How To Establish Ad-hoc Network Between 2 or More Systems

By : Reena Yadav
Hrishikesh Tak

Ad-hoc Network ?

- An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range.

How to create Ad-hoc Network

- **step 1 :** Root permission will required

- **step 2 :** edit the file /etc/network/interfaces with following commands on each system .

On Node A

- **step 3 :**
- auto wlan0
- iface wlan0 inet static
- address 192.168.1.1
- netmask 255.255.255.0
- wireless-channel 1
- wireless-essid MYNETWORK
- wireless-mode ad-hoc

On Node B

- **step 4 :**
- auto wlan0
- iface wlan0 inet static
- address 192.168.1.2
- netmask 255.255.255.0
- wireless-channel 1
- wireless-essid MYNETWORK
- wireless-mode ad-hoc

- **step 5 :** Save the file and exit the editor
- **step 6 :** Reboot your System
- Raise the interface on each node by using this command : **ifup wlan0**
- ifup - bring a network interface up
- wlan0 is your wifi card. wlan is wireless lan and 0 is the number of your card. The count starts from 0 and goes up

- Scan for ad-hoc cells in range by using this command : **iwlist wlan0 scan**
- iwlist - Get more detailed wireless information from a wireless interface
- scan - Give the list of Access Points and Ad-Hoc cells in range
- To test, ping node A from node B:
- **ping 192.168.1.1**

Network Interface ?

- A network interface is the point of interconnection between a computer and a private or public network.

Creation of OpenSSH Server & Client

- OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
- Make one system as SSH server & other as client

Steps to install OpenSSH sshd server

- **step 1 : sudo apt-get update**
- **step 2 : sudo apt-get install openssh-server**

  By default openssh will run on the TCP port 22. You can verify the same with the following command:

- **step 3 : netstat -tulpn | grep :22**

  netstat - Print network connections, routing tables, interface statistics

- **step 4 :** Type the following commands as root user:
- # service ssh stop
- # service ssh start
- # service ssh restart
- # service ssh status

  OR
- # /etc/init.d/ssh stop
- # /etc/init.d/ssh start
- # /etc/init.d/ssh restart
- # /etc/init.d/ssh status

Steps to install OpenSSH Client

- **step 1 : sudo apt-get install openssh-client**
- **step 2 :** Switch back to your normal user (not root, respectively). Then type these commands in order:

  mkdir ~/.ssh

  chmod 700 ~/.ssh

  cd ~/.ssh

- We generate our key-pair, a public-key and a private-key. The public-key will be placed on the server, and you will log in with your private-key. When asked, type your passphrase (it'll be needed for future logins, so remember it!):
- step 3 : ssh-keygen -t rsa -C "public_key... private_key..."

- Then we copy the public key (which we've generated just before) to our (remote) server. The remoteuser should not be root! Choose the default non-root user as remoteuser. (Note the colon at the end of the line! It's important.
- **scp -p id_rsa.pub remoteuser@remotehost:**
- scp — secure copy (remote file copy program)
- scp copies files between hosts on a network

- Then we log in with SSH, and we copy the public key to its right place:
- ssh remoteuser@remotehost
- mkdir ~/.ssh
- chmod 700 ~/.ssh
- cat id_rsa.pub >> ~/.ssh/authorized_keys
- chmod 600 ~/.ssh/authorized_keys
- mv id_rsa.pub ~/.ssh
- logout

- This is the Linux scp command syntax to send file or directory to a remote computer:

- **scp -r [/path/filename] [login name@ipaddress]:**

- This is the Linux scp command syntax to retrieve file or directory from a remote computer:
- **scp -r [login name@ip address] : [/path/filename]**

Thank You !!!