

Advanced Computer Network



ADVANCED COMPUTER NETWORK

22520

Practical Manual 2019-2020

Prepared By:-

**Mr.Palwe R.M.,
Lecturer in Computer Engineering,
M.M.Polytechnic, Thergaon**

Computer Engineering Program Vision

To develop technically proficient and competent professional's with latest technology and ethical values to serve society.

Computer Engineering Program Mission

- **To impart latest and sound technical education**
- **To provide strong theoretical and practical knowledge of computer engineering branch with an emphasis to maintain software and hardware systems.**
- **Groom students with necessary skills and ethical values.**

Program Educational Objectives (PEO's)

- **PEO1: To prepare students for successful careers in Industry that meet the needs of Indian and multinational companies.**
- **PEO2: To develop the ability among students to synthesize data and technical concepts for application to product design.**
 - **PEO3: To provide opportunity for students to work as part of teams on multidisciplinary projects.**
- **PEO4: To prepare diploma Students to pursue higher education and research**
- **PEO5: 5 To promote students for life-long learning and make them aware of professional ethics and codes of professional practice.**

COURSE OUTCOMES

CO1: Implement network layer protocol

CO2: Configure IPv6 network

CO3: Choose routing protocol in given network situation

CO4: Implement different transport layer protocols

CO5: Configure various application layer protocols

Maharashtra State Board of Technical Education, Mumbai**CERTIFICATE**

This is to certify that

Mr. /Ms _____

Roll-No. _____ of Fifth Semester of Diploma in **Computer Engineering** of **Marathwada Mitra Mandal's Polytechnic** has completed the lab satisfactorily in course **Advanced Computer Network(22520)** for the academic year 2019-20as prescribed in the curriculum.

Place _____

Enrollment No _____

Date _____

Exam Seat No _____

Course Coordinator
[Mr.Palwe R.M.]

HOD
[Mr.Solanke V.S.]

Principal
[Mrs.Joshi G.S.]



INDEX

Sr. No	Name of Experiment	Date of Performance	Date of Submission	Marks	Sign of Staff
1	From given data find subnet,broadcast,range,subnet bits				
2	Capture ICMPv4 packets generated by Utility programs				
3	Configure IPv6 network				
4	Configure static IP routing				
5	Configure RIP IP routing				
6	Configure OSPF IP routing				
7	Run different SCTP Commands				
8	Configure DHCP				
9	Configure DNS				
10	Configure FTP & HTTP				
11	Configure SMTP,POP3,IMAP				
12	Configure MIME,SNMP				
TOTAL					

Practical No.1

IPv4 Addressing and Sub netting

Given an IP address and network mask, determine other information about the IP address such as:

- Network address
- Network broadcast address
- Total number of host bits
- Number of hosts

Given: IP Address: - 70.12.100.132

Network Mask: -
255.255.255.192

To find: Network address:-**First address = (any address) AND (network mask)**
= 70.12.100.132 AND 255.255.255.192
= 70.12.100.128

Network broadcast address:-**Last address = (any address) OR [NOT (network mask)]**
= 70.12.100.132 OR 0.0.0.63
= 70.12.100.191

Total number of host bits: - $32-26 = 6$ bits

Number of hosts:- $N \square 2^{32-n}$ in which n is the prefix length and N is the number of addresses in the block.

$$= 2^6 = 64 \text{ hosts}$$

Q 1. Given an IP address, network mask, and subnetwork mask, determines other information about the IP address such as:

- The subnet address of this subnet
- The broadcast address of this subnet
- The range of host addresses for this subnet
- The maximum number of subnets for this subnet mask
- The number of hosts for each subnet
- The number of subnet bits
- The number of this

subnet Example:--

Consider class a ip address 10.0.0.0 the its default subnet mask is 255.0.0.0 which means we can represent it by

10.0.0.0/8 the “/” factor indicates the CIDR value

If we decide to block some of the bits to minimize no of host in any given subnet then that technique is called as variable length subnet masking (VLSM)

Let us see the example where we borrow some bits from host part and minimize the count to an extent and create small independent N/W's of big N/W .Or even we can say that we want 8 N/W out of 1 big n/w then we will observe following N/W created with their VLSM 255.224.0.0 and no of hosts per subnet $2^{21} = 2097152 - 2 = 2097150$

ID	Subnetwork	Broadcast	First Host	Last
Host 1	10.0.0.0	10.31.255.255	10.0.0.1	10.31.255.254
2	10.32.0.0	10.63.255.255	10.32.0.1	10.63.255.254
3	10.64.0.0	10.95.255.255	10.64.0.1	10.95.255.254
4	10.96.0.0	10.127.255.255	10.96.0.1	10.127.255.254
5	10.128.0.0	10.159.255.255	10.128.0.1	10.159.255.254
6	10.160.0.0	10.191.255.255	10.160.0.1	10.191.255.254
7	10.192.0.0	10.223.255.255	10.192.0.1	10.223.255.254
8	10.224.0.0	10.255.255.255	10.224.0.1	10.255.255.254

Practical No.2

USE OF PING AND TRACERT / TRACEROUTE AND ARP UTILITIES

Diagnostic commands help you detect TCP/IP networking problems. Some of the diagnostic commands are **arp**, **hostname**, **ipconfig**, **netstat**, **ping**, **route**, and **tracert**.

i) **arp**

This diagnostic command displays and modifies the IP-to-Ethernet or Token Ring physical address translation tables used by the Address Resolution Protocol (ARP).

Syntax

```
arp -a [inet_addr] [-N [if_addr]]
arp -dinet_addr [if_addr]
arp -sinet_addr ether_addr [if_addr]
```

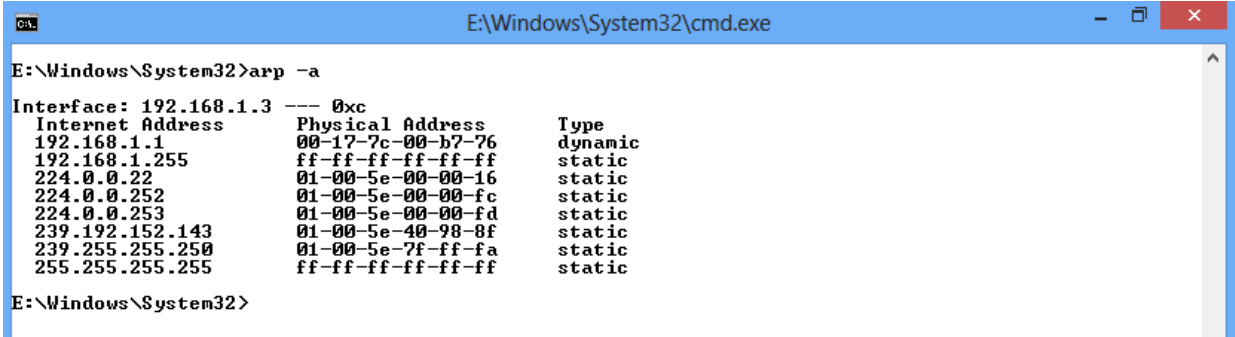
Parameters

-a Displays current ARP entries by querying TCP/IP. If *inet_addr* is specified, only the IP and physical addresses for the specified host are displayed.

-d Deletes the entry specified by *inet_addr*

-s Adds an entry in the ARP cache to associate the IP address *inet_addr* with the physical address *ether_addr*. The physical address is given as 6 hexadecimal bytes separated by hyphens. The IP address is specified using dotted decimal notation. The entry is static. It will not be automatically removed from the cache after the timeout expires and will not exist after a reboot of your computer.

-N [if_addr] Displays the ARP entries for the network interface specified by *if_addr*. *ether_addr* Specifies a physical address. *if_addr* Specifies, if present, the IP address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used. *inet_addr* Specifies an IP address in dotted decimal notation.



```
E:\Windows\System32\cmd.exe
E:\Windows\System32>arp -a
Interface: 192.168.1.3 --- 0xc
Internet Address      Physical Address      Type
192.168.1.1          00-17-7c-00-b7-76    dynamic
192.168.1.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.252          01-00-5e-00-00-fc    static
224.0.0.253          01-00-5e-00-00-fd    static
239.192.152.143      01-00-5e-40-98-8f    static
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static
E:\Windows\System32>
```

```

E:\Windows\System32>arp -a -v
Interface: 127.0.0.1 --- 0x1
  Internet Address      Physical Address      Type
  224.0.0.22            00-00-00-00-00-00    static
  224.0.0.252           00-00-00-00-00-00    static
  224.1.1.1             00-00-00-00-00-00    static
  239.192.152.143      00-00-00-00-00-00    static
  239.255.255.250      00-00-00-00-00-00    static
Interface: 192.168.1.3 --- 0xc
  Internet Address      Physical Address      Type
  192.168.1.1           00-17-7c-00-b7-76    dynamic
  192.168.1.2           00-00-00-00-00-00    invalid
  192.168.1.4           00-00-00-00-00-00    invalid
  192.168.1.7           00-00-00-00-00-00    invalid
  192.168.1.11          00-00-00-00-00-00    invalid
  192.168.1.32          00-00-00-00-00-00    invalid
  192.168.1.57          00-00-00-00-00-00    invalid
  192.168.1.64          00-00-00-00-00-00    invalid
  192.168.1.72          00-00-00-00-00-00    invalid
  192.168.1.100         00-00-00-00-00-00    invalid
  192.168.1.102         00-00-00-00-00-00    invalid
  192.168.1.113         00-00-00-00-00-00    invalid
  192.168.1.117         00-00-00-00-00-00    invalid
  192.168.1.134         00-00-00-00-00-00    invalid
  192.168.1.135         00-00-00-00-00-00    invalid
  192.168.1.255         ff-ff-ff-ff-ff-ff    static
  224.0.0.22            01-00-5e-00-00-16    static
  224.0.0.252           01-00-5e-00-00-fc    static
  224.0.0.253           01-00-5e-00-00-fd    static
  239.192.152.143      01-00-5e-40-98-8f    static
  239.255.255.250      01-00-5e-7f-ff-fa    static
  255.255.255.255      ff-ff-ff-ff-ff-ff    static
E:\Windows\System32>

```

ii) hostname

This diagnostic command prints the name of the host on which the command is used.

Syntax

hostname -- This command has no parameters.

iii) ipconfig

This diagnostic command displays all current TCP/IP network configuration values. This command is useful on computers running DHCP because it enables users to determine which TCP/IP configuration values have been configured by DHCP. If you enter only **ipconfig** without parameters, the response is a display of all of the current TCP/IP configuration values, including IP address, subnet mask, and default gateway.

Syntax

ipconfig [/all | /renew [*adapter*] | /release [*adapter*]]

Parameters

all Produces a full display. Without this switch, **ipconfig** displays only the IP address, subnet mask, and default gateway values for each network card.

renew [*adapter*] Renews DHCP configuration parameters. This option is available only on computers running the DHCP Client service. To specify an adapter name, type the adapter name that appears when you use **ipconfig** without parameters.

release [adapter] Releases the current DHCP configuration. This option disables TCP/IP on the local computer and is available only on DHCP clients. To specify an adapter name, type the adapter name that appears when you use **ipconfig** without parameters.

```
E:\Windows\System32\cmd.exe
E:\Windows\System32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::455b:8e0d:b47d:1e02%12
    IPv4 Address. . . . . : 192.168.1.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter isatap.{4ED9E15D-6856-4CB6-959E-9FB537F76402}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:0:9d38:90d7:38b7:1c6:c447:de85
    Link-local IPv6 Address . . . . . : fe80::38b7:1c6:c447:de85%14
    Default Gateway . . . . . : ::

E:\Windows\System32>
```

```
E:\Windows\System32\cmd.exe
E:\Windows\System32>ipconfig /release

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::455b:8e0d:b47d:1e02%12
    Default Gateway . . . . . : 

Tunnel adapter isatap.{4ED9E15D-6856-4CB6-959E-9FB537F76402}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:0:9d38:90d7:38b7:1c6:c447:de85
    Link-local IPv6 Address . . . . . : fe80::38b7:1c6:c447:de85%14
    Default Gateway . . . . . : ::

E:\Windows\System32>
```

```

E:\Windows\System32>ipconfig /renew
Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::455b:8e0d:b47d:1e02%12
    IPv4 Address. . . . . : 192.168.1.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter isatap.<4ED9E15D-6856-4CB6-959E-9FB537F76402>:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:0:9d38:6abd:188f:f81:c447:de85
    Link-local IPv6 Address . . . . . : fe80::188f:f81:c447:de85%14
    Default Gateway . . . . . : ::

E:\Windows\System32>

```

iv) **netstat**

This diagnostic command displays protocol statistics and current TCP/IP network connections.

Syntax

netstat [-a] [-e][-n][-s] [-p *protocol*] [-r] [*interval*]

Parameters

-a Displays all connections and listening ports; server connections are usually not shown. **-e** Displays Ethernet statistics. This can be combined with the **-s** option. **-n** Displays addresses and port numbers in numerical form (rather than attempting name lookups). **-s** Displays per-protocol statistics. By default, statistics are shown for TCP, UDP, ICMP, and IP; the **-p** option can be used to specify a subset of the default.

-p protocol Shows connections for the protocol specified.

-r Displays the contents of the routing table.

Interval Redisplays selected statistics, pausing *interval* seconds between each display.

```

C:\WINDOWS\system32\cmd.exe
C:\>netstat -a
Active Connections

Proto Local Address           Foreign Address         State
TCP   computer_1:snmp         computer_1:0           LISTENING
TCP   computer_1:http         computer_1:0           LISTENING
TCP   computer_1:epmap        computer_1:0           LISTENING
TCP   computer_1:https        computer_1:0           LISTENING
TCP   computer_1:microsoft-ds computer_1:0           LISTENING
TCP   computer_1:1035         computer_1:0           LISTENING
TCP   computer_1:1044         computer_1:0           LISTENING
TCP   computer_1:1118         computer_1:0           LISTENING
TCP   computer_1:2393         computer_1:0           LISTENING
TCP   computer_1:2394         computer_1:0           LISTENING
TCP   computer_1:2725         computer_1:0           LISTENING
TCP   computer_1:27657        computer_1:0           LISTENING
TCP   computer_1:1078         computer_1:0           LISTENING
TCP   computer_1:5152         computer_1:0           LISTENING
TCP   computer_1:10000        computer_1:0           LISTENING
TCP   computer_1:netbios-ssn  computer_1:0           LISTENING
TCP   computer_1:6405         130.117.190.216:https TIME_WAIT
TCP   computer_1:6408         130.117.190.216:https TIME_WAIT
TCP   computer_1:6410         38.113.165.80:https   TIME_WAIT
TCP   computer_1:6411         195.122.169.7:http    TIME_WAIT
TCP   computer_1:6413         38.113.165.80:https   TIME_WAIT
TCP   computer_1:6414         i154.IP-82.178.78.omante1.net.om:18964 SYN_SE

TCP   computer_1:6415         130.117.190.207:https TIME_WAIT
TCP   computer_1:6416         38.113.165.80:https   TIME_WAIT
TCP   computer_1:6417         94.75.236.122:http    TIME_WAIT
TCP   computer_1:6419         tracker.publicbt.com:http SYN_SENT
TCP   computer_1:6420         82.178.113.7:61015    SYN_SENT
UDP   computer_1:microsoft-ds *:*
UDP   computer_1:isatftp     *:*
UDP   computer_1:1025        *:*
UDP   computer_1:1136        *:*
UDP   computer_1:1137        *:*
UDP   computer_1:1142        *:*
UDP   computer_1:ms-sql-m    *:*
UDP   computer_1:3456        *:*
UDP   computer_1:4500        *:*
UDP   computer_1:6771        *:*
UDP   computer_1:27657       *:*
UDP   computer_1:ntp         *:*
UDP   computer_1:1041        *:*
UDP   computer_1:1900        *:*
UDP   computer_1:ntp         *:*
UDP   computer_1:netbios-ns *:*
UDP   computer_1:netbios-dgm *:*
UDP   computer_1:1079       *:*
UDP   computer_1:1900       *:*

```

```

C:\WINDOWS\system32\cmd.exe
C:\>netstat -e
Interface Statistics

Received Sent
Bytes 26520289 39481237
Unicast packets 62492 80110
Non-unicast packets 858 582
Discards 0 0
Errors 0 0
Unknown protocols 0 0

C:\>netstat -n
Active Connections

Proto Local Address           Foreign Address         State
TCP   192.168.1.2:6432        117.200.54.179:42596   ESTABLISHED
TCP   192.168.1.2:6443        117.254.37.99:44240   FIN_WAIT_1
TCP   192.168.1.2:6446        115.135.209.124:30441 LAST_ACK
TCP   192.168.1.2:6450        119.152.38.16:33423   ESTABLISHED
TCP   192.168.1.2:6455        130.117.190.207:443   TIME_WAIT
TCP   192.168.1.2:6456        119.154.182.5:48599   TIME_WAIT
TCP   192.168.1.2:6459        115.241.108.53:51574 TIME_WAIT
TCP   192.168.1.2:6460        111.92.29.227:51602   LAST_ACK
TCP   192.168.1.2:6463        122.167.70.201:49384 TIME_WAIT
TCP   192.168.1.2:6471        81.29.28.116:18168    TIME_WAIT
TCP   192.168.1.2:6478        38.113.165.80:443     TIME_WAIT
TCP   192.168.1.2:6479        130.117.190.207:443   TIME_WAIT
TCP   192.168.1.2:6480        59.161.60.52:10648    SYN_SENT
TCP   192.168.1.2:6481        59.99.32.102:30300    TIME_WAIT
TCP   192.168.1.2:6488        197.226.112.11:25786  SYN_SENT
TCP   192.168.1.2:6489        39.48.151.125:35684   TIME_WAIT
TCP   192.168.1.2:6491        130.117.190.207:443   TIME_WAIT
TCP   192.168.1.2:6492        27.107.10.22:26129    ESTABLISHED
TCP   192.168.1.2:6494        217.164.47.146:12971 SYN_SENT
TCP   192.168.1.2:6495        94.75.236.122:80      TIME_WAIT
TCP   192.168.1.2:6497        14.97.35.166:32802    ESTABLISHED
TCP   192.168.1.2:6498        14.98.55.11:45327     SYN_SENT
TCP   192.168.1.2:6499        14.99.16.6:48962      SYN_SENT
TCP   192.168.1.2:6500        180.234.95.68:59435   SYN_SENT
TCP   192.168.1.2:6501        223.176.222.63:48430 SYN_SENT

```

```

C:\WINDOWS\system32\cmd.exe
C:\>netstat -p
Active Connections
Proto Local Address          Foreign Address         State
C:\>netstat -R
Route Table
-----
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...00 0f b0 da c1 34 ..... Realtek RTL8139 Family PCI Fast Ethernet NIC -
Packet Scheduler Miniport
0x3 ...00 16 6f 0f 2d b5 ..... Intel(R) PRO/Wireless 2200BG Network Connectio
n Packet Scheduler Miniport
-----
Active Routes:
Network Destination     Netmask          Gateway          Interface        Metric
0.0.0.0                 0.0.0.0          192.168.1.1      192.168.1.2       20
127.0.0.0               255.0.0.0        127.0.0.1        127.0.0.1         1
192.168.1.0             255.255.255.0    192.168.1.2      192.168.1.2       20
192.168.1.2             255.255.255.255  127.0.0.1        127.0.0.1         20
192.168.1.255          255.255.255.255  192.168.1.2      192.168.1.2       20
224.0.0.0               240.0.0.0        192.168.1.2      192.168.1.2       20
255.255.255.255        255.255.255.255  192.168.1.2      192.168.1.2       1
255.255.255.255        255.255.255.255  192.168.1.2      192.168.1.2       1
Default Gateway:        192.168.1.1
-----
Persistent Routes:
None
C:\>_

```

v) ping

This diagnostic command verifies connections to one or more remote computers.

