP | Other component | |

***רכיבי IoT***

בסניף הזה יש שני רכיבי IoT, מכונת כפה ו קומקם.

שני הרכיבים מחוברים לנקודת גישה. שני הרכיבים מקבלים כתובות IP דרך שרת DHCP.

הרכיבים מחוברים לנקודת גישה ומתחברים דרך :  
SSID : IoT  
PSK PASS : 123456789

***חיבור בין שני הסניפים***

חיבור בין שני הסניפים נעשה דרך הרוטרים.

חיברנו את שני הראוטרים באמצעות פרוטוקול ניתוב RIP שעובד דרך צעדים, הוספנו את הרשתות שנמצאות בנסיף של כל אחד מהשותפים לראוטר משלו כדי שהראוטר יקיר אותם ותהיה לנו גישה לסניף השני

**שרת HTTP עשינו בסניף חיפה :**

|  |  |
| --- | --- |
| IP | Server |
| 192.168.1.80 | HTTP |
| http//ksp.com | Domain-Name |

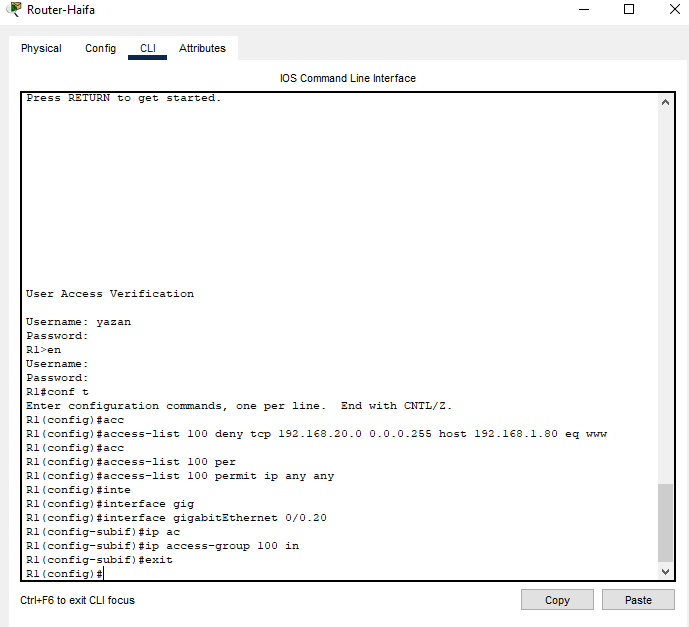
שרת AAA :

|  |  |
| --- | --- |
| IP | Server |
| 192.168.1.8 | AAA |

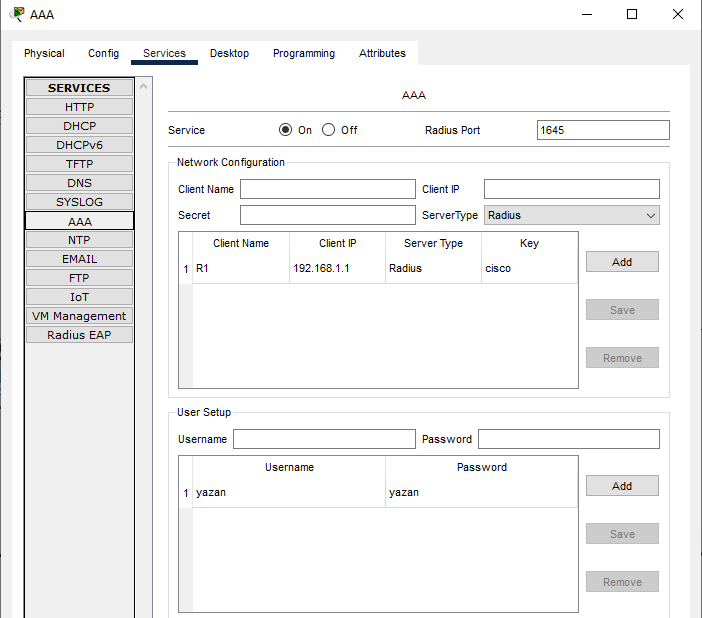
בשרת AAA ה TYPE שלו הוא ראדיוס ונוצר משתמש אחד לכל סניף   
\*\* הבקודות בהמשך

**לחסום את מחשבי העובדים (לא מנהלים) של אחד הסניפים לבחירתך את הגישה לתכני HTTP:**

החסימה נעשת למחלקת העובדים שעובד על VLAN 20 וכל מחשב חדש נוסף למחלקת העובדים לא תהיה גישה לשרת HTTP.



