ADHOC MOBILE WIRELESS NETWORK ENHANCEMENT BASED ON CISCO DEVICES

Mohamed E. Khedr, Mohamed S. Zaghloul and Mohamed I. El-Desouky

Department of Electronics and Communications, Arab Academy for Science, Tech. and Maritime Transport, Alexandria, Egypt, BOX 1029

ABSTRACT

Adhoc wireless networks become one of the most researchable areas in the studying of routing protocols depending on the Open System Interconnection (OSI Model). This paper use Cisco devices as a reference to enhance the performance of the network. This enhancement will be due to high processing, reliability, average cost, power consumption and accessibility. The aim of this research not only to get the cost down, it also to choose a time to time device to process the data as rapid as it can. Using NAT, Access List and DHCP protocols defined in Cisco (Graphical Unit Interface) GUI of the (Command Line Interface) CLI, the task can be made.

KEYWORDS

Adhoc, Wireless Networks, Cisco Access Points, Adhoc using Cisco devices.

1.INTRODUCTION

Cisco a leading networking company all over the world right now with the highest sales rates all over the world becomes the first premiere networks company in our time.[1] So, in this paper we will define, illustrate and configure some of routing protocols,(Domain Name Server) DNS, (Dynamic Host Configuration Protocol)DHCP and Access List (ACL) and (Network Address Translation) NAT that can be used during the communication ways with all data packets of sending and receiving processes. The usage of Cisco real routers and switches will give us an advance in high data processing. So, our goal can be targeted definitely is the “Time” of sending, receiving and acknowledgment due to the TCP/IP protocol called by 3 ways hand shake. In addition use to the encryption and the last step using (Wi-Fi Protected Access) WPA/WPA2 technologies. [2]

2.ILLUSTRATING THE PROBLEM

Our main goal is not to make the adhoc terminal only under the coverage area and always connected, but also with a very good communication timing during sending and receiving. Our main problem that there are no coordinators in the schema. this is not a huge problem but can be define it as advantage, that’s why all intermediate devices will be coordinators for the other end

DOI : 10.5121/ijcnc.2015.7107

devices and replication of the routing tables will be the major aid due to the geographical case of adhoc terminals movements, though its remains a problem due to adhoc well defined protocol.

High security is the second main goal, but as known wireless networking security is weak a bit, so this research will consider it step by step.

3.USED NETWORK'S DEVICES

Networks devices are needed in this paper to be selected due to certain specifications for outdoors, indoors and controllers.

1.Indoors (end points): Aironet 3700 Series (Power over Ethernet) (POE)

Fig.1. Aironet 3700 series

2.Outdoors (Coordinators): Aironet 1532E Series (Power over Ethernet) (POE)

Fig2. Aironet 1532E

3.Controllers (Routers): Catalyst 2800 series with 2 smart serial module, (2.4 and 5.0 GHz) wireless module and Sim card module

Fig.3. Cisco 2800 Series Catalyst Router

4.Fast Ethernet and smart serial cables to connect controllers with outdoors

4.ESTIMATED SCHEMA TO DEAL WITH

To illustrate the whole case issue, a simulation software is used called “Cisco packet Tracer V6.0.1”

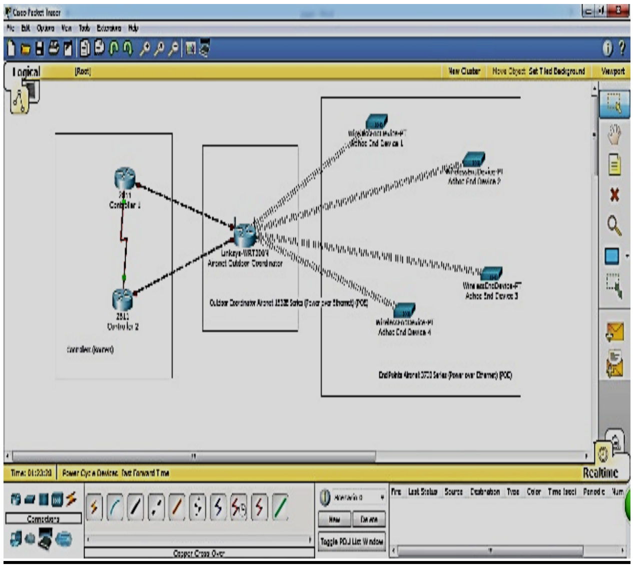


Fig4. Whole Schema using simulation Packet Tracer

This whole schema shows how this paper will operate over 3 layers

1- Core Layer (Controllers)
2- Outdoor Coordinator
3- End points

And now it’s the time to prepare the devices for configuration but there are some protocols and options that can be defined and considered.