Syntax

```
ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s
count] [[-j host-list] | [-k host-list]] [-w timeout] destination-list
```

Parameters

-t Pings the specified host until interrupted.

-a Resolves addresses to host names.

-n count sends the number of ECHO packets specified by *count*. The default is 4.

-l length Sends ECHO packets containing the amount of data specified by *length*. The default is 64 bytes; the maximum is 8192.

-f Sends a Do Not Fragment flag in the packet. The packet will not be fragmented by gateways on the route.

-itl Sets the time to live field to the value specified by *ttl*.

-v tos Sets the type of service field to the value specified by *tos*.

-r count Records the route of the outgoing packet and the returning packet in the record route field. A minimum of 1 to a maximum of 9 hosts must be specified by *count*.

-s count Specifies the timestamp for the number of hops specified by *count*.

-j host-list Routes packets via the list of hosts specified by *host-list*. Consecutive hosts can be separated by intermediate gateways (loose source routed). The maximum number allowed by IP is 9.

-k host-list Routes packets via the list of hosts specified by *host-list*. Consecutive hosts cannot be separated by intermediate gateways (strict source routed). The maximum number allowed by IP is 9.

-w timeout Specifies a timeout interval in milliseconds.

destination-list Specifies the remote hosts to ping.

```
C:\WINDOWS\system32\cmd.exe - ping -t 192.168.1.2
C:\>ping -t 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
```

```
C:\WINDOWS\system32\cmd.exe
C:\>ping -a 192.168.1.2
Pinging computer_1 [192.168.1.2] with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping -n 6 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.2:
    Packets: Sent = 6, Received = 6, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping -l 3 192.168.1.2
Pinging 192.168.1.2 with 3 bytes of data:
Reply from 192.168.1.2: bytes=3 time<1ms TTL=128
Reply from 192.168.1.2: bytes=3 time<1ms TTL=128
Reply from 192.168.1.2: bytes=3 time<1ms TTL=128
Reply from 192.168.1.2: bytes=3 time<1ms TTL=128
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```

C:\WINDOWS\system32\cmd.exe
C:\>ping -f 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping -i 2 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping -i 2 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

```

E:\Windows\System32\cmd.exe
E:\Windows\System32>ping google.co.in
Pinging google.co.in [173.194.36.23] with 32 bytes of data:
Reply from 173.194.36.23: bytes=32 time=31ms TTL=58
Reply from 173.194.36.23: bytes=32 time=31ms TTL=58
Reply from 173.194.36.23: bytes=32 time=31ms TTL=58
Reply from 173.194.36.23: bytes=32 time=32ms TTL=58
Ping statistics for 173.194.36.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 32ms, Average = 31ms
E:\Windows\System32>_

```

vi) route

This diagnostic command manipulates network routing tables.

Syntax

route [-f] [*command* [*destination*] [**MASK** *netmask*] [*gateway*] [**METRIC** *metric*]]

Parameters

-f Clears the routing tables of all gateway entries. If this parameter is used in conjunction with one of the commands, the tables are cleared prior to running the command.

command Specifies one of four commands.

Command	Purpose
Print	Prints a route

Add	Adds a route
------------	--------------

Command	Purpose
Delete	Deletes a route
change	Modifies an existing route

destination Specifies the host to send *command*.

MASK Specifies, if present, that the next parameter be interpreted as the *netmask* parameter.

netmask Specifies, if present, the subnet mask value to be associated with this route entry. If not present, this parameter defaults to 255.255.255.255.

gateway Specifies the gateway.

METRIC Specifies the route metric (cost) for the destination.

```

C:\WINDOWS\system32\cmd.exe
C:\>route PRINT
=====
Interface List
-----
0x1 ...00 0f b0 da c1 34 ..... MS TCP Loopback interface
0x2 ...00 0f b0 da c1 34 ..... Realtek RTL8139 Family PCI Fast Ethernet NIC
0x3 ...00 16 6f 0f 2d b5 ..... Intel(R) PRO/Wireless 2200BG Network Connecti
- Packet Scheduler Miniport
=====
Active Routes:
-----
Network Destination        Netmask          Gateway          Interface        Metric
127.0.0.0                  255.0.0.0        127.0.0.1        127.0.0.1         1
192.168.1.0                255.255.255.0    192.168.1.2      192.168.1.2      20
192.168.1.2                255.255.255.255  127.0.0.1        127.0.0.1        20
192.168.1.255             255.255.255.255  192.168.1.2      192.168.1.2      20
224.0.0.0                 240.0.0.0        192.168.1.2      192.168.1.2      20
255.255.255.255           255.255.255.255  192.168.1.2      192.168.1.2      1
255.255.255.255           255.255.255.255  192.168.1.2      192.168.1.2      3
=====
Persistent Routes:
None

C:\>route PRINT 169*
=====
Interface List
-----
0x1 ...00 0f b0 da c1 34 ..... MS TCP Loopback interface
0x2 ...00 0f b0 da c1 34 ..... Realtek RTL8139 Family PCI Fast Ethernet NIC
0x3 ...00 16 6f 0f 2d b5 ..... Intel(R) PRO/Wireless 2200BG Network Connecti
- Packet Scheduler Miniport
=====
Active Routes:
None
Persistent Routes:
None

```

vii) tracert

This diagnostic utility determines the route taken to a destination by sending Internet Control Message Protocol (ICMP) echo packets with varying time-to-live (TTL) values to the destination. Each router along the path is required to decrement the TTL on a packet by at least 1 before forwarding it, so the TTL is effectively a hop count. When the TTL on a packet reaches 0, the router is supposed to send back an ICMP Time Exceeded message to the source computer.

Tracert determines the route by sending the first echo packet with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum TTL is

reached. The route is determined by examining the ICMP Time Exceeded messages sent back by intermediate routers. Notice that some routers silently drop packets with expired TTLs and will be invisible to **tracert**.

Syntax

```
tracert[-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name
```

Parameters

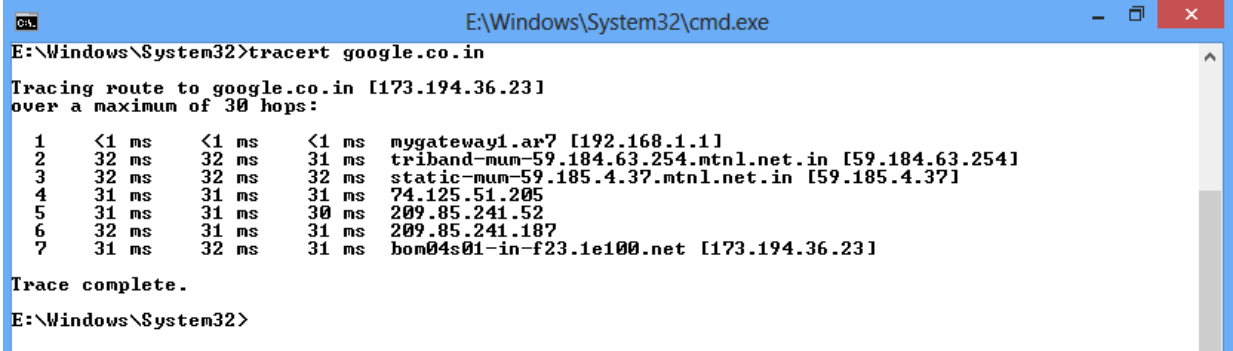
-d Specifies not to resolve addresses to host names.

-h *maximum_hops* Specifies maximum number of hops to search for target.

-j *host-list* Specifies loose source route along *host-list*.

-w *timeout* Waits the number of milliseconds specified by *timeout* for each reply.

target_name Name of the target host.



```
cmd E:\Windows\System32\cmd.exe
E:\Windows\System32>tracert google.co.in
Tracing route to google.co.in [173.194.36.23]
over a maximum of 30 hops:
  0  <1 ms    <1 ms    <1 ms    mygateway1.ar7 [192.168.1.1]
  1  32 ms    32 ms    31 ms    triband-mun-59.184.63.254.mtnl.net.in [59.184.63.254]
  2  32 ms    32 ms    32 ms    static-mun-59.185.4.37.mtnl.net.in [59.185.4.37]
  3  31 ms    31 ms    31 ms    74.125.51.205
  4  31 ms    31 ms    30 ms    209.85.241.52
  5  32 ms    31 ms    31 ms    209.85.241.187
  6  31 ms    32 ms    31 ms    bom04s01-in-f23.1e100.net [173.194.36.23]
Trace complete.
E:\Windows\System32>
```

Practical No.3

Configure IPv6

Cisco routers do not have IPv6 routing enabled by default. To configure IPv6 on a Cisco routers, you need to do two things:

1. enable IPv6 routing on a Cisco router using the *ipv6 unicast-routing* global configuration command. This command globally enables IPv6 and must be the first command executed on the router.
2. configure the IPv6 global unicast address on an interface using the *ipv6 address address/prefix-length [eui-64]* command. If you omit the *eui-64* parameter, you will need to configure the entire address manually. After you enter this command, the **link local address** will be automatically derived.

Here is an IPv6 configuration example:

```
R1(config)#ipv6 unicast-routing
R1(config)#int Gi0/0
R1(config-if)#ipv6 address 2001:0BB9:AABB:1234::/64 eui-64
```

We can verify that the IPv6 address has been configured by using the *show ipv6 interface Gi0/0* command:

```
R1#show ipv6 interface Gi0/0
GigabitEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::201:42FF:FE65:3E01
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:BB9:AABB:1234:201:42FF:FE65:3E01, subnet is 2001:BB9:AABB:1234::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF65:3E01
  MTU is 1500 bytes
  ....
```

From the output above we can verify two things:

1. the link local IPv6 address has been automatically configured. Link local IP addresses begin with FE80::/10 and the interface ID is used for the rest of the address. Because the MAC address of the interface is 00:01:42:65:3E01, the calculated address is **FE80::201:42FF:FE65:3E01**.
2. the global IPv6 address has been created using the [modified EUI-64 method](#). Remember that IPv6 global addresses begin with 2000::/3. So in our case, the IPv6 global address is **2001:BB9:AABB:1234:201:42FF:FE65:3E01**.

We will also create an IPv6 address on another router. This time we will enter the whole address:

```
R2(config-if)#ipv6 address 2001:0BB9:AABB:1234:1111:2222:3333:4444/64
```

Notice that the IPv6 address is in the same subnet as the one configured on R1 (**2001:0BB9:AABB:1234/64**). We can test the connectivity between the devices using *ping* for IPv6:

```
R1#ping ipv6 2001:0BB9:AABB:1234:1111:2222:3333:4444
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:0BB9:AABB:1234:1111:2222:3333:4444, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

As you can see from the output above, the devices can communicate with each other.

Practical No.4

Configure IP static routing

Static Route Configuration

Static Route

1. Static routing method is most trusted by a router.
2. Static routing is not really a routing protocol.
3. Static routes do not dynamically adapt to network changes, are not particularly scalable, and require manual updating to reflect changes.

Static routing has the following advantages

1. There is no bandwidth usage between routers, which means you could possibly save money on WAN links.
2. There is no overhead on the router CPU, which means you could possibly buy a cheaper router than you would use if you were using dynamic routing.
3. It adds security because the administrator can choose to allow routing access to certain networks only.

Static routing has the following disadvantages

1. Static routes don't dynamically adapt to network change.
2. If a network is added to the internetwork, the administrator has to add a route to it on all routers—by hand.
3. It's not feasible in large networks because maintaining it would be a full-time job in itself.
4. With static routing, as your network grows, it can be difficult just keep adding static routes makes sure everybody can still get everything.
5. The administrator must really understand the internetwork and how each router is connected in order to configure routes correctly.

There are two different styles to configure an "ip route" command:

1. Using a next hop IP address
2. Using an outgoing interface

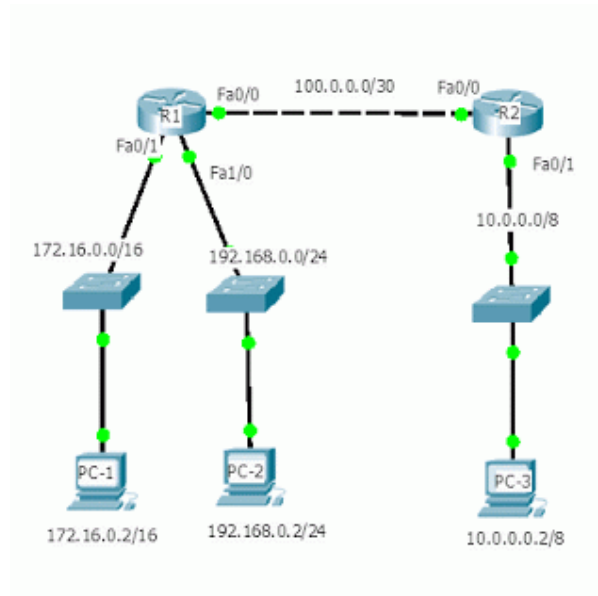
Static Route Lab with Packet Tracer Tutorial

Static Route Lab with Packet Tracer

Configure **Static Route** on Cisco Routers with following information:

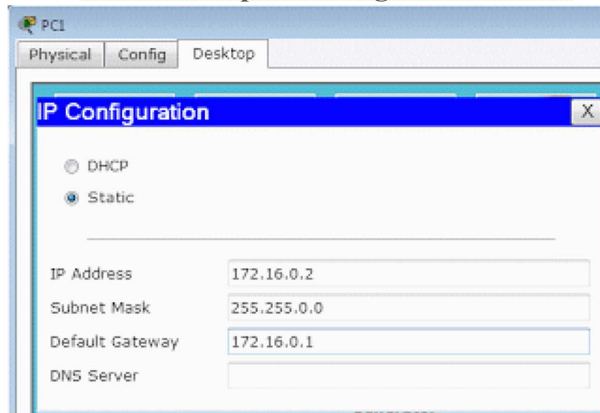
Network: 172.16.0.0/16, 192.168.0.0/24, 10.0.0.0/8

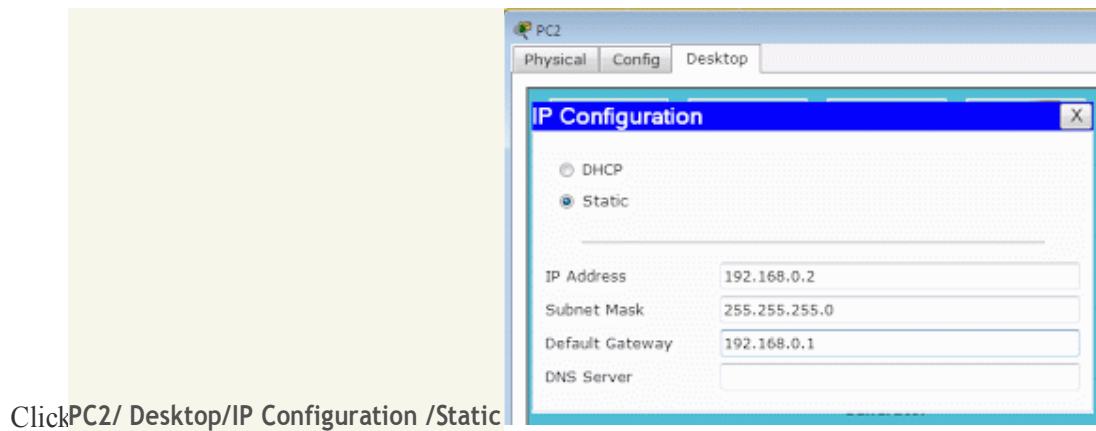
Gateway Address: 172.16.0.1/16, 192.168.0.1/24, 10.0.0.1/8



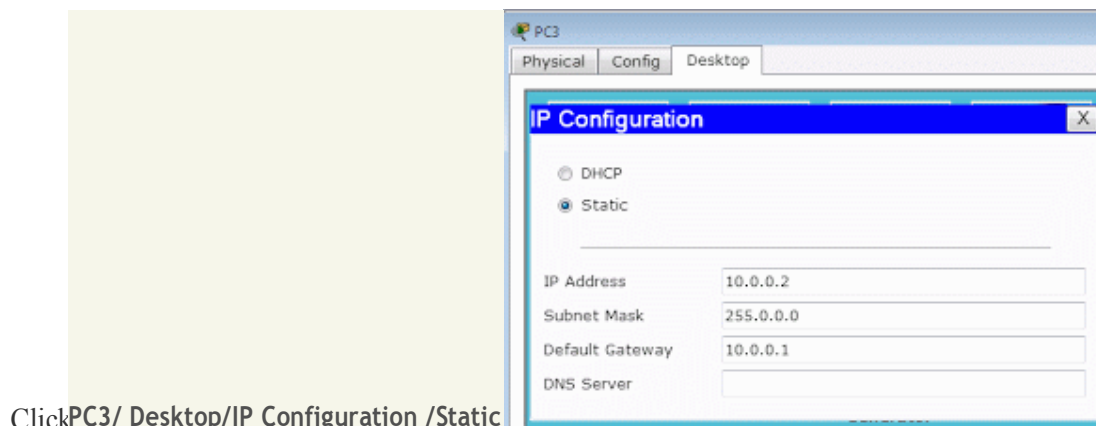
Putting three IP addresses, subnet mask and default gateway to three PCs.

Click **PC1/ Desktop/IP Configuration /Static**





Click PC2/ Desktop/IP Configuration /Static



Click PC3/ Desktop/IP Configuration /Static

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R1
R1(config)#int fa 0/1
R1(config-if)#ip address 172.16.0.1 255.255.0.0
R1(config-if)#no shut
R1(config-if)#int fa 1/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shut
R1(config)#int fa 0/0
R1(config-if)#ip address 100.0.0.1 255.255.255.252
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#

```

Configure Router R1

Configure Router R2

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R2
R2(config)#int fa 0/0
R2(config-if)#ip address 100.0.0.2 255.255.255.252
R2(config-if)#no shut
R2(config)#int fa 0/1
R2(config-if)#ip address 10.0.0.1 255.0.0.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#
```

Configure **Static Route** to router R1

Go to config mode, type **ip route** command, the subnet number, followed by the mask, and next hop ip address.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 10.0.0.0 255.0.0.0 100.0.0.2
R1(config)#^Z
```

See routing table of router R1

```
R1#show ip route

Gateway of last resort is not set

S 10.0.0.0/8 [1/0] via 100.0.0.2
   100.0.0.0/30 is subnetted, 1 subnets
C   100.0.0.0 is directly connected, FastEthernet0/0
C 172.16.0.0/16 is directly connected, FastEthernet0/1
C 192.168.0.0/24 is directly connected, FastEthernet1/0
R1#
```

Note a **static route** added to the routing table. The character **S** means **static route**. It references **10.0.0.0 subnet** and it says to get there via **100.0.0.2**. via means that the next hop router's IP address.

Now check IP connectivity

Click PC-1/ **Desktop/Command Prompt**

```
PC>ping 10.0.0.2
```

```
Pinging 10.0.0.2 with 32 bytes of data:
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Ping statistics for 10.0.0.2:
```

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
PC>
```

However PC-1 can't ping PC-3 right now, the ping fails.