**לנהל את תהליך האימות בשרת AAA :**



Router(config)#hostname R1

R1(config)#username admin secret admin

R1(config)#enable password 123

R1(config)#aaa new-model

R1(config)#aaa authentication login default group radius local

R1(config)#aaa authentication enable default group radius local

R1(config)#radius-server host 192.168.1.8 key cisco

R1(config)#ip domain-name cisco.com

R1(config)#ip ssh version 2

Please create RSA keys (of at least 768 bits size) to enable SSH v2.

R1(config)#crypto key generate rsa

The name for the keys will be: R1.cisco.com

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#line vty 0 4

R1(config-line)#login authentication default

R1(config-line)#

R1(config-line)#end

מקורות

<https://www.youtube.com/watch?v=vjjx7E_NpvE&t=203s>

<https://www.youtube.com/watch?v=pAcWxanMNJQ>

<https://www.youtube.com/watch?v=bQ7qytz3oZw&t=65s>

<https://www.youtube.com/watch?v=bjgg0veyST8>

<https://www.youtube.com/watch?v=geTkZ3kfBe4>

**Routerהגדרת**

Router>EN

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#inter

Router(config)#interface gig

Router(config)#interface gigabitEthernet 3/0

Router(config-if)#no shutdown

Router(config-if)#interface gigabitEthernet 3/0.20

Router(config-subif)#encap

Router(config-subif)#encapsulation do

Router(config-subif)#encapsulation dot1Q 20

Router(config-subif)#ip address

Router(config-subif)#ip address 192.168.20.1 255.255.255.0

Router(config-subif)#ip helper-address 192.168.1.2

Router(config-subif)#ex

Router(config)#inter

Router(config)#interface gig

Router(config)#interface gigabitEthernet 3/0.30

Router(config-subif)#

%LINK-5-CHANGED: Interface GigabitEthernet3/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet3/0.30, changed state to up

Router(config-subif)#encap

Router(config-subif)#encapsulation

Router(config-subif)#encapsulation dot1Q 30

Router(config-subif)#ip address 192.168.30.1 255.255.255.0

Router(config-subif)#ip helper-

Router(config-subif)#ip helper-address 192.168.1.2

Router(config-subif)#ex

Router(config)

#

**הגדרת אבטלת Switch**

Switch>en

Switch#conf t

Switch(config)#enable secret 1999

Switch(config)#line console 0

Switch(config-line)#password 2222

Switch(config-line)#login

Switch(config-line)#exit

Switch(config)#line vty 0 4

Switch(config-line)#password 2222

Switch(config-line)#login

Switch(config-line)#exit

Switch(config)#serv

Switch(config)#service pass

Switch(config)#service password-encryption

Switch(config)#int

Switch(config)#interface fastEthernet 0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security

Switch(config-if)#switchport port-security mac-address sticky

Switch(config-if)#switchport port-security maximum 1

Switch(config-if)#ex

Switch(config)#ex

Switch#show running-config

**סניף תל אביב K.S.P**

**בסניף יש 2 מחלקות , מחלקה של מעבדות ומחלקה של קניות**

**בכל מחלקה יש 2 מחשבים מחשב של מנהל ומחשב לעובד וכל מנהל יש לו מדפסת .**

**לכל מחלקה יש מתג שישלו VLAN שמחובר ל ROUTER**

**יש שני שרתים בסניף :**

**שרת DHCP במחלקה של LAB**

הוא שרת שמחלק כתובות למחלקות, השרת מחלק כתובות למנהלים ולעובדים ולכל רכיב חדש שמתחבר. ה Vlan לכל אחד מהבריכות שונה, כלומר מחשב מנהל יש לו Vlan שונה מהמחשב של העובד וכך הלאה.

**שרת FTP במחלקה של MARKET**

זהו שרת שיכול להעביר קבצים ממחשב אחד למשנהו על ידי העלאתם לשרת FTP היכנס לשרת מהמחשב השני והורד את הקבצים הנדרשים

|  |  |
| --- | --- |
| **192.168.60.15** | **FTP** |
| **192.168.10.10** | **DHCP** |

הגדרת הבריכה:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Max number of users** | **DNS** | **Starting ip** | **Default gateway** | **Pool name** |
| 20 | 192.168.30.3 | 192.168.60.61 | 192.168.60.1 | **Vlan60** |
| 30 | 192.168.30.3 | 192.168.70.11 | 192.168.70.1 | **Vlan70** |
| 255 | 192.168.30.3 | 192.168.10.0 | 0.0.0.0 | **Serve pool** |