5.NETWORK ADDRESS TRANSLATION (NAT):

To go to the Internet a public IP address must be available and it is unique all over the world. If each host in the world required a unique public IP address, IPs will be run over a few years. But by using Network Address Translation (NAT) huge number of IPs van be saved. So, NAT can be defined: “NAT allows a host that does not have a valid registered IP address to communicate with other hosts through the Internet”. For example a computer is assigned by private IP address of 10.0.0.9 and of course this address cannot be routed on the internet but you can still access the internet. This is because your router (or modem) translates this address into a public IP address, 123.12.23.1.For example, before routing your data into the internet [3].

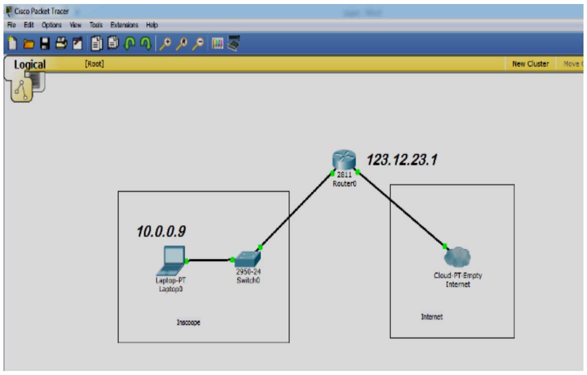


Fig5. NAT Illustration

Of course when a router receives a reply packet destined for 123.12.23.1 it will convert back to the private IP 10.0.0.9 before sending that packet to source.

Suppose an organization has 500 end points but the Internet Service Provider (ISP) only gives 50 public IP addresses. It means that the organization can only allow 50 hosts to access the internet at the same time. Here NAT comes to save this case!

One thing that should be noticed in real life, not all of end devices uses internet at the same time. Using NAT can dynamically assign these 50 public IP addresses to those who really need them at that time. This is called dynamic NAT.

But the above NAT solution does not solve the problem completely because in some days there can be more than 50 end points using the network. In this case, only the first 50 people can access internet, others must wait to their turns.

Another problem is, in fact, ISP only gives much lesser IP addresses than the number 50 because each public IP is very precious now. To solve the two problems above, another feature of NAT can be used: NAT Overload or sometimes called Port Address Translation(PAT) PAT permits multiple devices on a local area network (LAN) to be mapped to a single public IP address with different port numbers. Therefore, it’s also known as port address translation (PAT). When using PAT, the router maintains unique source port numbers on the inside global IP address to distinguish between translations. In the below example, each host is assigned to the same public which is IP address 123.1.1.1 1 but with different port numbers (from 1000 to 1002).

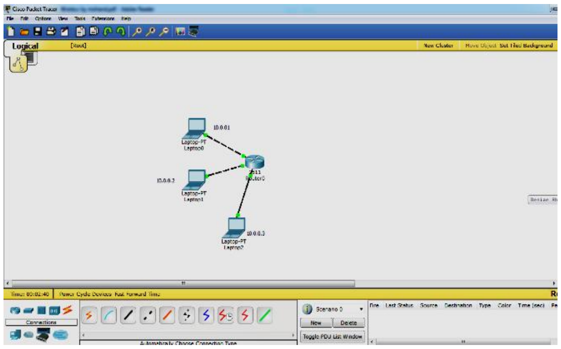


Fig6. PAT Example

Table1: PAT Table

Inside Local	Inside global
10.0.0.1	123.1.1.1:1000
10.0.0.2	123.1.1.1:1001
10.0.0.3	123.1.1.1:1003