See routing table of router R2

```
R2#show ip route
```

```
Gateway of last resort is not set
```

```
C 10.0.0.0/8 is directly connected, FastEthernet0/1
```

```
  100.0.0.0/30 is subnetted, 1 subnets
```

```
C   100.0.0.0 is directly connected, FastEthernet0/0
```

```
R2#
```

The output confirms that R2 does not have route to reach subnet 172.16.0.2/16, 192.168.0.2/24 or PC-1, PC-2. As a result, if PC-1 tries to ping PC-3 or PC-3 tries to ping PC-1 right now, the ping will fail.

So, we have to add a routing protocol (in this case, static route) that points PC-3's subnet namely 10.0.0.0/8.

In this way we will tell R1 how to forward packet to 10.0.0.0/8 subnet.

The packet arrives at R2, R2 has a directly connected route PC-3's subnet.

Configure **Static Route** to router R2


```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 172.16.0.0 255.255.0.0 100.0.0.1
R2(config)#ip route 192.168.0.0 255.255.255.0 100.0.0.1
R2(config)#^Z
R2#
```

Now, see routing table of router R2

```
R2#show ip route

Gateway of last resort is not set

C 10.0.0.0/8 is directly connected, FastEthernet0/1
100.0.0.0/30 is subnetted, 1 subnets
C 100.0.0.0 is directly connected, FastEthernet0/0
S 172.16.0.0/16 [1/0] via 100.0.0.1
S 192.168.0.0/24 [1/0] via 100.0.0.1
R2#
```

Now check IP connectivity

Click PC-1/ **Desktop/Command Prompt**

```
PC>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=12ms TTL=126
Reply from 10.0.0.2: bytes=32 time=13ms TTL=126
Reply from 10.0.0.2: bytes=32 time=12ms TTL=126
Reply from 10.0.0.2: bytes=32 time=20ms TTL=126

Ping statistics for 10.0.0.2:
    Packets: Sent=4, Received=4, Lost=0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 20ms, Average = 14ms

PC>
```

We can reach 10.0.0.0 network.

Click PC-2/ **Desktop/Command Prompt**

```
PC>ping 10.0.0.2
```

```
Pinging 10.0.0.2 with 32 bytes of data:
```

```
Reply from 10.0.0.2: bytes=32 time=12ms  
TTL=126 Reply from 10.0.0.2: bytes=32  
time=14ms TTL=126 Reply from 10.0.0.2:  
bytes=32 time=24ms TTL=126 Reply from  
10.0.0.2: bytes=32 time=11ms TTL=126
```

```
Ping statistics for 10.0.0.2:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 11ms, Maximum = 24ms, Average = 15ms
```

```
PC>
```

We can reach 10.0.0.0 network.

Click PC-3/ **Desktop/Command Prompt**

```
PC>ping 172.16.0.2
```

```
Pinging 172.16.0.2 with 32 bytes of data:
```

```
Reply from 172.16.0.2: bytes=32 time=10ms  
TTL=126 Reply from 172.16.0.2: bytes=32  
time=11ms TTL=126 Reply from 172.16.0.2:  
bytes=32 time=12ms TTL=126 Reply from  
172.16.0.2: bytes=32 time=16ms TTL=126
```

```
Ping statistics for 172.16.0.2:
```

```
Packets: Sent=4, Received=4, Lost=0(0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 10ms, Maximum = 16ms, Average = 12ms
```

```
PC>
```

We can reach 172.16.0.0 network.

```
PC>ping 192.168.0.2
```

```
Pinging 192.168.0.2 with 32 bytes of data:
```

```
Reply from 192.168.0.2: bytes=32 time=12ms TTL=126
```

```
Reply from 192.168.0.2: bytes=32 time=11ms TTL=126
```

```
Reply from 192.168.0.2: bytes=32 time=22ms TTL=126
```

```
Reply from 192.168.0.2: bytes=32 time=10ms TTL=126
```

```
Ping statistics for 192.168.0.2:
```

```
    Packets: Sent=4, Received=4, Lost=0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 10ms, Maximum = 22ms, Average = 13ms
```

```
PC>
```

We can reach 192.168.0.0 network.

Practical No.5

Configure IP routing using RIP

Routing Information Protocol - RIP

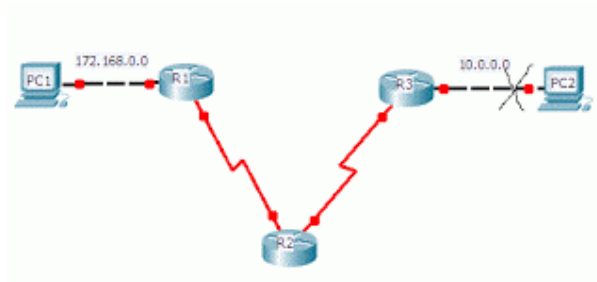
There are two versions of RIP: RIPv1 and RIPv2.

Comparing between RIPv1 and RIPv2

1. Both RIPv1 and RIPv2 have the **Administrative distance** 120.
2. Both RIPv1 and RIPv2 are distance vector routing protocol.

Both RIPv1 and RIPv2's metric is hop count.

Maximum hop count = 15. Max routers = 16.



For example, all routers are running RIP and network 10.0.0.0 goes down.

After hold timer expires, that network will be advertised by metric 16 and everyone will know that the network is down and that network will be seen in routing table as possibly down.

4. Both RIPv1 and RIPv2 send routing updates or complete routing table or broadcast every 30 seconds. i.e. The default routing update period for both version of RIP is 30 seconds. i.e. Both have the same timers.
5. Both RIPv1 and RIPv2 use split horizon to prevent routing loops.
6. Both RIPv1 and RIPv2 are configured with **router rip**.
7. **network** command tells both RIPv1 and RIPv2 to send hellos, out an interface, to find neighbors and to advertise routes.

```
R1(config-router)#network ?
A.B.C.D Network number
R1(config-router)#network 172.16.0.0 ?
<cr>
```

```
R1(config-router)#^Z
R1#
```

8. Both RIPv1 and RIPv2 are verified with **show ip protocols**.

```
Router#show ip protocols
R 10.0.0.10[120/3] via 20.0.0.7, 00:00:15, Serial0/0
```

The first number in the brackets is the administrative distance of the information source.

The second number is the metric for the route.

In this case, the administrative distance is 120, default AD for RIP routes, and the 3 represents the metric, which is the number of router hops in RIP.

Difference

1. RIPv1 used broadcast. RIPv2 used multicast(224.0.0.9).
2. RIPv1 is a **classful**. (**Classful**: all subnet mask must be the same in the network.) RIPv2 is a classless.
3. RIPv1 does not support VLSM. RIPv2 supports VLSM. **subnet mask field** was added to the RIPv2 message header by RFC 1723 to add support for VLSM and CIDR.
4. RIPv1 does not allow authentication. RIPv2 allows MD5 authentication
5. RIP enabled interfaces **send** version 1(RIPv1) updates. Do not send version 2(RIPv2) updates. RIP enabled interfaces **receive** any version(RIPv1 and RIPv2).
6. RIPv2 sends the subnet mask in updates and RIPv1 does not. i.e. Subnet mask information is included in RIPv2 routing updates that is not included in RIPv1.

Advantage of RIPv2 over RIPv1

1. RIPv2 supports MD5 authentication for routing updates. i.e. RIP version 2 supports routing update authentication.
2. RIPv2 used multicast(224.0.0.9) rather than broadcast.
3. RIPv2 auto summarize advertised routes across classful boundaries.
To disable this behavior, should apply **no auto-summary** command under the RIP process.

4. RIPv2 is **classless** routing protocol means that it sends subnet mask information when updates. By sending the subnet mask information with the updates, RIPv2 can support Variable Length Subnet Mask (VLSMs) as well as the summarization of network boundaries.

Disadvantage of RIPv1 and RIPv2

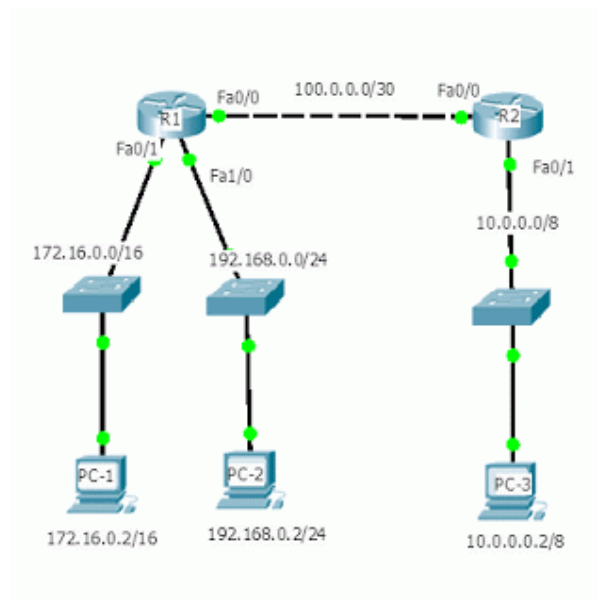
1. Both RIPv1 and RIPv2 send full routing tables out every 30 seconds. It's a lot of overhead, require too much bandwidth. Sending full routing table is unnecessary.
2. RIPv1 and RIPv2 does not form adjacency.
3. RIPv1 and RIPv2 work only on hop count(not consider the bandwidth).
4. RIPv1 and RIPv2 have slow convergence.
5. Not scalable, because hop count is only 15.

RIPv1 Lab with Packet Tracer Tutorial

RIPv1 Lab with Packet Tracer

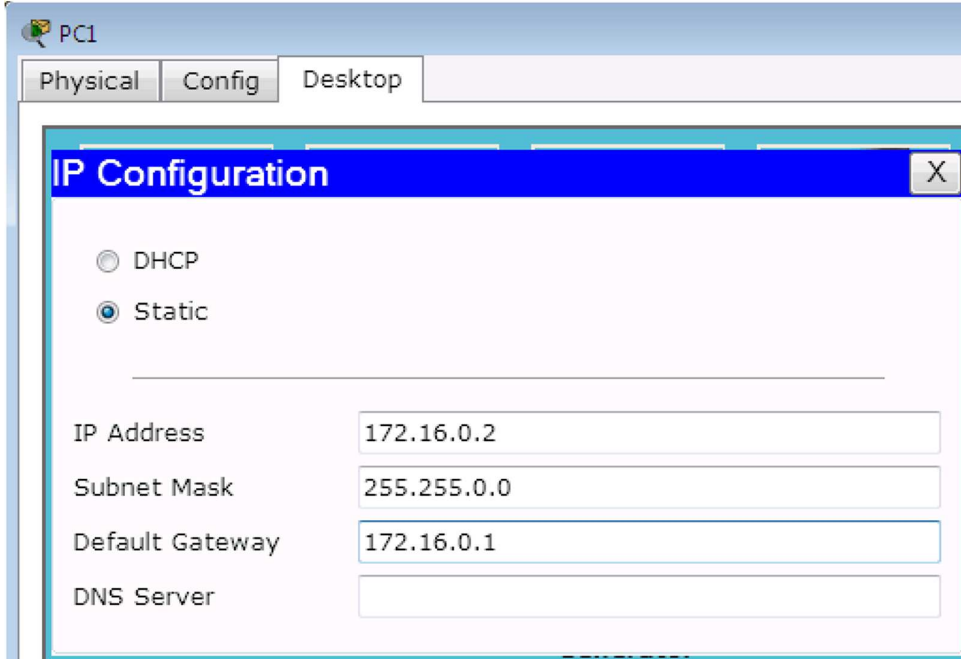
Configure RIPv1 on Cisco Routers with following information:
 Network: 172.16.0.0/16, 192.168.0.0/24, 10.0.0.0/8

Gateway Address: 172.16.0.1/16, 192.168.0.1/24, 10.0.0.1/8



Putting three IP addresses, subnet mask and default gateway to three PCs.

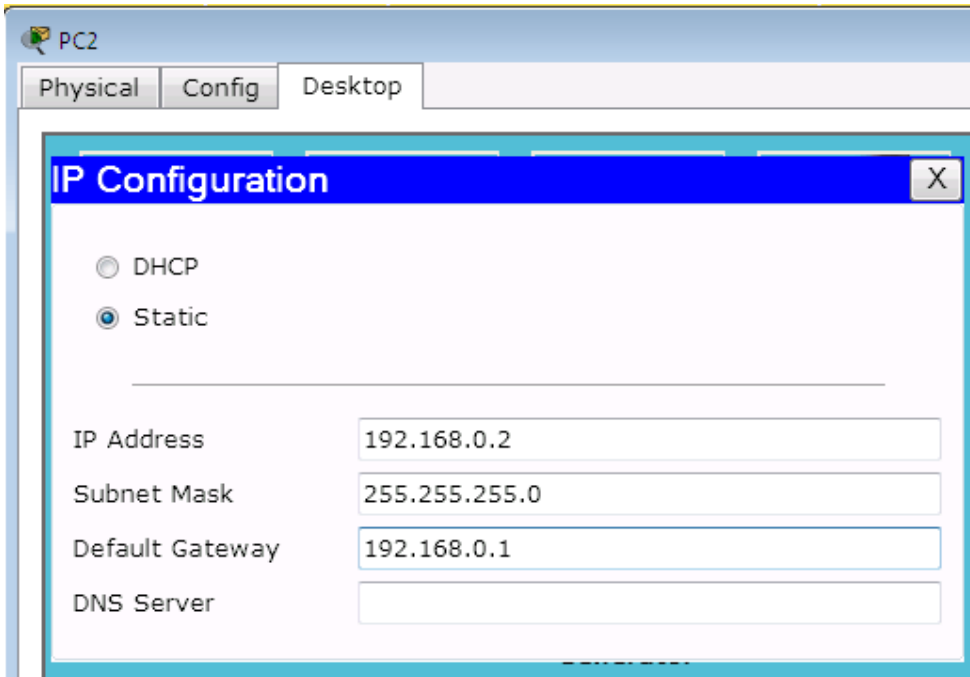
Click PC1/ Desktop/IP Configuration/Static



The screenshot shows the 'IP Configuration' dialog box for PC1. The 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IP Address	172.16.0.2
Subnet Mask	255.255.0.0
Default Gateway	172.16.0.1
DNS Server	

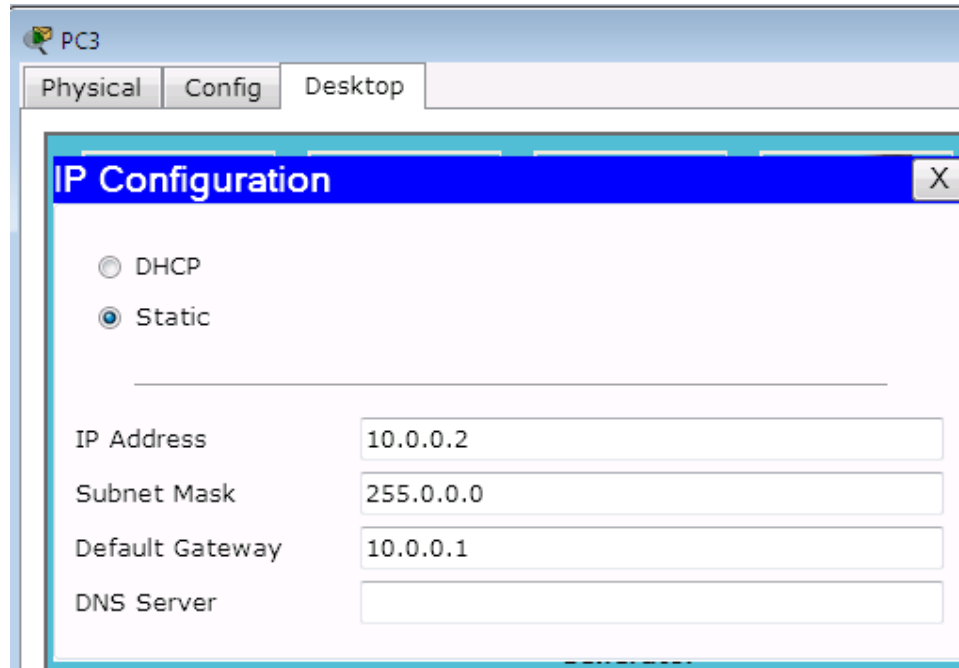
Click PC2/ Desktop/IP Configuration/Static



The screenshot shows the 'IP Configuration' dialog box for PC2. The 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IP Address	192.168.0.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DNS Server	

Click PC3/ Desktop/IP Configuration/Static



Configure Router R1

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R1
R1(config)#int fa 0/1
R1(config-if)#ip address 172.16.0.1 255.255.0.0
R1(config-if)#no shut
R1(config-if)#int fa 1/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shut
R1(config)#int fa 0/0
R1(config-if)#ip address 100.0.0.1 255.255.255.252
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#
```

Configure Router R2


```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R2
R2(config)#int fa 0/0
```

```
R2(config-if)#ip address 100.0.0.2 255.255.255.252
R2(config-if)#no shut
R2(config)#int fa 0/1
R2(config-if)#ip address 10.0.0.1 255.0.0.0
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#
```

Configure RIPv1 to router R1 Here we put all three network those are connected to R1 router.

A numeric value is required for EIGRP, OSPF. With EIGRP, AS number, with OSPF, the process number, but RIP, there is no number.

```
R1(config)#router rip
R1(config-router)#network ?
  A.B.C.D Network number
R1(config-router)#network 172.16.0.0 ?
  <cr>
R1(config-router)#network 172.16.0.0
R1(config-router)#network 192.168.0.0
R1(config-router)#network 100.0.0.0
R1(config-router)#^Z
R1#
```

Configure RIPv1 to router R2

Here we put two network those are connected to R2 router.