**כתובות המחשבים בסניף תל-אביב :**

**מחלקת מעבדות :**

**מעבדה היא מקום המספק תנאים מבוקרים וציוד המאפשרים מחקר, ניסויים ובדיקות.**

**מחלקה מוגדרת ב VLAN 60 ויש במחלקה**

**מחשב מנהל עם כתובת STATIC**

**מחשב עובד עם כתובת STATIC**

**מדפסת למנהל עם כתובת DHCP**

|  |  |
| --- | --- |
| **רכיב** | **IP** |
| **מחשב מנהל** | **192.168.60.60** |
| **מחשב עובד** | **192.168.70.10** |
| **מדפסת** | **DHCP** |

**מחלקת קניות :**

**תפקידה של מחלקת הקניות של KSP להביא לידי ביטוי יכולת קנייה מרוכזת ולנצל את יתרון הגודל של הארגון. המחלקה מופקדת על כל תחומי הרכש של KSP**

|  |  |
| --- | --- |
| **רכיב** | **IP** |
| **מחשב מנהל** | **192.168.60.62** |
| **מחשב עובד** | **192.168.70.11** |
| **מדפסת** | **DHCP** |

**רכיבי IoT:**

בסניף הזה יש שני

שני הרכיבים מחוברים לנקודת גישה. שני הרכיבים מקבלים כתובות IP דרך שרת DHCP.

הרכיבים מחוברים לנקודת גישה והגדרנו את שם הרשת בנקודת הגישה כ “saleh” והסיסמה כ 123456789

רכיבי IoT : מכונת כפה ו רַמקוֹל.

**Routerהגדרת**

Router>enable

Router#

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface GigabitEthernet0/0

Router(config-if)#exit

Router(config)#inter

Router(config)#interface gig

Router(config)#interface gigabitEthernet 0/0.60

Router(config-subif)#enc

Router(config-subif)#encapsulation dot

Router(config-subif)#encapsulation dot1Q 60

Router(config-subif)#ip add

Router(config-subif)#ip address 192.168.60.1 255.255.255.0

Router(config-subif)#ip help

Router(config-subif)#ip helper-address 192.168.10.10

Router(config-subif)#exit

Router(config)#inter

Router(config)#interface gig

Router(config)#interface gigabitEthernet 0/0.70

Router(config-subif)#enc

Router(config-subif)#encapsulation dot

Router(config-subif)#encapsulation dot1Q 70

Router(config-subif)#ip add

Router(config-subif)#ip address 192.168.70.1 255.255.255.

^

% Invalid input detected at '^' marker.

Router(config-subif)#ip address 192.168.70.1 255.255.255.0

Router(config-subif)#ip help

Router(config-subif)#ip helper-address 192.168.10.10

Router(config-subif)#no shutdown

Router(config-subif)#exit

Router(config)#

**הגדרות SWITCH**

PRINT>en

PRINT#conf t

PRINT#conf terminal

PRINT>en

PRINT#conf t

PRINT(config)#enable secret \*\*\*\*

PRINT(config)#line console 0

PRINT(config-line)#password \*\*\*\*

PRINT(config-line)#login

PRINT(config-line)#exit

PRINT(config)#line vty 0 4

PRINT(config-line)#password \*\*\*\*

PRINT(config-line)#login

PRINT(config-line)#exit

PRINT(config)#serv

PRINT(config)#service pass

PRINT(config)#service password-encryption

PRINT(config)#int

PRINT(config)#

PRINT(config)#int

PRINT(config)#interface f

PRINT(config)#interface fastEthernet 0/1

PRINT(config-if)#switch

PRINT(config-if)#switchport mode

PRINT(config-if)#switchport mode ac

PRINT(config-if)#switchport mode access

PRINT(config-if)#sw

PRINT(config-if)#switchport po

PRINT(config-if)#switchport port-security

PRINT(config-if)#sw

PRINT(config-if)#switchport po

PRINT(config-if)#switchport port-security mac

PRINT(config-if)#switchport port-security mac-address s

PRINT(config-if)#switchport port-security mac-address sticky

PRINT(config-if)#sw

PRINT(config-if)#switchport por

PRINT(config-if)#switchport port-security max

PRINT(config-if)#switchport port-security maximum 1

PRINT(config-if)#

PRINT(config-if)#exit

PRINT(config)#exit

**הגדרות VPN Graphical user interface, application, Word

Description automatically generated**  R2r>en

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2 (config)#license boot module c2900 ?