Cisco uses the term inside local for the private IP addresses and inside global for the public IP addresses replaced by the router. The outside host IP address can also be changed with NAT. The outside global address represents the outside host with a public IP address that can be used for routing in the public Internet. NAT will be used while configuring the devices

6.ACCESS LIST CONTROL

Access control lists (ACLs) is equivalent to packets filtering by allowing the coordinator or the admin to permit or deny IP packets from specific end point of interface. To use ACLs, the system administrator must first configure ACLs and then apply them to specific interfaces. There are 3 popular types of ACL: Standard, Extended and Named ACLs [4].

And will be used to configure the devices.

7.IEEE 802.11 STANDARDS

At the time, there are 3 foundations effect on wireless LAN standards all over the world [5] and listed as bellow:

- ITU-R: is responsible for allocation of the RF bands
- IEEE: specifies how RF is modulated to transfer data

- Wi-Fi Alliance: improves the interoperability of wireless products among vendors but the most popular type of wireless LAN today is based on the IEEE 802.11 standard, which is known informally as Wi-Fi. Access points can support several or all of the three most popular IEEE

WLAN standards including 802.11a, 802.11b and 802.11g. WLAN has two basic modes of operation: Ad-hoc mode In this mode devices send data directly to each other and the Infrastructure mode and used to Connect to a wired LAN, supports two modes (service sets): Basic Service Set (BSS): uses only a single AP to create a WLAN and Extended Service Set (ESS): uses more than one AP to create a WLAN, allows roaming in a larger area than a single AP. [6]

8.ORTHOGONAL DIVISION MULTIPLEXING (OFDM)

The purpose is to encode a single transmission into multiple subcarriers to save bandwidth. OFDM selects channels that overlap but do not interfere with each other by selecting the frequencies of the subcarriers so that at each subcarrier frequency, all other subcarriers do not contribute to overall waveform. In the picture below, notice that only the peaks of each subcarrier carry data. [7] At the peak of each of the subcarriers, the other two subcarriers have zero amplitude.

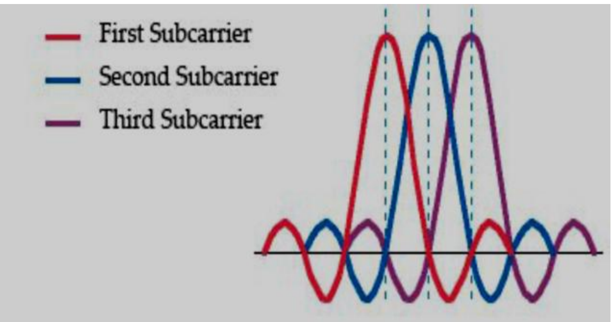


Fig7. OFDM Sub-carriers

9.DIRECT SEQUENCE SPREAD SPECTRUM (DSSS)

This method transmits the signal over a wider frequency band than required by multiplying the original user data with a pseudo random spreading code. The result is a wide-band signal which is very “durable” to noise. Even some bits in this signal are damaged during transmission; some statistical techniques can recover the original data without the need for retransmission. [8]

Note: Spread spectrum here means the bandwidth used to transfer data is much wider than the bandwidth needs to transfer that data. Traditional communication systems use narrowband signal to transfer data because the required bandwidth is minimum but the signal must have high power to cope with noise.[9] Spread Spectrum does the opposite way when transmitting the signal with much lower power level (can transmit below the noise level) but with much wider bandwidth. Even if the noise affects some parts of the signal, the receiver can easily recover the original data with some algorithms.