```
R2(config)#router rip
R2(config-router)#network ?
  A.B.C.D Network number
R2(config-router)#network 100.0.0.0
R2(config-router)#network 10.0.0.0
R2(config-router)#^Z
R2#
```

See routing table of router R1

```
R1#show ip route
```

Gateway of last resort is not set

```
R 10.0.0.0/8 [120/1] via 100.0.0.2, 00:00:20, FastEthernet0/0
  100.0.0.0/30 is subnetted, 1 subnets
C   100.0.0.0 is directly connected, FastEthernet0/0
```

```
C 172.16.0.0/16 is directly connected, FastEthernet0/1
C 192.168.0.0/24 is directly connected, FastEthernet1/0
R1#
```

```
R1#show ip rip database
```

```
10.0.0.0/8
  [1] via 100.0.0.2, 00:00:12, FastEthernet0/0
100.0.0.0/30 directly connected, FastEthernet0/0
172.16.0.0/16 directly connected, FastEthernet0/1
192.168.0.0/24 directly connected, FastEthernet1/0
R1#
```

See routing table of router R2

```
R2#show ip route
```

Gateway of last resort is not set

```
C 10.0.0.0/8 is directly connected, FastEthernet0/1
  100.0.0.0/30 is subnetted, 1 subnets
C   100.0.0.0 is directly connected, FastEthernet0/0
R 172.16.0.0/16 [120/1] via 100.0.0.1, 00:00:09, FastEthernet0/0
R 192.168.0.0/24 [120/1] via 100.0.0.1, 00:00:09, FastEthernet0/0
R2#
```

```
R2#show ip rip database
10.0.0.0/8   directly connected, FastEthernet0/1
100.0.0.0/30 directly connected, FastEthernet0/0
172.16.0.0/16
  [1] via 100.0.0.1, 00:00:19, FastEthernet0/0
192.168.0.0/24
  [1] via 100.0.0.1, 00:00:19, FastEthernet0/0
R2#
```

Now check IP connectivity

Click PC-1/ **Desktop/Command Prompt**

```
PC>ping 10.0.0.2
```

Pinging 10.0.0.2 with 32 bytes of data:

```
Reply from 10.0.0.2: bytes=32 time=12ms TTL=126
```

```
Reply from 10.0.0.2: bytes=32 time=13ms TTL=126
```

```
Reply from 10.0.0.2: bytes=32 time=12ms TTL=126
```

```
Reply from 10.0.0.2: bytes=32 time=20ms TTL=126
```

Ping statistics for 10.0.0.2:

Packets: Sent=4, Received=4, Lost=0(0% loss),

Approximate round trip times in milli-seconds:

Minimum = 12ms, Maximum = 20ms, Average = 14ms

```
PC>
```

We can reach 10.0.0.0 network.

Click PC-2/ **Desktop/Command Prompt**

```
PC>ping 10.0.0.2
```

Pinging 10.0.0.2 with 32 bytes of data:

```
Reply from 10.0.0.2: bytes=32 time=12ms
```

```
TTL=126 Reply from 10.0.0.2: bytes=32
```

```
time=14ms TTL=126 Reply from 10.0.0.2:
```

```
bytes=32 time=24ms TTL=126 Reply from
```

```
10.0.0.2: bytes=32 time=11ms TTL=126
```

Ping statistics for 10.0.0.2:

Packets: Sent=4, Received=4, Lost=0(0% loss),

Approximate round trip times in milli-seconds:

Minimum = 11ms, Maximum = 24ms, Average = 15ms

PC>

We can reach 10.0.0.0 network.

Click PC-3/ **Desktop/Command Prompt**

PC>ping 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:

Reply from 172.16.0.2: bytes=32 time=10ms

TTL=126 Reply from 172.16.0.2: bytes=32

time=11ms TTL=126 Reply from 172.16.0.2:

bytes=32 time=12ms TTL=126 Reply from

172.16.0.2: bytes=32 time=16ms TTL=126

Ping statistics for 172.16.0.2:

Packets: Sent=4, Received=4, Lost=0(0% loss),

Approximate round trip times in milli-seconds:

Minimum = 10ms, Maximum = 16ms, Average = 12ms

PC>

We can reach 172.16.0.0 network.

```
PC>ping 192.168.0.2
Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=12ms TTL=126
Reply from 192.168.0.2: bytes=32 time=11ms TTL=126
Reply from 192.168.0.2: bytes=32 time=22ms TTL=126
Reply from 192.168.0.2: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.0.2:
    Packets: Sent=4, Received=4, Lost=0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 22ms, Average = 13ms

PC>
```

We can reach 192.168.0.0 network.

Routing Information Protocol - RIP Command Tutorial

RIP Command

1. The command **show ip route** followed by the protocol will show that protocol's route from the entire routing table.

```
R1#show ip route rip
```

2. The command **show protocols** is used to view the RIP routing protocol settings and configuration.

3. The command **show ip rip database** will display RIP routing updates or RIP routing information as they are sent and received. But to see the updates in real time, we need command **Debug not Show**.

But don't do **debug ip rip**, don't do **debug all**. It may crash your router. Because all possible debugs will start and consume router's whole processing and memory.

4. If The command **Router(config-router)#version 2** is entered on the routers, only version 2 updates are sent to 224.0.0.9.

5. If The command **Router(config-router)#no version 2** is entered on the routers, version 1 and 2 updates will be received and the version 2 updates will not be sent.

6. The command **debug ip rip** shows the routes being advertised in RIP updates and the metrics of these routes. i.e. **debug ip rip** will display RIP activity as it occurs on a router.

```
R1#debug iprip
```

7. The command **clear ip route *** should apply after the command **debug ip rip** to clear the routing table of its dynamic routes.

R1#**clear ip route ***

The command **undebug all** **turn off all debugs.**

R1#**undebug all**

8. To turn off specific debugs, run the command **no debug** followed by the type of debug you want to turn off.

R1#**no debug ip rip**

Practical No.6

Configuring OSPF.

Link: Interface on a router

OSPF Terminology

Link state: Description of an interface and of its relationship to its neighboring routers.

The collection of all the link-states would form a link-state database.

1. OSPF uses cost as a metric, which is the inverse of the bandwidth of a link. OSPF identifies the best route by use of cost.
2. OSPF uses Dijkstra or SPF(Shortest Path First) algorithm. Dijkstra or SPF is a same algorithm.
3. OSPF provides a loop free topology.
4. OSPF's **administrative distance** is 110.
5. Before exchanging routing information, OSPF routers find out neighbors.
OSPF routers exchange LSAs, and the OSPF algorithm uses the contents of those LSAs to build their routing table. In this way, OSPF allows extensive control of routing updates.
6. OSPF is complex to configure and difficult to troubleshoot. 7. OSPF does not support IPX.
8. OSPF requires more memory and faster processors to handle OSPF than distance vector protocol. i.e. OSPF is a CPU-intensive protocol, and very large OSPF networks can experience routing and update traffic problems that seriously impact network performance.
9. OSPF confines network instability to a single area of the network.
10. OSPF uses WILDCARD MASK instead subnet mask.

Advantages of OSPF

1. OSPF is an open-standard, purely link-state protocol.
RIP, IGRP and EIGRP are distance-vector (routing by rumor) routing protocols, susceptible to routing loops, split-horizon, and other issues.
2. OSPF converges very quickly - from the point of recognizing a failure, it often can converge in less than 10

seconds.

3. OSPF sends updates only changed portion or partial updates of a network when link status changes rather than the complete routing table. In this way, it reduces the usage of bandwidth (BW) and decreases routing overhead by sending triggered updates to announce changes in the network. RIP and IGRP hold-down timers can cause slow convergence.

4. OSPF supports VLSM and CIDR. OSPF supports route summarization. RIPv1 and IGRP do not.

5. OSPF is a classless protocol, not classful.

6. OSPF uses the concept of areas to implement **hierarchical design**, not a flat design like RIP.

7. With OSPF, a router does not flood its own LSAs when its age reaches 30 minutes. The flooding, however, does not happen all at once, so the overhead is minimal. RIP sends its entire routing table every 30 seconds, IGRP every 90 seconds.

8. Link state protocol like OSPF doesn't have anything like Hop. i.e. Do not use hops to mark networks as unreachable.

When an OSPF router does not receive a Hello packet for a specified time period, it assumes that the neighbor is down. The router then runs the SPF algorithm to calculate new routes.

OSPF Area Tutorial

OSPF Area

1. OSPF uses the concept of areas which helps route summarization.

2. Area 0 is called the backbone area.

3. Multiple OSPF areas must connect to area 0.

4. If you have only one area, it must be called area 0.

5. The area number can be in the range from 0 to 4,294,967,295; or 0 to 4.2 million.

6. The backbone area is not a network type, but a collection of OSPF network links.

Area 0 is reserved as the backbone area, and routers within area 0 may or may not go through the DR/BDR election process, depending on the network type.

7. If a network in an area goes down, it will not affect routers in other areas.

8. The OSPF command `network 0.0.0.0 255.255.255.255 area 0` includes all of its interfaces in area 0.

OSPF Adjacency/Neighbor Tutorial

OSPF Adjacency

1. OSPF neighbor relationship table is called an adjacency database.
2. Before exchanging routing information, OSPF routers find out neighbors. Each router discovers its neighbors on each interface. The list of neighbors is kept in a neighbor table.
3. Each router uses a reliable protocol to exchange topology information with its neighbors.
4. If OSPF is configured correctly, OSPF form neighbor relationships only with the routers directly connected to it.
5. To share information with another router, they must be neighbors: their area numbers and types, timers, and passwords must match.

To form a neighbor relationship

The following must match before routers become neighbors:

1. Hello and Dead interval must match on the two routers on the same link or they will not form adjacency.
2. The area type must match on the segments.
i.e. The router that is formed a neighbor relationship must be in the same area.
3. Subnet mask must match on the segments.
4. MTU size must match on the segments.
5. Authentication password.

OSPF Router ID Tutorial

OSPF Router ID

Router ID – Used to identify the routers in the OSPF network.

1. Each OSPF router has an ID, which is either the highest IP address on a loopback interface, if one exists, or the highest IP address on an active interface.
2. To configure **network instability** to one area of the network, OSPF uses router ID(RID) or a 32-bit IP address selected at the beginning of the OSPF process.
3. If a router's OSPF RID is hard coded or change a router's OSPF RID, router reload or clear the OSPF process is needed.

Or

Changing the OSPF RID, will require to either reload the router or clear your OSPF process.

4. RIDs have no relationship with areas.

Process of selecting RID

1. The highest IP address configured on the router is the router ID, if no loopback exist.
i.e. At the moment of OSPF process startup, the highest IP address on any active interface will be the Router ID(RID).
2. When loopback interface is created on a router, the IP address of loopback(logical) interface override the IP address and becomes the RID(router ID).
3. If multiple loopback interfaces are configured, the highest loopback address becomes the RID.

OSPF-Difference Between RIP and EIGRP Tutorial

1. OSPF is link-state routing protocol.
RIP and EIGRP are distance-vector (routing by rumor) routing protocols, susceptible to routing loops, split-horizon, and other issues.
2. OSPF has fastconvergence.
RIP use hold-down timers can cause slow convergence.
3. OSPF supports VLSM and CIDR.
RIPv1 does not supports VLSM and CIDR.
4. OSPF metric is based on bandwidth.
RIP metric is based on hop count.
EIGRP metric is based on bandwidth, delay, reliability, load.
5. OSPF only sends out changes when they occur. With OSPF, a router does flood its own LSAs when it age reaches 30 minutes.
RIP sends entire routing table every 30 seconds, IGRP every 90 seconds.
6. OSPF uses the concept of areas to implement hierarchical routing.
There are no hierarchical concept to RIP and EIGRP.

OSPF Commands Tutorial

OSPF Commands

Enable OSPF process or routing

Syntax

```
Router(config)#router ospf <process-id>
```

Configure Router R1

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R1
R1(config)#int f0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.252
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#
```

Configure Router R2

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R2
R2(config)#int f0/0
R2(config-if)#ip add
R2(config-if)#ip address 192.168.1.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#
```

Configure OSPF on router R1

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0.0.3area0
R1(config-router)#^Z
R1#
Configure OSPF on router R2
R2(config)#router ospf 1
R2(config-router)#network 192.168.1.0.0.3area0
R2(config-router)#
00:09:35: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on FastEthernet0/0 from LOADING to FULL, Loading
Done

R1#
00:09:38: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on FastEthernet0/0 from LOADING to FULL, Loading
Done
```

R1 and R2 formed adjacency over their fast Ethernet interfaces.

To see the default dead time on the fa0/0 interface of router R1:

```
R1#sh ip ospf int fa0/0
FastEthernet0/0 is up, line protocol is up
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

R1#
```

From the output, we see that the **Hello** time is 10 seconds, dead time is 40 seconds.

We want to double this **Dead** value using the command **ip ospf dead-interval** or **ip ospf hello-interval**.

By default, the dead time is four times of hello times in ospf.

So, if we double the hello time, dead time will be dynamically be doubled.

Since hello time is 10 seconds on a broadcast segment, we could put 20 here.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int fa0/0
R1(config-if)#ip ospf hello-interval 20
R1(config-if)#^Z
R1#
R1#sh ip ospf int fa0/0
Timer intervals configured, Hello 20, Dead 80, Wait 80, Retransmit 5
R1#

R2#
00:24:30: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on FastEthernet0/0 from FULL to DOWN, Neighbor
Down: Dead timerexpired

00:24:30: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on FastEthernet0/0 from FULL to Down: Interface
down or detached
R2#
```

From the output, we see that the dead time is double now.

Now we have a problem with adjacency.

```
R1#sh ip ospf neighbor
R1#
```

The adjacency went down, because we have configured hello time which effected on router R2.

To see the default dead time on the interface fa0/0 of R2 router:

```
R2#sh ip ospf int fa0/0
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
R2#
```

Using the command **ip ospf hello** on R2's fa0/0 interface to double the hello time:

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int fa0/0
R2(config-if)#ip ospf hell
R2(config-if)#ip ospf hello-interval 20
R2(config-if)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

00:35:40: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on FastEthernet0/0 from EXCHANGE to FULL,
Exchange Done

R2#

R2#sh ip ospf int fa0/0
  Timer intervals configured, Hello 20, Dead 80, Wait 80, Retransmit 5
R2#

Note, both hello and dead timer now have changed.
R1#
00:35:44: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.2 on FastEthernet0/0 from EXCHANGE to FULL,
Exchange Done
```

And we see that, adjacency again formed between R1 and R2 routers.

Practical No.7

Run different SCTP commands.

sctp

To enter the Stream Control Transmission Protocol (SCTP) configuration, use the sctp command in IDSN User Adaptation Layer (IUA) configuration mode. To disable, use the no form of this command.

sctp [[**t1-init***milliseconds*] [**t3-rtx-min***seconds*] [**t3-rtx-max***milliseconds*] [**startup-rtxnumber**] [**assoc-rtxnumber**] [**path-rtxnumber**]]

nosctp

Syntax Description

t1 - initmilliseconds	Timer T1 initiation value in milliseconds. Valid values are from 1000 to 60000. The t1-init configurable option applies only during the creation of an SCTP instance.
t3 -rtx-min seconds	Timer T3 retransmission minimum timeout in seconds. Valid values are from 1 to 300.
t3 -rtx-max milliseconds	Timer T3 retransmission maximum timeout in milliseconds. Valid values are from 1000 to 60000.
startup -rtx number	Maximum startup retransmissions. The startup-rtx configurable option applies only during the creation of an SCTP instance. Valid values are from 2 to 20.
assoc -rtx number	Maximum association retransmissions. Valid values are from 2 to 20.
path-rtx number	Maximum path retransmissions. Valid values are from 2 to 20.

Command Default

SCTP configuration commands cannot be entered.

Command Modes

IUA configuration (config-iaa)

To enter SCTP configuration commands, you must first enter IUA configuration mode and then enter sctp at the Router(config-iaa)# prompt to enter SCTP configuration mode.

Examples

The following example shows how to enter IUA configuration mode:

Router# configure terminal

Enter configuration commands, one per line.

End with CNTL/Z.

Router(config)# **iaa**

Router(config-iaa)#

The following is an example of how to set failover time (in milliseconds) between 1 and 10 seconds as part of SCTP configuration of the T1 initiation timer. This example uses the lowest failover timer value allowed (1 second):

Router(config-iaa)# **as as5400-3 fail-over 1000**

The following is an example of how to set SCTP maximum startup retransmission interval. This example uses the maximum startup retransmission interval value allowed:

Router(config-iaa)# **as as5400-3 sctp-startup 20**

The following is an example of how to configure the number of SCTP streams for this AS. This example uses the maximum SCTP streams allowed:

Router(config-iaa)# **as as5400-3 sctp-streams 57**

The following is an example of how to configure the SCTP T1 initiation timer (in milliseconds). This example uses the maximum timer value allowed:

Router(config-iaa)# **as as5400-3 sctp-t1init 60000**

Related Commands

Command	Description
pri-group (pri-slt)	Specifies an ISDN PRI on a channelized T1 or E1 controller.

show debugging

To display information about the types of debugging that are enabled for your router, use the show debugging command in privileged EXEC mode.

showdebugging**Syntax Description**

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Use this command to display the current SCTP association and instance identifiers, the current state of SCTP associations, and the local and remote port numbers and addresses that are used in the associations.

Examples

The following is sample output from this command for three association identifiers:

Router# **show ipsctp association list**

```
*** SCTP Association List ***
AssocID:0, Instance ID:0 Current
state:ESTABLISHED
Local port:8989, Addr:10.1.0.2 10.2.0.2 Remote
port:8989, Addr:10.6.0.4 10.5.0.4 AssocID:1,
Instance ID:0
Current state:ESTABLISHED
Local port:8989, Addr:10.1.0.2 10.2.0.2 Remote
port:8990, Addr:10.6.0.4 10.5.0.4 AssocID:2,
Instance ID:0
Current state:ESTABLISHED
Local port:8989, Addr:10.1.0.2 10.2.0.2 Remote
port:8991, Addr:10.6.0.4 10.5.0.4
```

The table below describes the significant fields shown in the display.

Table 11 show ipsctp association list Field Descriptions	
Field	Description
Assoc ID	SCTP association identifier.
Instance ID	SCTP association instance identifier.
Current state	SCTP association state, which can be ESTABLISHED, CLOSED, COOKIE-WAIT, and COOKIE-ECHOED.
Local port, Addr	Port and IP address for the local SCTP endpoint.
Remote port, Addr	Port and IP address for the remote SCTP endpoint.

Related Commands

Command	Description
clear ipsctp statistics	Clears statistics counts for SCTP.
debug ipsctppi	Reports SCTP diagnostic information and messages.
show ipsctp association parameters	Displays the parameters configured for the association defined by the association identifier.
show ipsctp association statistics	Displays the current statistics for the association defined by the association identifier.

Command	Description
show ipsctp errors	Displays error counts logged by SCTP.
show ipsctp instances	Displays the currently defined SCTP instances.
show ipsctp statistics	Displays the overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an application server.
show iua asp	Displays information about the current condition of an application server process.

showipsctp association parameters

To display configured and calculated parameters for the specified Stream Control Transmission Protocol (SCTP) association, use the show ipsctp association parameters command in privileged EXEC mode.

showipsctpassociationparametersassoc-id

Syntax Description

assoc-id Association identifier. Shows the associated ID statistics for the SCTP association.

Command Modes

Privileged EXEC (#)

The following sample output shows the statistics accumulated for SCTP association 0:

Router# **show ipsctp association statistics 0**

** SCTP Association Statistics **

AssocID/InstanceID: 0/1

Current State: ESTABLISHED

Control Chunks

Sent: 623874 Rcvd: 660227

Data Chunks Sent

Total: 14235644 Retransmitted: 60487

Ordered: 6369678 Unordered: 6371263

Avg bundled: 18 Total Bytes: 640603980

Data Chunks Rcvd

Total: 14496585 Discarded: 1755575

Ordered: 6369741 Unordered: 6371269

Avg bundled: 18 Total Bytes: 652346325

Out of Seq TSN: 3069353

ULP Dgrams

Sent: 12740941 Ready: 12740961 Rcvd: 12740941

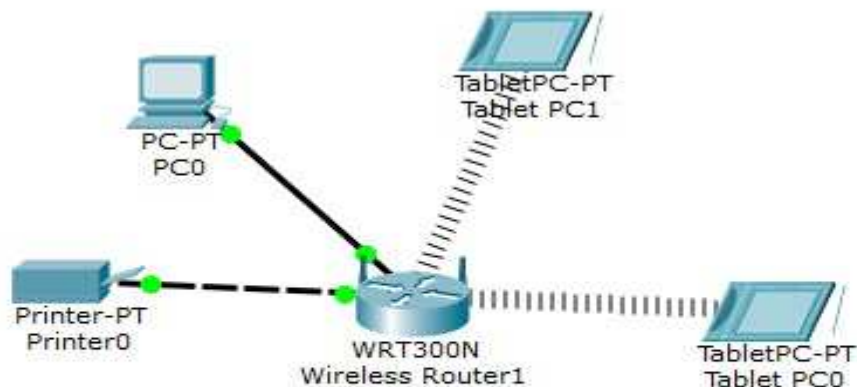
The table below describes the significant fields shown in the display.