technology-package product technology group

R2 (config)#license boot module c2900 technology-packge security9

ACCEPT? [yes/no]: yes

R2#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

R2#reload

Proceed with reload? [confirm]

//////////////////////////////////////////////////////////////////////////////////////////////////////////////

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2 (config)#ip local pool PoolVPN 192.168.88.100 192.168.88.115

R2 (config)#aaa new-model

R2 (config)#aaa authentication login UserVPN local

R2 (config)#aaa authorization network GroupVPN local

R2 (config)#username uservpn secret ciscovpn

R2 (config)#crypto isakmp policy 100

R2 (config-isakmp)#encryption aes 256

R2 (config-isakmp)#hash sha

R2 (config-isakmp)#authentication pre-share

R2 (config-isakmp)#group 5

R2 (config-isakmp)#lifetime 3600

R2 (config-isakmp)#exit

R2 (config)#crypto isakmp client configuration group GroupVPN

R2 (config-isakmp-group)#key ciscogroupvpn

R2 (config-isakmp-group)#pool PoolVPN

R2 (config-isakmp-group)#exit

R2 (config)#crypto ipsec transform-set SetVPN esp-aes esp-sha-hmac

R2 (config)#crypto dynamic-map DynamicVPN 100

R2 (config-crypto-map)#set transform-set SetVPN

R2 (config-crypto-map)#reverse-route

R2 (config-crypto-map)#exit

R2 (config)#crypto map StaticMap client configuration address respond

R2 (config)#crypto map StaticMap client authentication list UserVPN

R2 (config)#crypto map StaticMap isakmp authorization list GroupVPN

R2 (config)#crypto map StaticMap 20 ipsec-isakmp dynamic DynamicVPN

R2 (config)#interface GigabitEtharnet 0/1

R2 (config-if)#crypto map StaticMap

\*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON

R2 (config-if)#

**הגדרות חסיםה של FTP**

Haifa router :

Graphical user interface, application

Description automatically generated

User Access Verification

Username: yazan

Password:

R1>en

Username:

Password:

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ac

R1(config)#access-list 110 per

R1(config)#access-list 110 permit u

R1(config)#access-list 110 permit udp a

R1(config)#access-list 110 permit udp any a

R1(config)#access-list 110 permit udp any any

R1(config)#ac

R1(config)#access-list 110 p

R1(config)#access-list 110 permit t

R1(config)#access-list 110 permit tcp a

R1(config)#access-list 110 permit tcp any h

R1(config)#access-list 110 permit tcp any host 192.168.30.30 eq pop3

R1(config)#ac

R1(config)#access-list 110 p

R1(config)#access-list 110 permit t

R1(config)#access-list 110 permit tcp a

R1(config)#access-list 110 permit tcp any h

R1(config)#access-list 110 permit tcp any host 192.168.1.80 eq www

R1(config)#ac

R1(config)#access-list 110 p

R1(config)#access-list 110 permit i

R1(config)#access-list 110 permit ic

R1(config)#access-list 110 permit icmp a

R1(config)#access-list 110 permit icmp any a

R1(config)#access-list 110 permit icmp any any

R1(config)#in

R1(config)#interface gig

R1(config)#interface gigabitEthernet 0/0.70

R1(config-subif)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0.70, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.70, changed state to up

R1(config-subif)#ip ac

R1(config-subif)#ip access-group 110 in

R1(config-subif)#exit

R1(config)#exit

R1#

%SYS-5-CONFIG\_I: Configured from console by console

Tel-aviv Router :

Graphical user interface, text

Description automatically generated

R1#

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#acc

R1(config)#access-list 110 pe

R1(config)#access-list 110 permit u

R1(config)#access-list 110 permit udp a

R1(config)#access-list 110 permit udp any a

R1(config)#access-list 110 permit udp any any

R1(config)#ac

R1(config)#access-list 110 d

R1(config)#access-list 110 deny t

R1(config)#access-list 110 deny tcp 192.168.20.0 0.0.0.255 h

R1(config)#access-list 110 deny tcp 192.168.20.0 0.0.0.255 host 192.168.6.11 eq ftp

R1(config)#ip acc

R1(config)#in

R1(config)#interface g

R1(config)#interface gigabitEthernet 3/0.20

R1(config-subif)#ip ac

R1(config-subif)#ip access-group 110 in

R1(config-subif)#exit

R1(config)#exit

R1#

%SYS-5-CONFIG\_I: Configured from console by console

R1#exit

[23:28]