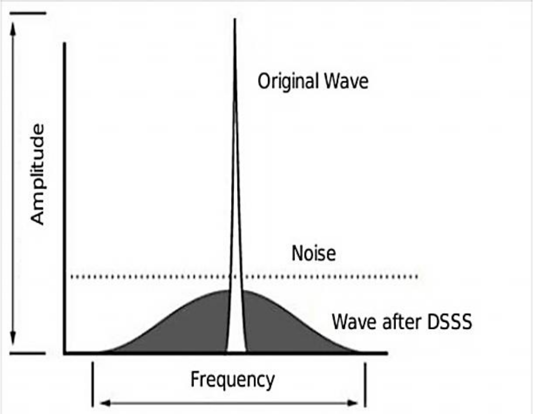


Fig8. DSSS wave form [10]

The 2.4 GHz band has a bandwidth of 82 MHz, with a range from 2.402 GHz to 2.483 GHz. In the USA, this band has 11 different overlapping DSSS channels while in some other countries it can have up to 14 channels. Channels 1, 6 and 11 have least interference with each other so they are preferred over other channels.

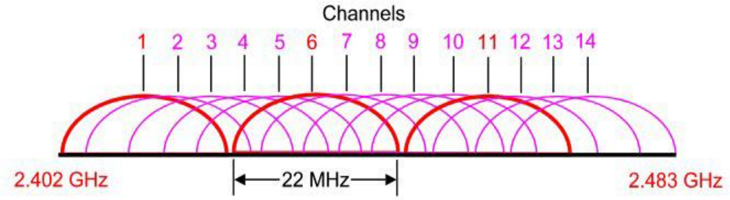


Fig.9. DSSS Channel Overlapping for Wi-Fi [11]

10.DEVICES CONFIGURATIONS

Table 2 devices and interfaces IPs

Device/interface	IP Address+ Subnet mask
Adhoc 1	15.15.15.15 255.0.0.0
Adhoc 2	15.15.15.16 255.0.0.0
Adhoc 3	15.15.15.17 255.0.0.0
Adhoc 4	15.15.15.18 255.0.0.0
Cont1:fa0/0	10.0.0.1 255.0.0.0
Cont:s0/3/0	12.0.0.1 255.0.0.0
Cont2:fa0/0	13.0.0.1 255.0.0.0
Cont2:s0/1/0	12.0.0.2 255.0.0.0

For Controller 1:

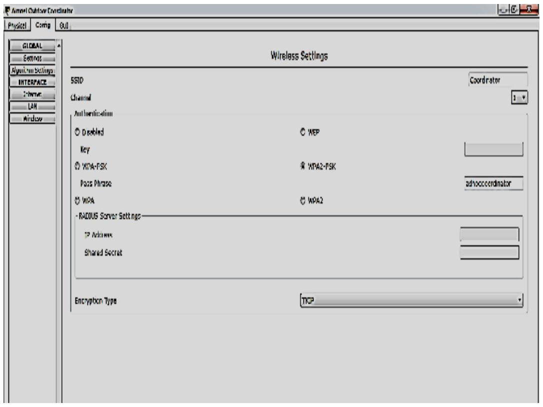
As shown in Appendix A

For Controller 2:

As shown in Appendix B

Coordinator (intermediate access point) Configuration

SSID (System Set Identifier): Coordinator
Key: adhocproject



Wireless Settings

SSID: Coordinator

Channel: 1

Authentication

○ Disabled ○ WEP

Key

○ WPA-PSK ● WPA2-PSK

Pass Phrase: adhoccoordinator

○ WPA ○ WPA2

RADIUS Server Settings

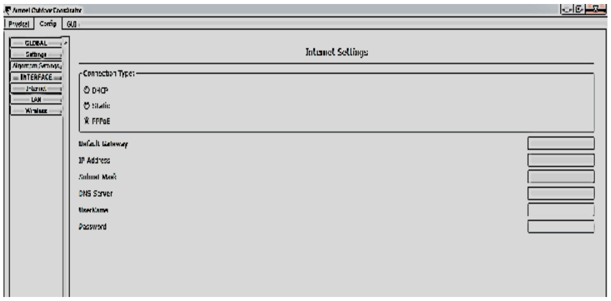
IP Address

Shared Secret

Encryption Type: TKIP

Fig.10. SSID and Pass Key

Connection Type: PPPOE (point to point over Ethernet)



Internet Settings

Connection Type:

○ DHCP

○ Static

● PPPoE

Default Gateway

IP Address

Subnet Mask

DNS Server

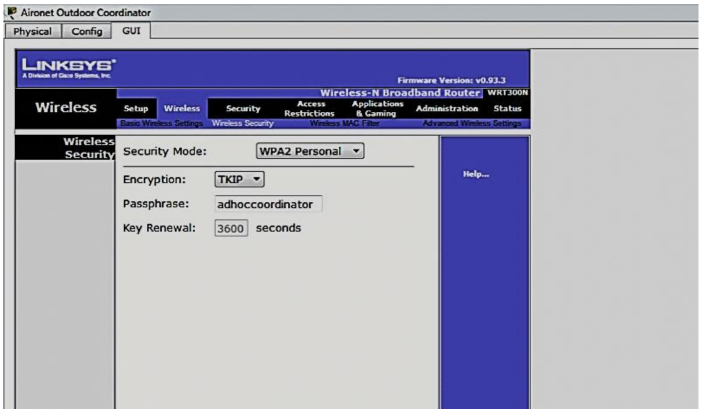
UserName

Password

Fig.11. PPPOE Connection Type

Wireless Security

SSID (System Set Identifier): Coordinator
Key: adhocproject



Security Mode: WPA2 Personal

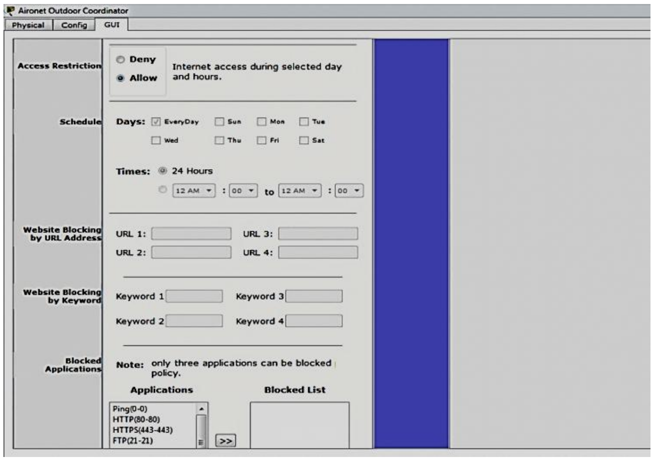
Encryption: TKIP

Passphrase: adhoccoordinator

Key Renewal: 3600 seconds

Fig.12. SSID and Pass Key after Connection

Access List Control (ACL)



Aironet Outdoor Coordinator

Physical | Config | GUI

Access Restriction: ○ Deny ● Allow Internet access during selected day and hours.

Schedule: Days: ☑ EveryDay □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Times: ● 24 Hours ○ 12 AM : 00 to 12 AM : 00

Website Blocking by URL Address: URL 1: URL 2: URL 3: URL 4:

Website Blocking by Keyword: Keyword 1 Keyword 2 Keyword 3 Keyword 4

Blocked Applications: Note: only three applications can be blocked policy.

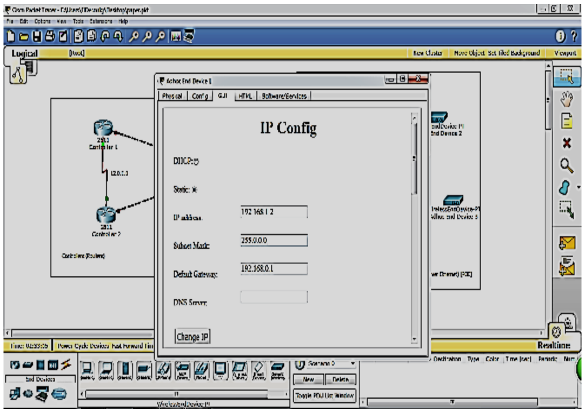
Applications: Ping(0-0) HTTP(80-80) HTTPS(443-443) FTP(21-21)