Table 13 show ipsectp association statistics Field Descriptions	
Field	Description
AssocID/InstanceID	SCTP association identifier and instance identifier.
Current State	State of SCTP association.
Control Chunks	SCTP control chunks sent and received.
Data Chunks Sent	SCTP data chunks sent, ordered and unordered.
Data Chunks Rcvd	SCTP data chunks received, ordered and unordered.
ULP Dgrams	Number of datagrams sent, ready, and received by the Upper-Layer Protocol (ULP).

Practical No.8

Configure DHCP

Topology



Step 1: Configure the PC printer with static IPv4 addressing.

- Click **PC** and click the **Desktop** tab, which displays the IP Settings.
- Assign IP 192.168.0.23 SUBNET 255.255.255.0 with gateway 192.168.0.1 Close the window.

Step 2: Configure WRS to provide DHCP services.

- Click **WRS** and click the **GUI** tab, and maximize the window.
- The Basic Setup window displays, by default. Configure the following settings in the Network Setup section:
 - Change the IP Address to **192.168.0.1**.
 - Set the Subnet Mask to **255.255.255.0**.
 - Enable the DHCP Server.
 - Set the Static DNS 1 address to **64.100.8.8**.
 - Scroll to the bottom and click **Save**.

6. Close the **WRS** window.

Step 3: Request DHCP addressing for the home laptop.

This activity focuses on the home office. The clients that you will configure with DHCP are **Home Laptop** and **Tablet**.

- a. Click **Home Laptop** and click the **Desktop** tab > **IP Configuration**.
- b. Click **DHCP** and wait until the DHCP request is successful.
- c. **Home Laptop** should now have a full IP configuration. If not, return to Step 2 and verify your configurations on **WRS**.
- d. Close the IP Configuration window and then close the **Home Laptop** window.

Step 4: Request DHCP addressing for the tablet.

- a. Click **Tablet** and click the **Desktop** tab > **IP Configuration**.
- b. Click **DHCP** and wait until the DHCP request is successful.
- c. **Tablet** should now have a full IP configuration. If not, return to Step 2 and verify your configurations on **WRS**.

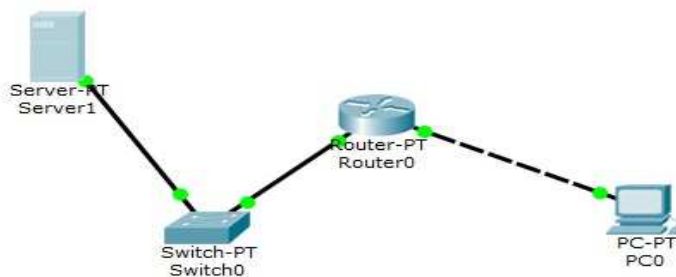
Step 5: Test access to websites.

- a. Close the **IP Configuration** window, and then click Web Browser.
- b. In the URL box, type **10.10.10.2** (for the **Central Server** website) or **64.100.200.1** (for the **Branch Server** website) and click **Go**. Both websites should appear.

Practical No.9

Configure Records on the DNS Server

Design Topology



Steps:

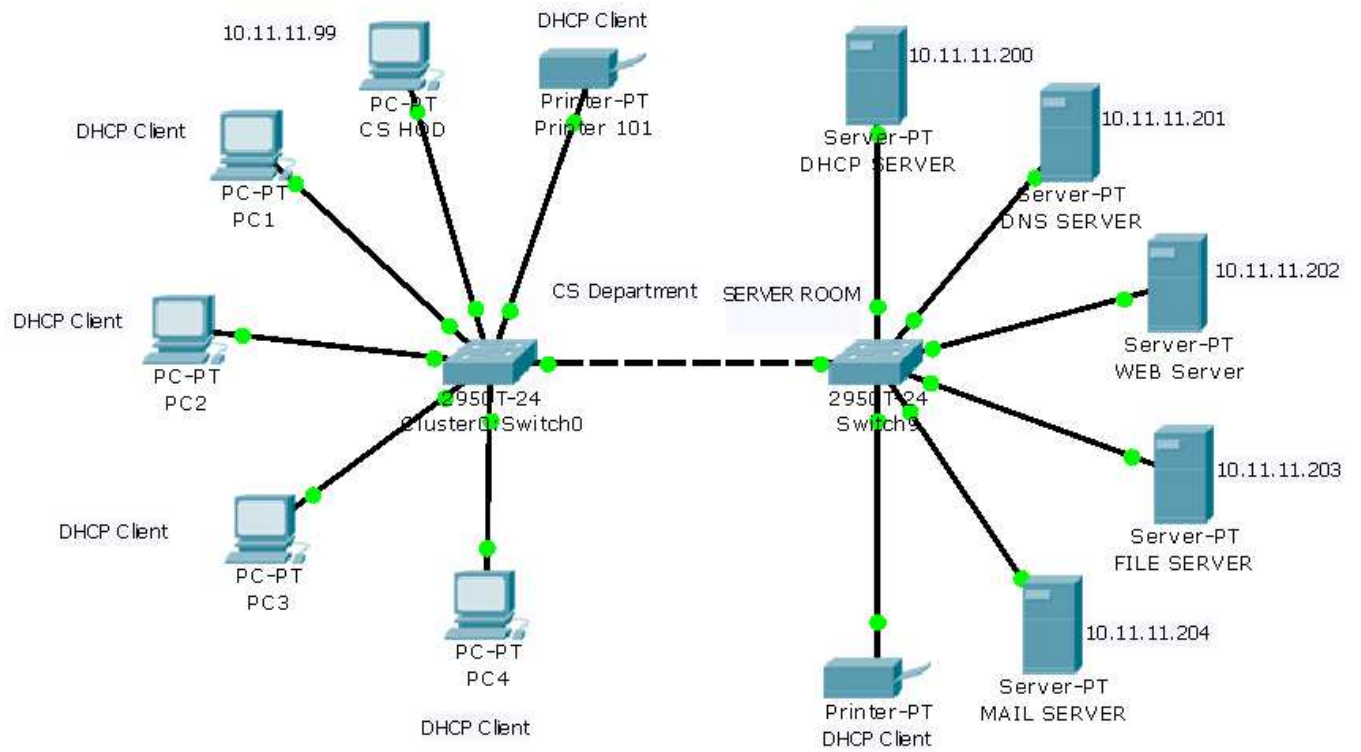
- a. Router as Ethernet 1 as 192.168.0.1 with subnet mask 255.255.255.0
- b. Router as Ethernet 1 as 192.168.1.1 with subnet mask 255.255.255.0
- c. Configure PC with IP 192.168.0.2 subnet mask 255.255.255.0 Gateway as 192.168.0.1 and DNS Server address as 192.168.1.2
- d. Configure server –Click on server—go to desktop—go to IP address.Assign IP as 192.168.1.2
- e.Go to Service tab—click on DNS—enter URL IN name field as www.mmpolytechnic.com and address as 192.168.1.2.
- f.Click on Add and then enable DNS service button.Close the window.

Test the configuration

Click on PC—click on web browser---enter URL www.mmpolytechnic.com and click GO.

Practical No.10 Configure FTP & HTTP

Sample Topology

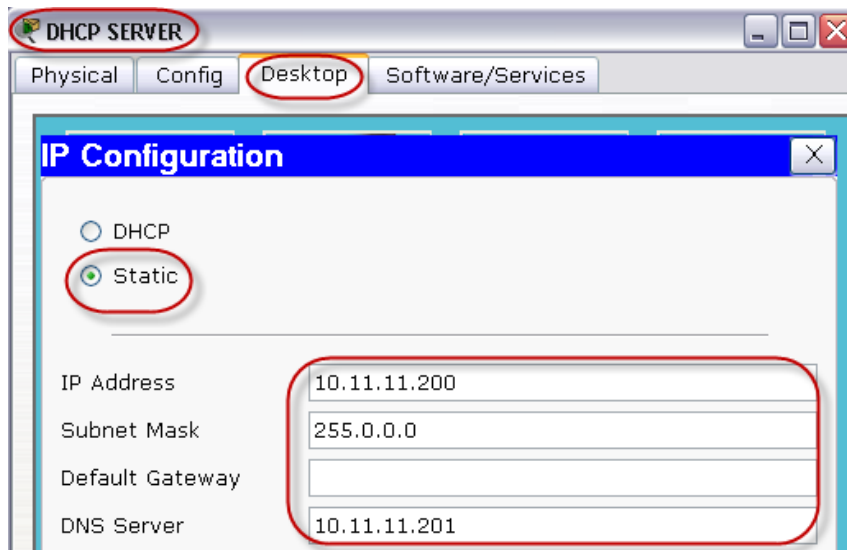


Step 1. Configure DHCP on the “DHCP SERVER” labeled Server.

- Click the Server. The server configuration window opens, Click the **Desktop** tab.
- Click the button on the Top left for **IP Configuration**.
- Verify the **Static** is Radio button selected. Set the IP Address Like:
 - ❖ IP Address: **10.11.11.200**
 - ❖ Subnet Mask: **255.0.0.0**
 - ❖ DNS Server: **10.11.11.201**

Then close the Ip configuration window.

- Click the Server. The server configuration window opens, Click the **Config** tab.
- The **Global Settings** appear. Click the button on the left for **DHCP**.
- Verify the service is **on**. **Turn OFF** other the Server services like: HTTP, FTP, AAA and Email.
- Set the **DNS Server** to like **10.11.11.201**, Set the **Start Ip Address** to **10.11.11.100**, **Subnet Mask** to **255.0.0.0** and **Maximum Number of Users** to **50**
- Click the **Save** button. **Note: Don't Click on ADD Button.**



GLOBAL

- Settings
- Algorithm Settings

SERVICES

- HTTP
- DHCP**
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP

INTERFACE

- FastEthernet

DHCP

Service: On Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 10.11.11.201

Start IP Address: 10 11 11 100

Subnet Mask: 255 0 0 0

Maximum number of Users: 50

TFTP Server: 0.0.0.0

Click Here

Add Save Remove

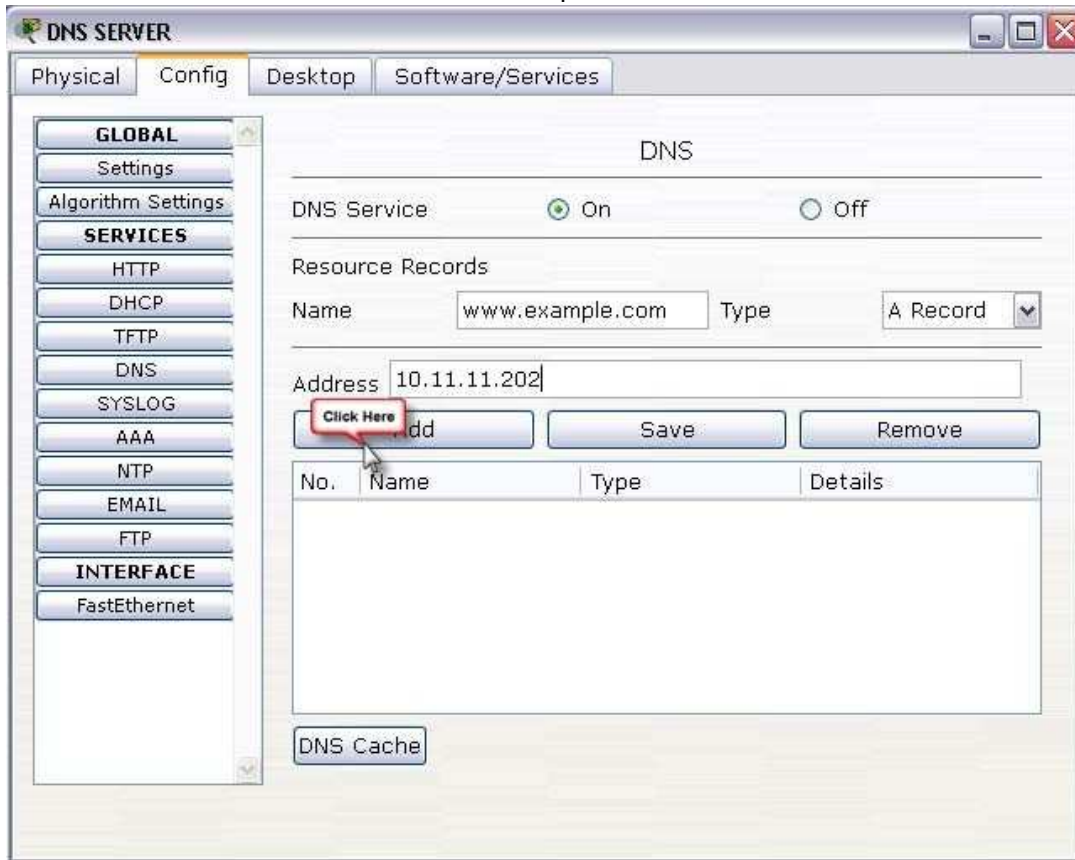
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Maximum Number of Users
serv...	0.0.0.0	10.11.11.201	10.11.11.100	255.0.0.0	50

Step 2. Configure DNS on the “DNS SERVER” labeled Server.

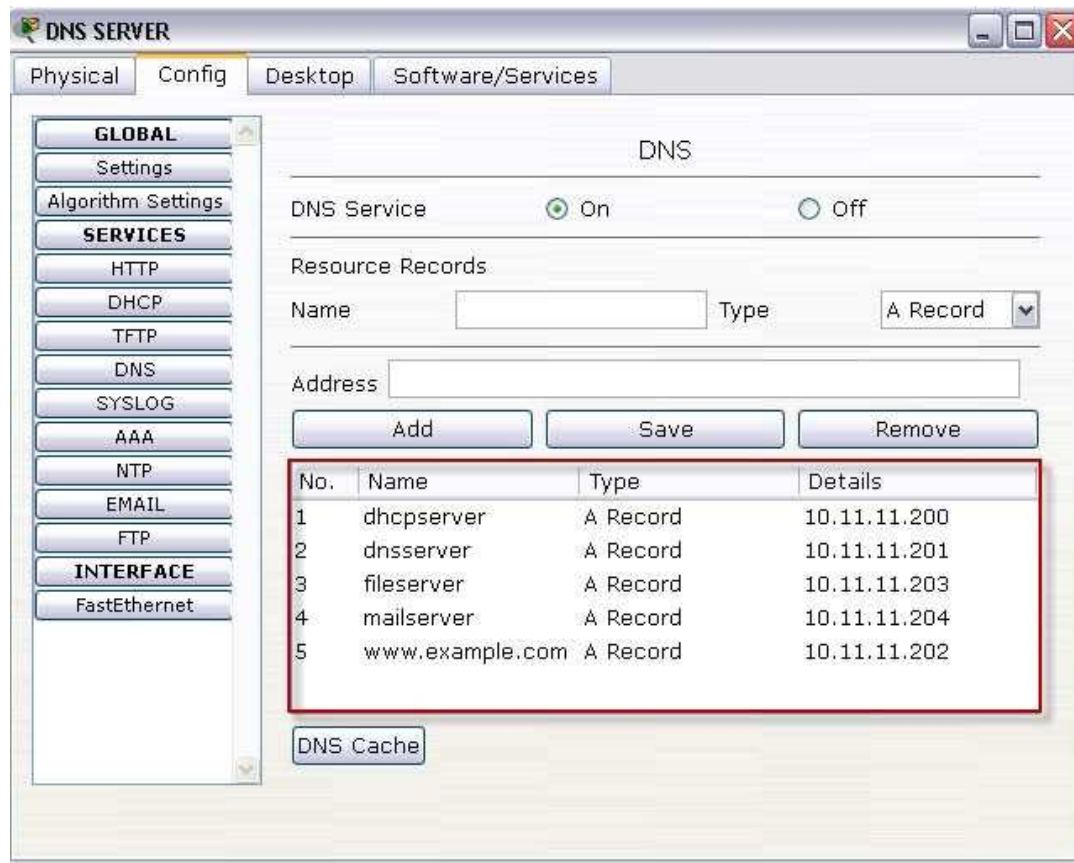
- Click the Server. The server configuration window opens, Click the **Desktop** tab.
- Click the button on the Top left for **IP Configuration**.
- Verify the **Static** is Radio button selected. Set the IP Address Like:
 - ❖ IP Address:**10.11.11.201**
 - ❖ Subnet Mask: **255.0.0.0**
 - ❖ DNS Sever: **10.11.11.201**

Then close the Ip configuration window.

- Click the Server. The server configuration window opens, Click the **Config** tab.
- The **Global Settings** appear. Click the button on the left for **DNS**.
- Verify the service is **on**. **Turn OFF** other the Server services like: HTTP, FTP, AAA and Email.
- Set the **Domain Name** to like **www.example.com** and the **IP Address** to **10.11.11.202**.
- Click the **Add** button. Additional domain names can be added in this fashion.



- Additional domain names can be added in this fashion.



The screenshot shows the 'DNS SERVER' configuration window. The 'DNS Service' is set to 'On'. The 'Resource Records' section is active, showing a table of records. The table has four columns: 'No.', 'Name', 'Type', and 'Details'. The records are as follows:

No.	Name	Type	Details
1	dhcpserver	A Record	10.11.11.200
2	dnsserver	A Record	10.11.11.201
3	filesserver	A Record	10.11.11.203
4	mailserver	A Record	10.11.11.204
5	www.example.com	A Record	10.11.11.202

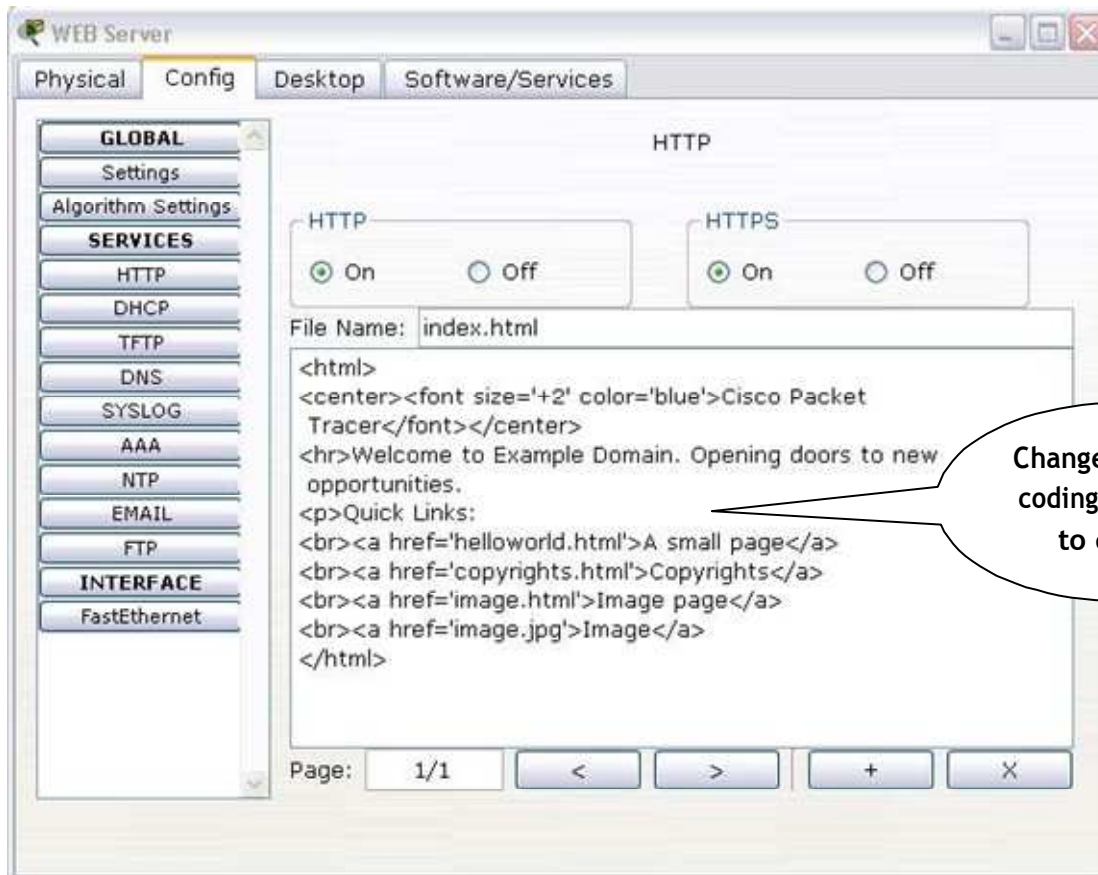
Below the table is a 'DNS Cache' button. The left sidebar shows a navigation menu with 'GLOBAL' and 'SERVICES' sections. The 'SERVICES' section includes 'HTTP', 'DHCP', 'TFTP', 'DNS', 'SYSLOG', 'AAA', 'NTP', 'EMAIL', and 'FTP'. The 'INTERFACE' section includes 'FastEthernet'.

Step 3. Configure HTTP on the “WEB Sever” labeled Server.

- Click the Server. The server configuration window opens, Click the **Desktop** tab.
- Click the button on the Top left for **IP Configuration**.
- Verify the **Static** is Radio button selected. Set the IP Address Like:
 - ❖ IP Address: **10.11.11.202**
 - ❖ Subnet Mask: **255.0.0.0**
 - ❖ DNS Sever: **10.11.11.201**

Then close the Ip configuration window.

- Click the button to select **HTTP**. Turn the service **On** and **Turn OFF** other the Server services like: DNS, FTP, AAA and Email.
- The **Default Page Content** window contains the page that is displayed when a web page is requested from the server. This page is in HTML format. This page can be changed if you would like to customize it. Close the server configuration window.

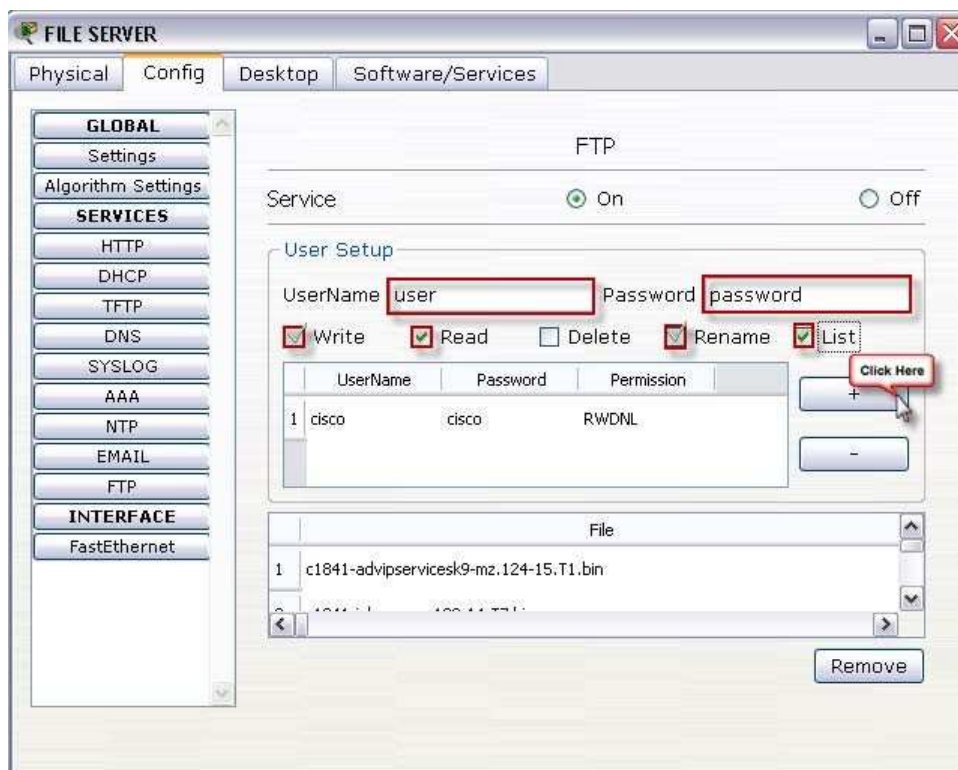


Step 4. Configure FTP on the Server (File SERVER).

- Click the Server. The server configuration window opens, Click the **Desktop** tab.
- Click the button on the Top left for **IP Configuration**.
- Verify the **Static** is Radio button selected. Set the IP Address Like:
 - ❖ IP Address: **10.11.11.203**
 - ❖ Subnet Mask: **255.0.0.0**
 - ❖ DNS Sever: **10.11.11.201**

Then close the Ip configuration window.

- Click the button to select **FTP**. Turn the service **On** and **Turn OFF** other the Server services like: HTTP, DNS, FTP, AAA and Email.



- Set the **User Name** to **user** and **Password** to **password**. And set User Permissions like Write, Read, Rename and List.
- Click the **Add(+)** button.

Step 5. Configure Mail on the Server (MAIL SERVER).

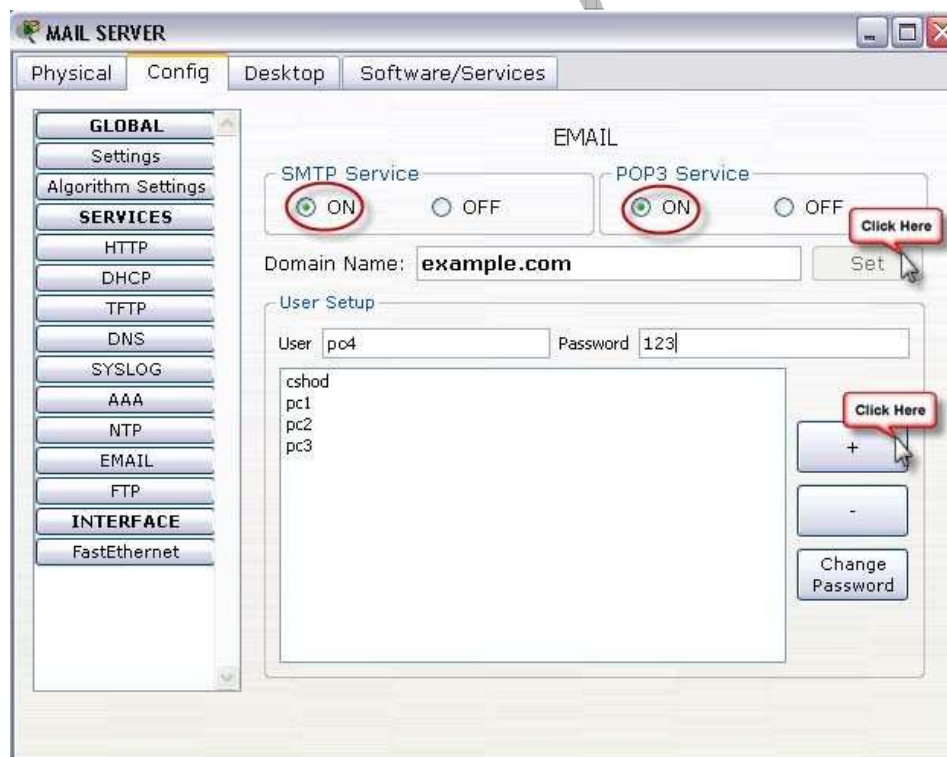
- Click the Server. The server configuration window opens, Click the **Desktop** tab.
- Click the button on the Top left for **IP Configuration**.
- Verify the **Static** is Radio button selected. Set the IP Address Like:
 - ❖ IP Address: **10.11.11.204**
 - ❖ Subnet Mask: **255.0.0.0**
 - ❖ DNS Sever: **10.11.11.201**

Then close the Ip configuration window.

- Click the Server. The server configuration window opens, Click the **Config** tab.
- The **Global Settings** appear. Click the button on the left for **Email**.
- Verify the **SMTP and POP3** services are **on**. **Turn OFF** other the Server services like: HTTP, FTP, AAA and DNS.
- Set the **Domain Name** to like **example.com** and then click the **Set** button.
- Now create some users like Ram, Shyam, Mohan, pc1, pc2, pc3 ect.. with some password.
- Click the **Add(+)** button

User Setup

User Name	Password
Cshod	123
Pc1	123
Pc2	123
Pc3	123
Pc4	123



Configure DNS support on the CS HOD labeled Client

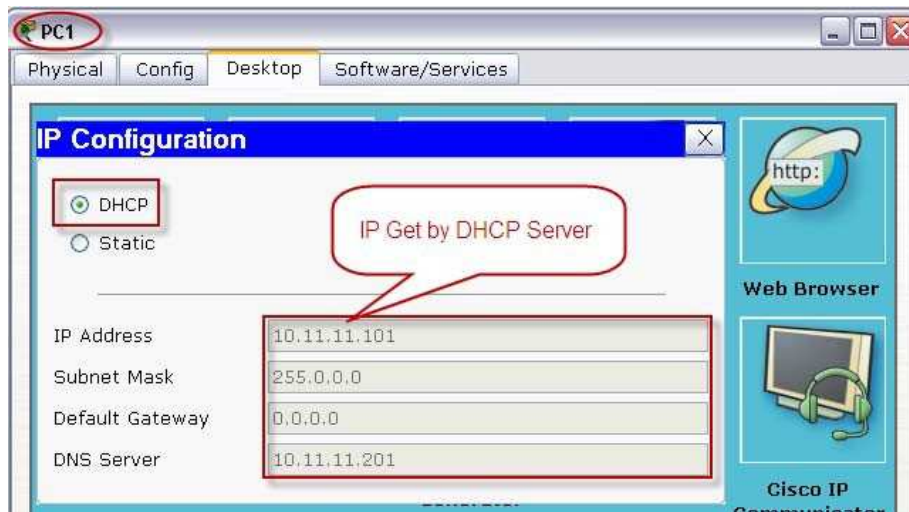
- Click the PC Client. The PC configuration window opens, Click the **Config** tab.
- Click the button on the Top left for **IP Configuration**.
- Verify the **Static** is Radio button selected. Set the IP Address Like:
 - ❖ IP Address: **10.11.11.99**
 - ❖ Subnet Mask: **255.0.0.0**
 - ❖ DNS Sever: **10.11.11.201**

Then close the IP Configuration window.



Configure DNS support on the PC1, PC2, PC3 and PC4 labeled Clients

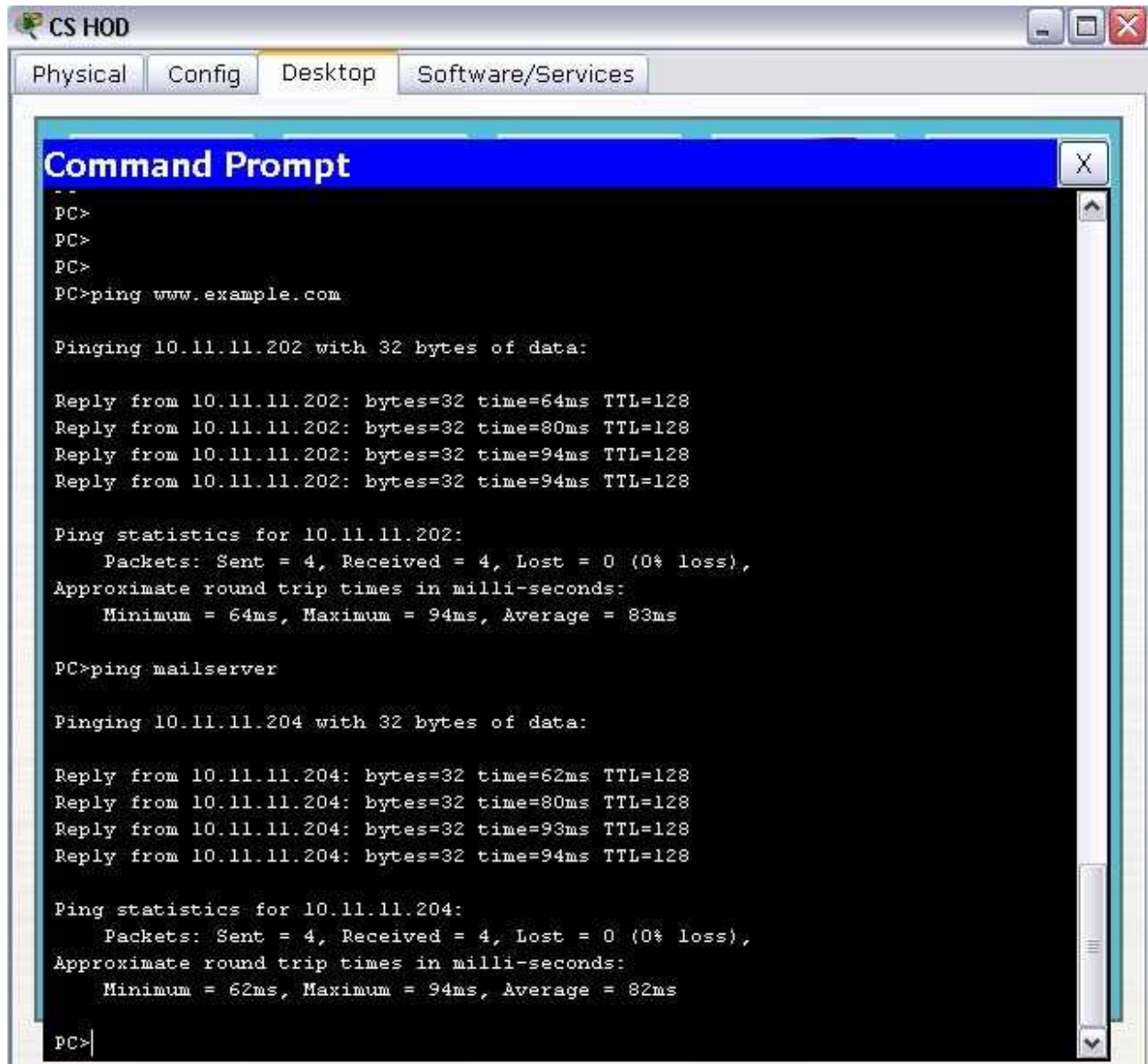
- Click the PC Client. The PC configuration window opens, Click the **Config** tab.
- Click the button on the Top left for **IP Configuration**.
- Verify the **DHCP** is Radio button selected.



Verify Connectivity in Real time Mode

Step 1. Ping the server using the URL.

Select the PC and click the **Desktop** tab. Click the **Command Prompt** button. A Command Prompt window opens. Type **ping www.example.com** (the URL of the Server) and press **Enter**. After the ping succeeds, close the Command Prompt window.



```
CS HOD
Physical Config Desktop Software/Services

Command Prompt
PC>
PC>
PC>
PC>ping www.example.com

Pinging 10.11.11.202 with 32 bytes of data:

Reply from 10.11.11.202: bytes=32 time=64ms TTL=128
Reply from 10.11.11.202: bytes=32 time=80ms TTL=128
Reply from 10.11.11.202: bytes=32 time=94ms TTL=128
Reply from 10.11.11.202: bytes=32 time=94ms TTL=128

Ping statistics for 10.11.11.202:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 64ms, Maximum = 94ms, Average = 83ms

PC>ping mailserver

Pinging 10.11.11.204 with 32 bytes of data:

Reply from 10.11.11.204: bytes=32 time=62ms TTL=128
Reply from 10.11.11.204: bytes=32 time=80ms TTL=128
Reply from 10.11.11.204: bytes=32 time=93ms TTL=128
Reply from 10.11.11.204: bytes=32 time=94ms TTL=128

Ping statistics for 10.11.11.204:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 62ms, Maximum = 94ms, Average = 82ms

PC>
```

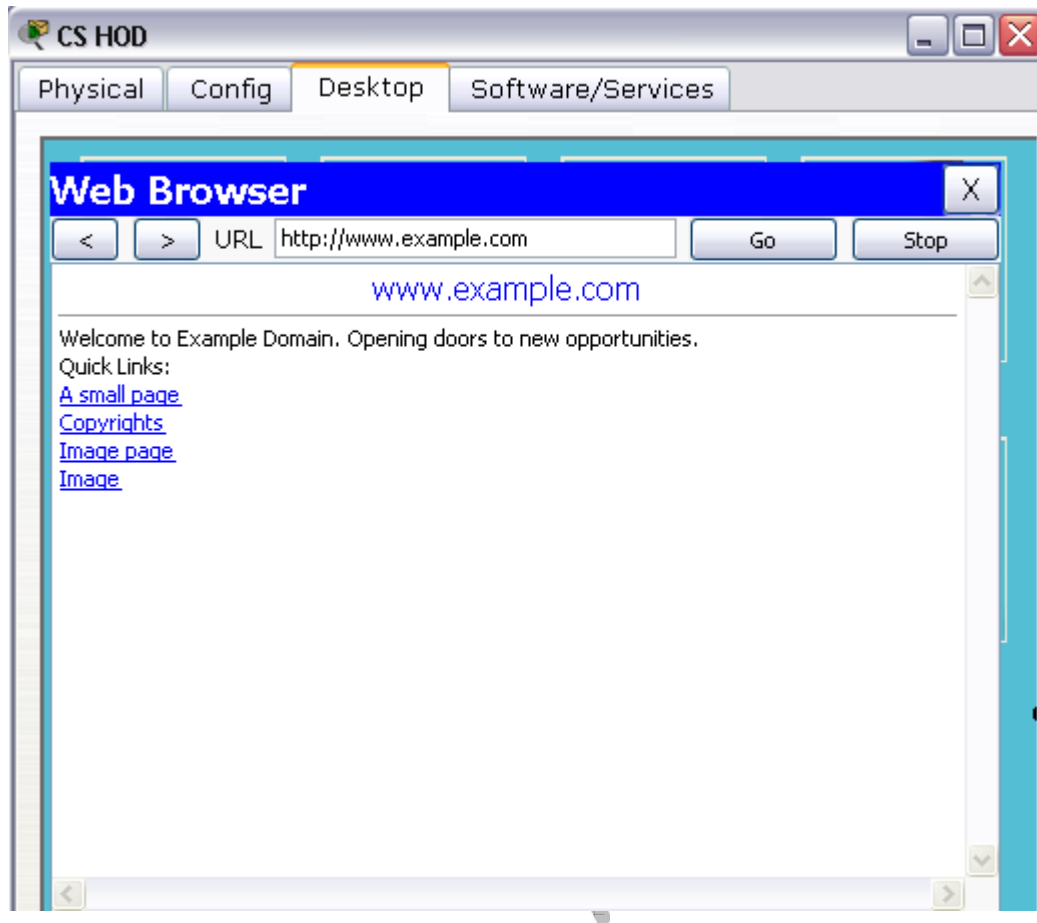
```
Server: [10.11.11.201]
Address: 10.11.11.201

Non-authoritative answer:
Name: www.example.com
Address: 10.11.11.202

PC>
```

Step 2. From the PC, Open a Web Page.

From the PC desktop, click the **Web Browser** button. A simulated web browser opens. Type **www.example.com** (the URL of the Server) into the **URL** box and click the **Go** button. A web page should appear. Close the PC configuration window.