Blocked List

Fig.13. ACL Configuration

End Point Configuration

1st End Point IP Address 192.168.1.2
Subnet mask 255.255.255.0



Adhoc End Device 1

Physical | Config | GUI | HTML | Software/Services

IP Config

DHCP: ○

Static: ●

IP address: 192.168.1.2

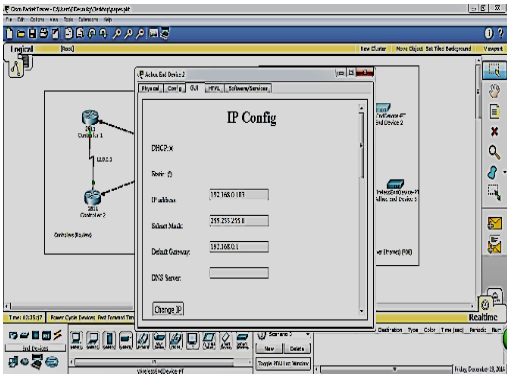
Subnet Mask: 255.0.0.0

Default Gateway: 192.168.0.1

DNS Server:

Fig.13. 1st Adhoc Endpoint

2nd End Point IP Address 192.168.1.103
Subnet mast 255.255.255.0



IP Config

DHCP: ●

Static: ○

IP address: 192.168.0.103

Subnet Mask: 255.255.255.0

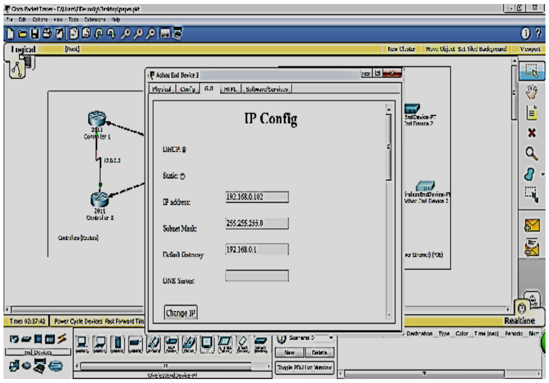
Default Gateway: 192.168.0.1

DNS Server:

Change IP

Fig.14. 2nd Adhoc End Point

3rd End Point IP Address 192.168.1.102
Subnet mast 255.255.255.0



IP Config

DHCP: ●

Static: ○

IP address: 192.168.0.102

Subnet Mask: 255.255.255.0

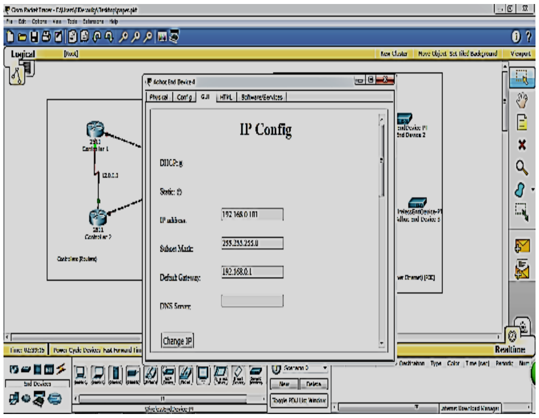
Default Gateway: 192.168.0.1

DNS Server:

Change IP

Fig.15. 3rd Adhoc End Point

4th End Point IP Address 192.168.1.102
Subnet mast 255.255.255.0



IP Config

DHCP: ●

Static: ○

IP address: 192.168.0.101

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

DNS Server:

Change IP

Fig.16. 4th Adhoc End Point

CONCLUSIONS

Adhoc wireless network can be especially applied in enterprise business compounds or military campuses. The desired design was limited into 3 stages (Core Layer, Intermediate Layer and the Endpoint Layer), in every layer a commands were placed to let the device work probably and use the right routing protocol (Static routing is used in this paper). So, the 3 layers can communicate with each other. In the other hand, the adhoc mobile end points don't need to route the sent message to the core layer, its waste of time by 66 msec. In our case it just sends the message to the coordinator and it has the lead to distribute the message to the destination end point.

References

[1] http://www.cisco.com/c/en/us/products/wireless/buyers-guide.html

[2] Sharam Hekmat, Communication Networks, 2011

[3] Robert Faludi, A Practical Guide to networking protocols, Building wireless networks, 2013

[4] Patric egilopacovic, Wireless networking, building AdHoc networks.802.11 a/b/g/n techniques, April 2011.