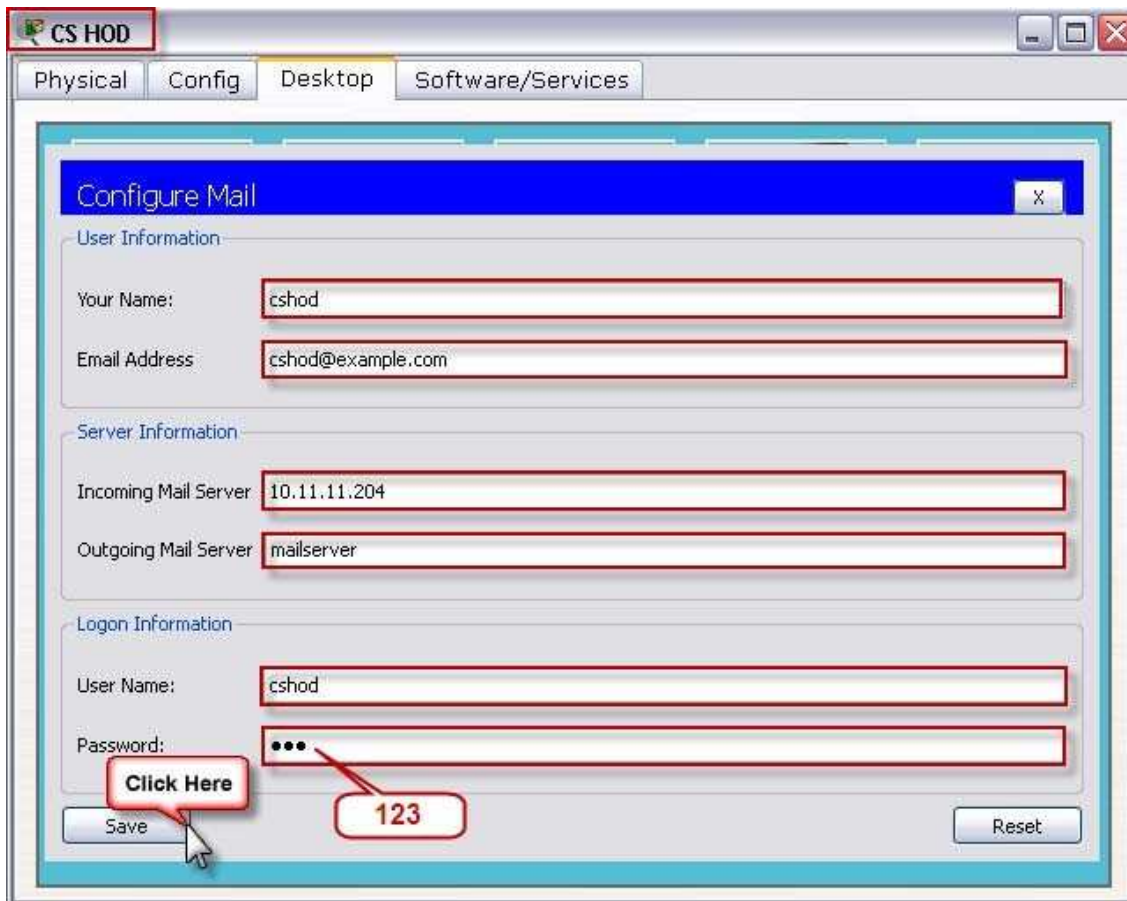
Step 3. Configure Email support on the CS HOD, PC1, PC2, PC3 and PC4 labeled Clients

- Click the PC Client. Click the **Desktop** tab. Click the button on **E mail**.
- The **Configure Mail** window opens.

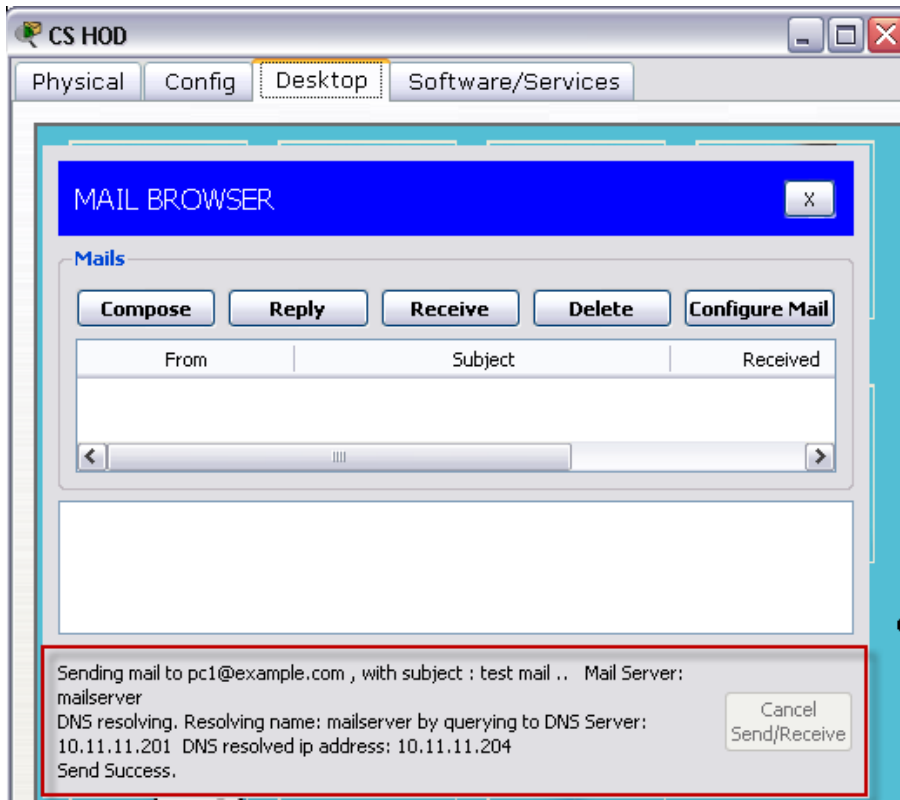
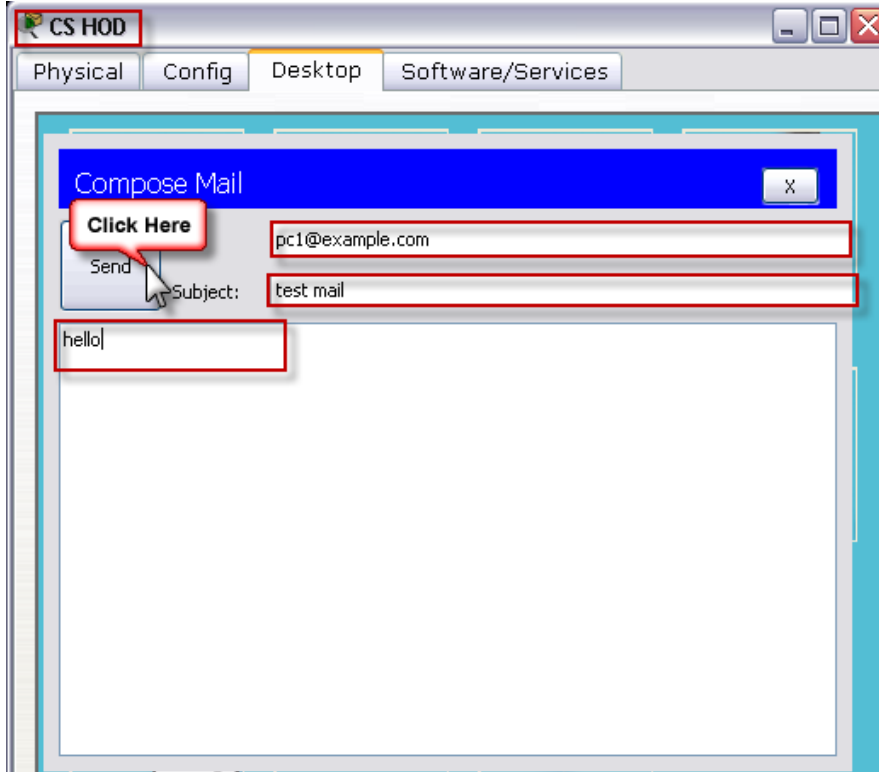
Configure Mail

User Information		
Your Name:	Cshod	
Email Address:	cshod@example.com	
Server Information		
Income mail Server	10.11.11.204 or mailserver (As per DSN Server)	
Outgoing mail Server	10.11.11.204 or mailserver (As per DSN Server)	
Logon Information		
User Name:	Cshod	
Password:	123	

Click the button on the Top **Save**.



- The **Mail Browser** window opens. Click the **Compose** button than create test mail.
- To: **pc1@example.com**
- Subject: **test mail**
- Message: Hello
- Click the button **Send**.



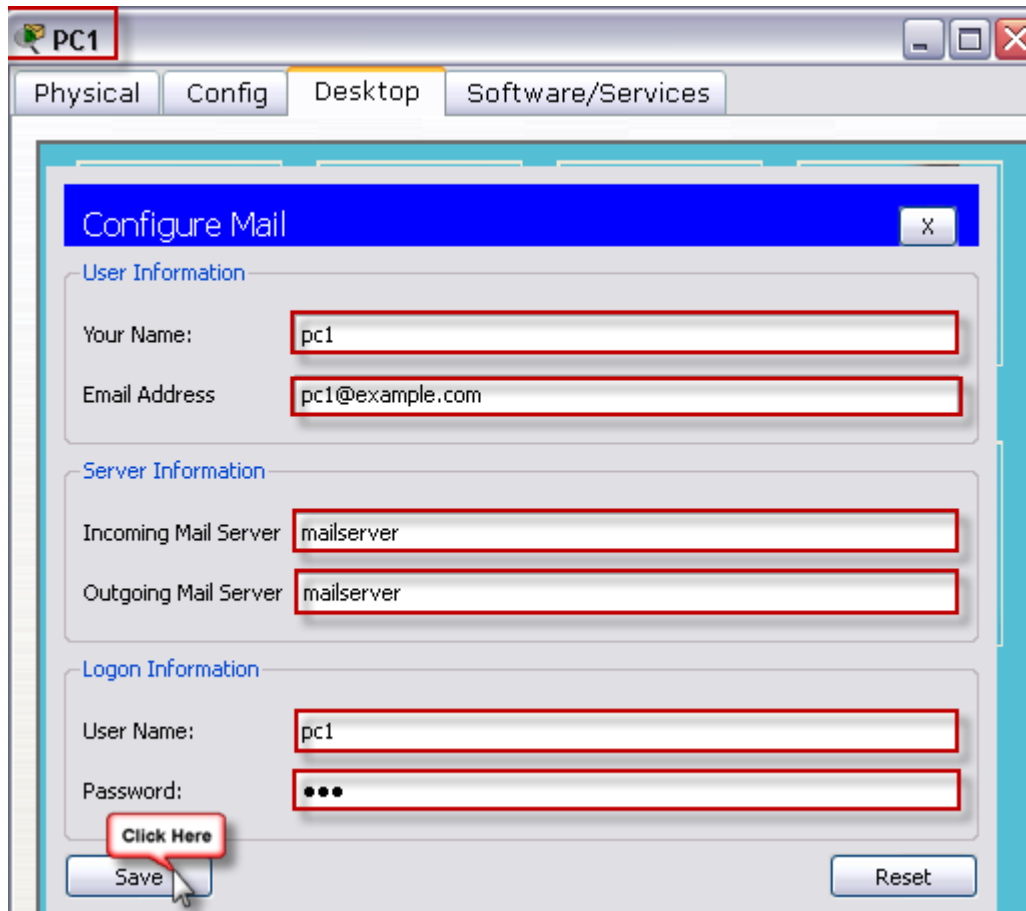
Configure Email support on the PC1, PC2, PC3 and PC4 labeled Clients

- Click the PC Client. Click the **Desktop** tab. Click the button on **E mail**.
- The **Configure Mail** window opens.

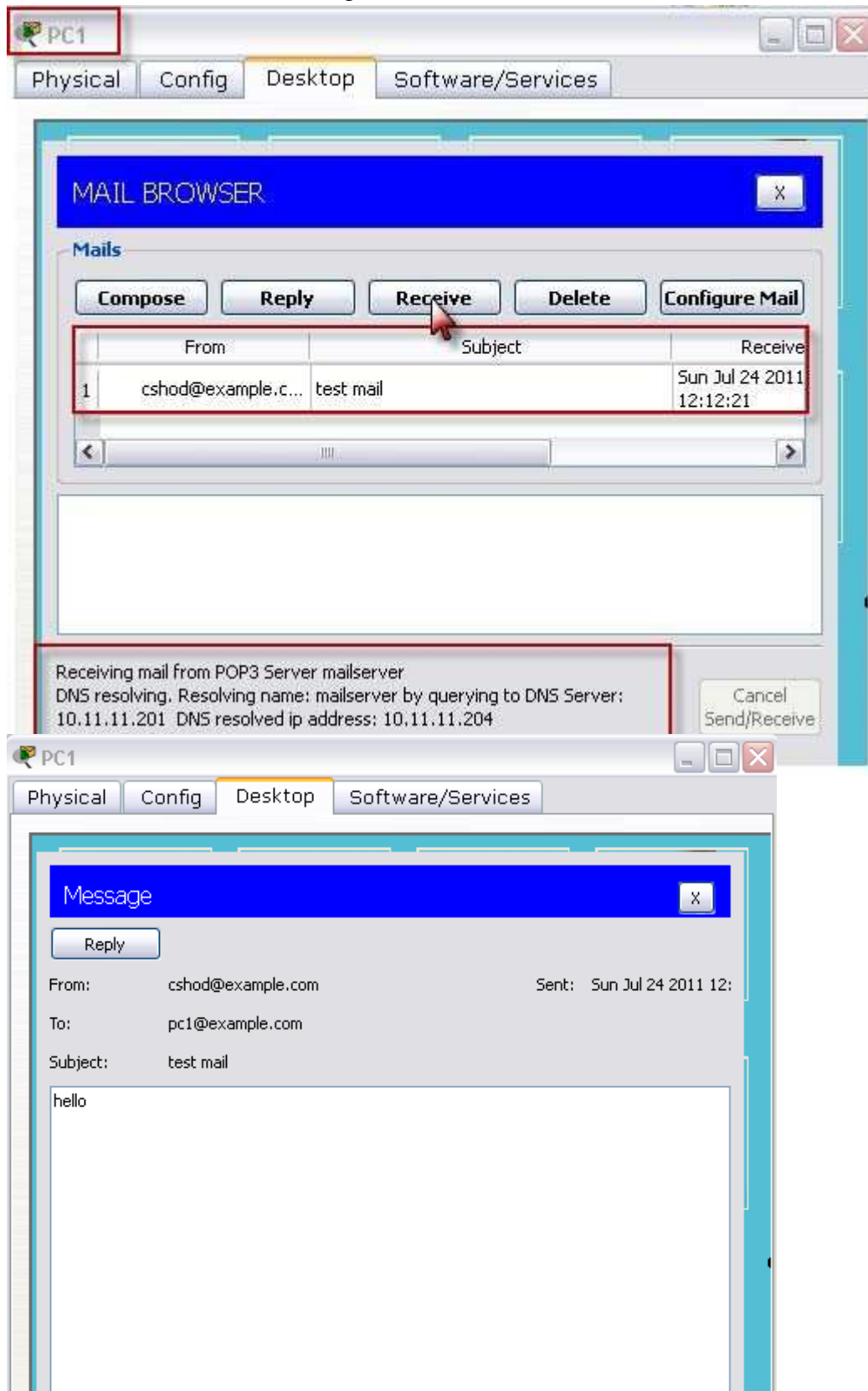
Configure Mail

User Information		
Your Name:	pc1	
Email Address:	pc1@example.com	
Server Information		
Income mail Server	10.11.11.204 or mailserver (As per DSN Server)	
Outgoing mail Server	10.11.11.204 or mailserver (As per DSN Server)	
Logon Information		
User Name:	pc1	
Password:	123	

Click the button on the Top **Save**.

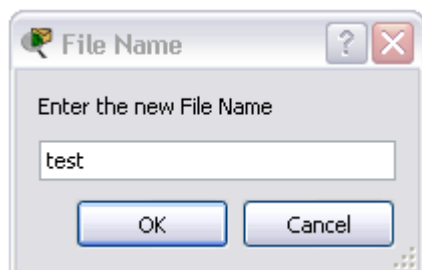


The **Mail Browser** window opens. Click the **Receive** button than find one test mail at mail box. Dabble click on mail and open it and read it.



Step 4. Configure FTP support on the PC1, PC2, PC3 and PC4 labeled Clients

- Click the CS HOD PC Client.
- Click the **Desktop** tab.
- Click the button on the Top **Text Editor**.



- Create one test file and save that file with the name test.
- Close Text Editor.
- Click the **Command Prompt** button. A Command Prompt window opens. Type dir and verify file test.txt exist or not. Than Type **ftp fileserv** or **ftp 10.11.11.203** (the URL of the file Server) and press **Enter**. After the ping succeeds, close the Command Prompt window.

The screenshot shows a CS HOD PC Client window with tabs for Physical, Config, Desktop, and Software/Services. The Desktop tab is active, displaying a Command Prompt window. The Command Prompt shows the following sequence of commands and outputs:

```
PC>dir
Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3
Directory of C:\
2/7/2106    11:58 PM    26          sampleFile.txt
1/1/1970    5:30 PM    51          test.txt
              77 bytes    2 File(s)
```

Annotations in the image include:

- A red arrow pointing to the `dir` command with the text "SHOW FILES".
- A red arrow pointing to the `ftp fileserver` command with the text "OR FTP 10.11.11.203".
- A callout box containing "User Name:user" and "Password:password" pointing to the login prompts.
- A callout box containing "show files at ftp server" pointing to the `ftp>dir` command.
- A callout box containing "Put command for copy file to ftp server put <file name>" pointing to the `ftp>put test.txt` command.
- A callout box containing "show files at ftp server" pointing to the second `ftp>dir` command.

```
PC>ftp fileserver
Trying to connect... fileserver
Connected to fileserver
220- Welcome to PT Ftp server
Username:user
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir
Listing /ftp directory from fileserver:
ftp>put test.txt
Writing file test.txt to fileserver:
File transfer in progress...
[Transfer complete - 51 bytes]
51 bytes copied in 0.172 secs (296 bytes/sec)
ftp>dir
Listing /ftp directory from fileserver:
0 : test.txt          51
ftp>
```

- Press **Ctrl + C** to exit ftp Prompt. Close the Command Prompt window.
- Click the **CS HOD PC Client**.
- Click the **Desktop** tab.
- Click the **Command Prompt** button. A Command Prompt window opens. Type `dir` and verify file `test.txt` exist or not. Then Type **ftp fileserver** or **ftp 10.11.11.203** (the URL of the file Server) and press **Enter**. After the ping succeeds, close the Command Prompt window.