[5] Yi-Bing Lin & Imrich Chlamtac, Wireless and Mobile network architectures, 2012

[6] Andrew S. Tanenbaum, Computer Networks, Sixth Edition, 2013

[7] Simon Haykin, Communication Systems, fifth edition, 2014

[8] J. F. Kurose and W. R. Ross, Computer Networking: A Top-Down Approach Featuring the Internet, 2014

[9] Andrew S.Tanenbaum, Computer Network, 2012

[10] J. Walrand & P. Varaiya, High-Performance Communication Networks, 2014

[11] Wendell Odom,Cisco CCNA Exam# 200-120 Certification Guide, Cisco Systems, 2014

Appendix A

Controller (Routers) Configuration
For Controller 1:

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname Controller 1
Controller1(config)#interface fastEthernet 0/0
Controller1(config-if)#ip address 10.0.0.1 255.0.0.0
Controller1(config-if)#no shutdown
Controller1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Controller1(config-if)#ip address 11.0.0.1 255.0.0.0
Controller1(config-if)#no shutdown
Controller1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

Controller1(config)#interface serial 0/3/0
Controller1(config-if)#ip address 12.0.0.1 255.0.0.0
Controller1(config-if)#clock rate 64000
Controller1(config-if)#no shutdown
```

```
Controller1(config-if)#
%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up

Controller1(config)#line console 0
Controller1(config-line)#password adhoc1admin
Controller1(config-line)#login


Controller1(config)#line vty 0 4
Controller1(config-line)#password adhoc1admin
Controller1(config-line)#login


Controller1(config)#ip route 13.0.0.0 255.0.0.0   12.0.0.2
```

Appendix B

For Controller 2:

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname Controller2
Controller2(config)#interface fastEthernet 0/0
Controller2(config-if)#ip address 13.0.0.1 255.0.0.0
Controller2(config-if)#no shutdown
Controller2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Controller2(config)#interface fastEthernet 0/1
Controller2(config-if)#ip address 14.0.0.1 255.0.0.0
Controller2(config-if)#no shutdown
Controller2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

Controller2(config)#interface serial 0/1/0
Controller2(config-if)#ip address 12.0.0.2 255.0.0.0
Controller2(config-if)#no shutdown
Controller2(config-if)#
%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up

Controller2(config)#line console 0
Controller2(config-line)#password adhoc1admin
Controller2(config-line)#login

Controller2(config)#line vty 0 4
Controller2(config-line)#password adhoc1admin
Controller2(config-line)#login
Controller2(config)#ip route 10.0.0.0 255.0.0.0   12.0.0.1
```

Authors

Mohamed Khedr obtained his B.Sc. degree from the Arab Academy for Science and Technology, Alexandria, Egypt in 1997, the M.S. degree from same university in 2000, and the Ph.D. degree from Ottawa University, Ottawa, Canada in 2004, all in Electrical Engineering.From 1997 to 2000, He was a Graduate Teaching and research assistant at AAST, Alexandria, Egypt.From 2000 to 2004 He was a Graduate Teaching and research assistant at Ottawa University, Ottawa, Canada.From 2005 to 2009, he was an assistant Professor at AAST, Department of Electronic and communications Engineering, Alexandria, Egypt.Since January 2009, He has been an Associate professor at AAST, Department of Electronic and communications Engineering, Alexandria, Egypt.Since Fall 2005, has been an Adjunct Professor at Virginia Tech, USA

Mohamed S. Zaghloul was born in 1954 in Alex, Egypt, graduate as electrical engineer in 1977 has his master from Alexandria University in 1990 has his PhD in Surface Acoustic wave in 2002 he works as doctor at Arab academy for science and Technology in electronic and communication department

Mohamed I. El-Desouky was born in 1989 in Alex, Egypt, graduate as electrical, Electronics and Communications engineer from The Arab Academy for Science, Technology and Maritime Transport in 2010, has started preparation his master from the same institute of graduation in 2011.