ODAL

The screenshot shows a Packet Tracer PC1 window with tabs for Physical, Config, Desktop, and Software/Services. The Command Prompt window is active, displaying the following sequence of commands and outputs:

```
Packet Tracer PC Command Line 1.0
PC>dir
Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3
Directory of C:\
2/7/2106    11:58 PM    26           sampleFile.txt
                26 bytes           1 File(s)

PC>ftp 10.11.11.203
Trying to connect...10.11.11.203
Connected to 10.11.11.203
220- Welcome to PT Ftp server
Username:user
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir
Listing /ftp directory from 10.11.11.203:
0 : test.txt                    51
ftp>get test.txt
Reading file test.txt from 10.11.11.203:
File transfer in progress...

[Transfer complete - 51 bytes]

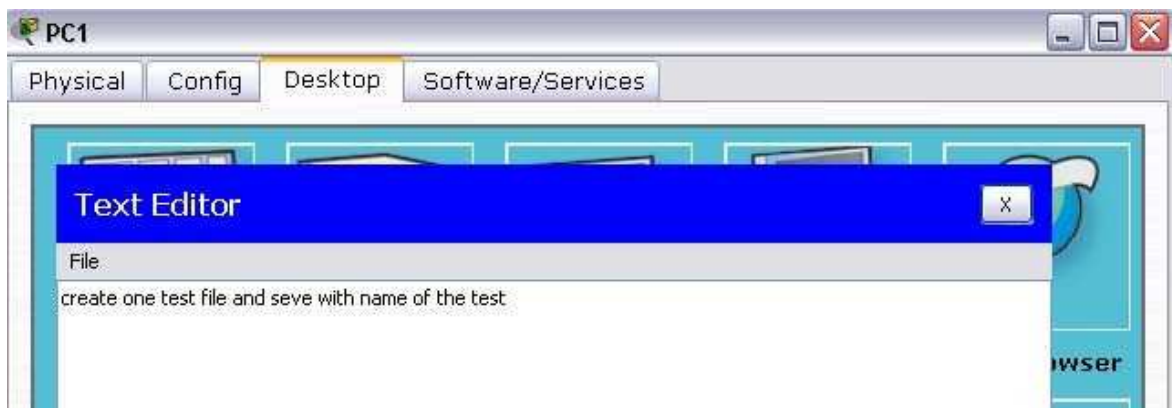
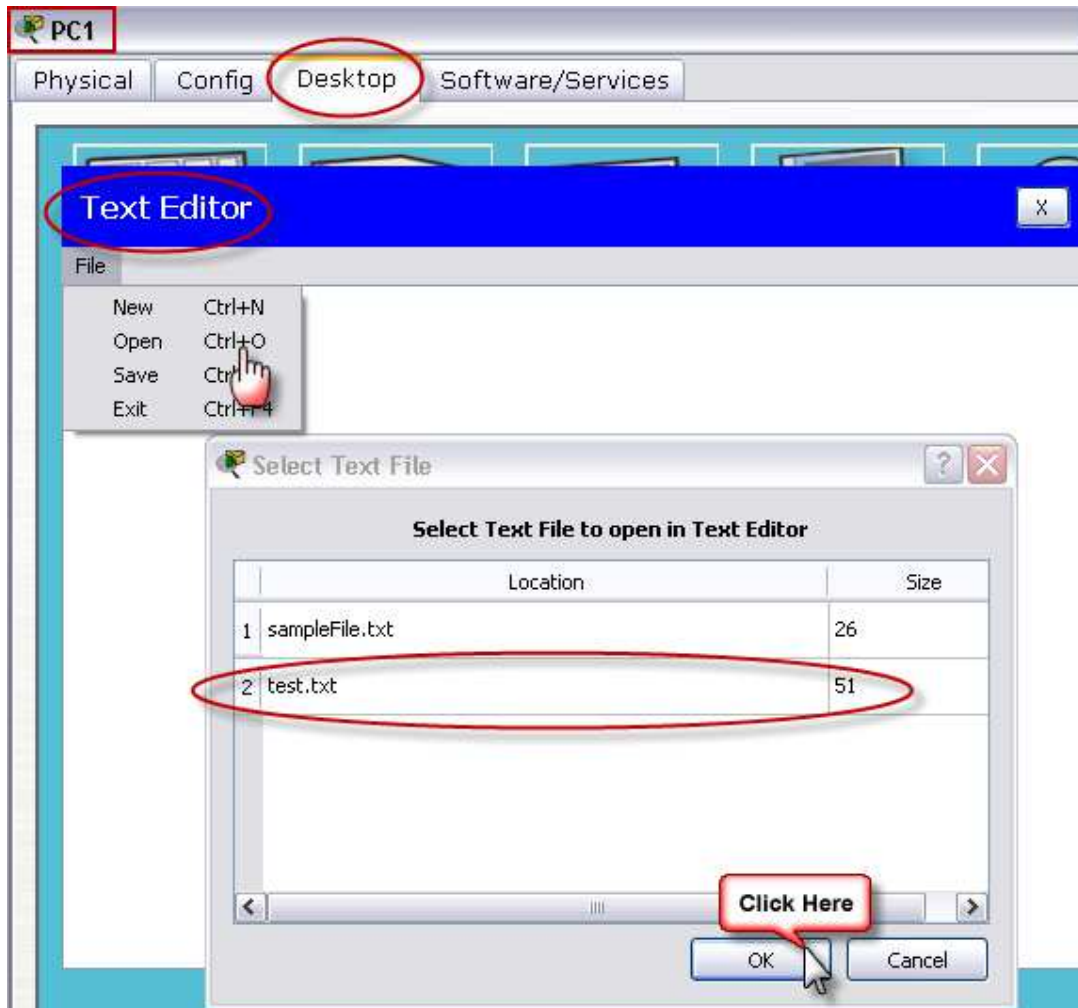
51 bytes copied in 0.156 secs (326 bytes/sec)
ftp>
Packet Tracer PC Command Line 1.0
PC>dir
Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3
Directory of C:\
2/7/2106    11:58 PM    26           sampleFile.txt
1/1/1970    5:30 PM    51           test.txt
                77 bytes           2 File(s)

PC>
```

Annotations in the image include:

- A red arrow pointing to the `PC>dir` command with the text **SHOW FILES**.
- A red arrow pointing to the `ftp 10.11.11.203` command with the text **OR FTP fileserver**.
- A callout box containing **User Name:user** and **Password:password**, with lines pointing to the corresponding input fields in the Command Prompt.
- A callout box containing **show files at ftp server**, with a line pointing to the `ftp>dir` command.
- A callout box containing **Get command for copy FTP Server to local** and **get <file name>**, with a line pointing to the `ftp>get test.txt` command.
- A second red arrow pointing to the final `PC>dir` command with the text **SHOW FILES**.

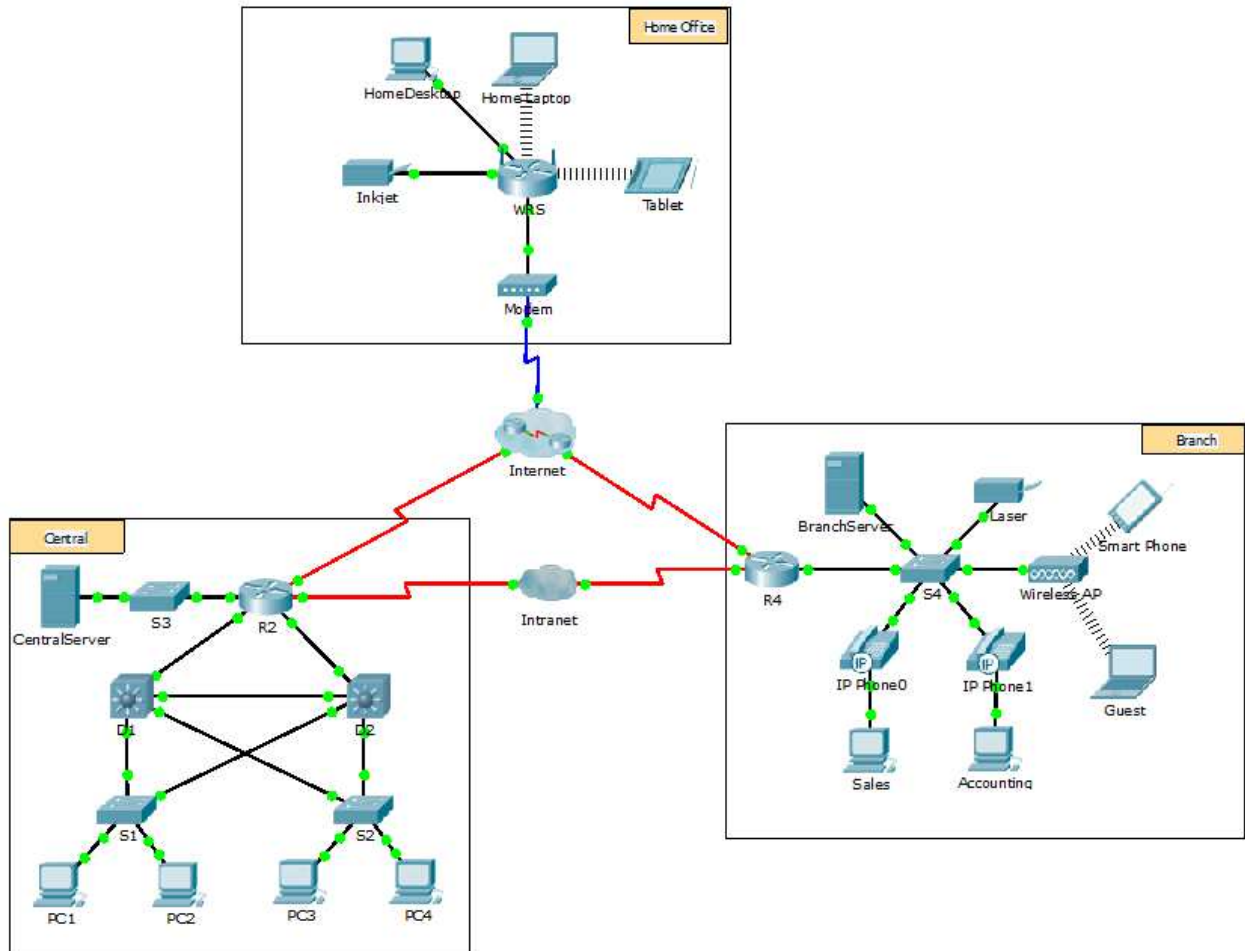
- Click the **PC1** Client.
- Click the **Desktop** tab.
- Click the button on the Top **Text Editor**.
- Click the **File Menu** than **Open**.
- Click the **file name** then click **ok**.



Practical No. 11

SMTP & POP3 (Web and Email Servers)

Topology



Objectives

Part 1: Configure and Verify Web Services

Part 2: Configure and Verify Email Services

Background

In this activity, you will configure HTTP and email services using the simulated server in Packet Tracer. You will then configure clients to access the HTTP and email services.

Note: Packet Tracer only simulates the process for configuring these services. HTTP and email software packages each have their own unique installation and configuration instructions.

Part 1: Configure and Verify Web Services

Step 1: Configure web services on Central Server and Branch Server.

- Click **Central Server** and click the **Services** tab >**HTTP**.

- b. Click **On** to enable HTTP and HTTP Secure (HTTPS).
- c. Optional. Personalize the HTML code.
- d. Repeat Step 1a –1c on **Branch Server**.

Step 2: Verify the web servers by accessing the web pages.

There are many endpoint devices in this network, but for the purposes of this step, use **PC3**.

- a. Click **PC3** and click the **Desktop** tab > **Web Browser**.
- b. In the URL box, enter **10.10.10.2** as the IP address and click **Go**. The **Central Server** website displays.
- c. In the URL box, enter **64.100.200.1** as the IP address and click **Go**. The **Branch Server** website displays.
- d. In the URL box, enter **centralserver.pt.pka** and click **Go**. The **Central Server** website displays.
- e. In the URL box, enter **branchserver.pt.pka** and click **Go**. The **Branch Server** website displays.
- f. What protocol is translating the **centralserver.pt.pka** and **branchserver.pt.pka** names to IP addresses?

Part 2: Configure and Verify Email Services on Servers

Step 1: Configure Central Server to send (SMTP) and receive (POP3) Email.

- a. Click **Central Server**, and then select the **Services** tab followed by the **EMAIL** button.
- b. Click **On** to enable the SMTP and POP3.
- c. Set the domain name to **centralserver.pt.pka** and click **Set**.
- d. Create a user named **central-user** with password **cisco**. Click + to add the user.

Step 2: Configure Branch Server to send (SMTP) and receive (POP3) Email.

- a. Click **Branch Server** and click the **Services** tab > **EMAIL**.
- b. Click **On** to enable SMTP and POP3.
- c. Set the domain name to **branchserver.pt.pka** and click **Set**.
- d. Create a user named **branch-user** with password **cisco**. Click + to add the user.

Step 3: Configure PC3 to use the Central Server email service.

- a. Click **PC3** and click the **Desktop** tab > **E Mail**.
- b. Enter the following values into their respective fields:
 - 1) Your Name: **Central User**
 - 2) Email Address: **central-user@centralserver.pt.pka**
 - 3) Incoming Mail Server: **10.10.10.2**
 - 4) Outgoing Mail Server: **10.10.10.2**
 - 5) User Name: **central-user**
 - 6) Password: **cisco**

- c. Click **Save**. The Mail Browser window displays.
- d. Click **Receive**. If everything has been set up correctly on both the client and server, the Mail Browser window displays the Receive Mail Success message confirmation.

Step 4: Configure Sales to use the Email service of Branch Server.

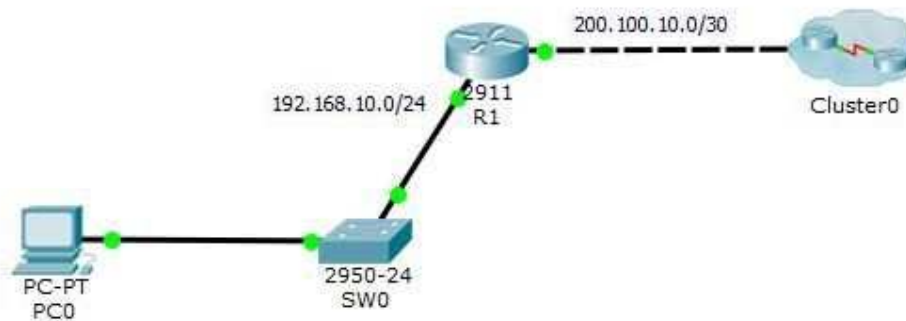
- a. Click **Sales** and click the **Desktop** tab > **E Mail**.
- b. Enter the following values into their respective fields:
 - 1) Your Name: **Branch User**
 - 2) Email Address: **branch-user@branchserver.pt.pka**
 - 3) Incoming Mail Server: **172.16.0.3**
 - 4) Outgoing Mail Server: **172.16.0.3**
 - 5) User Name: **branch-user**
 - 6) Password: **cisco**
- c. Click **Save**. The Mail Browser window displays.
- d. Click **Receive**. If everything has been set up correctly on both the client and server, the Mail Browser window displays the Receive Mail Success message confirmation.
- e. The activity should be 100% complete. Do not close the Sales configuration window or the Mail Browser window.

Step 5: Send an Email from the Sales client and the PC3 client.

- a. From the **Sales Mail Browser** window, click **Compose**.
- b. Enter the following values into their respective fields:
 - 1) To: **central-user@centralserver.pt.pka**
 - 2) Subject: *Personalize the subject line.*
 - 3) **Email Body:** *Personalize the email.*
- c. Click **Send**.
- d. Verify that **PC3** received the email. Click **PC3**. If the Mail Browser window is closed, click **E Mail**.
- e. Click **Receive**. An email from Sales displays. Double-click the email.
- f. Click **Reply**, personalize a response, and click **Send**.
- g. Verify that **Sales** received the reply.

Practical No.12

Configure SNMP



1. Enable SNMP on Router (R1)

Open the **R1** console and configure SNMP Protocol with the following router command. Before configuring SNMP, you must configure the basic configuration like, setting up **IP address** and basic **routing configuration**.

```
R1>enable
```

```
R1#configure terminal
```

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

```
R1(config)#snmp-server community R1 ro
```

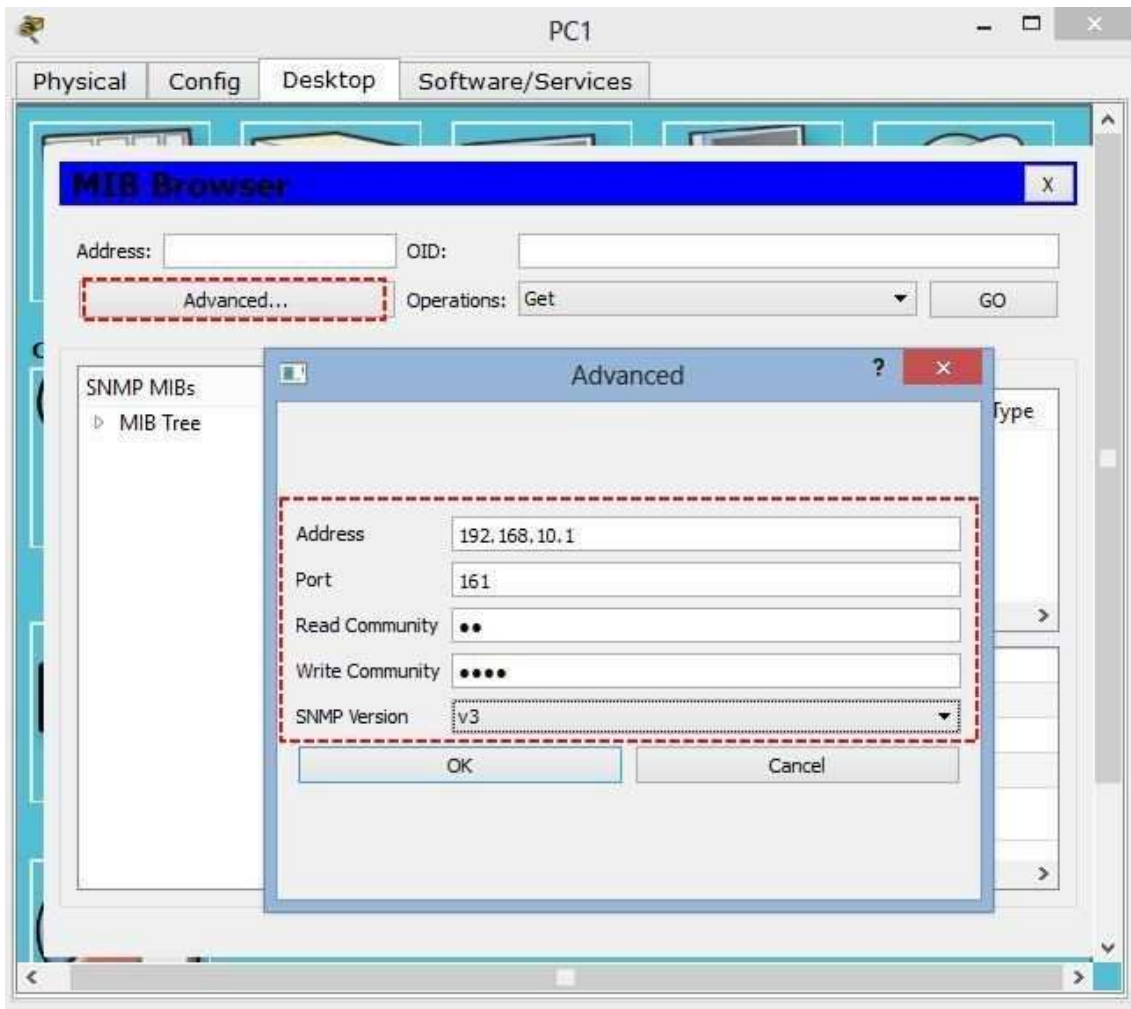
```
R1(config)#snmp-server community R1rw rw
```

```
R1(config)#
```

2. Testing SNMP from a PC

OK, the SNMP has been configured on R1 router. Now try to test it from the PC1 using MIB Browser.

Click on **PC1** and click **Desktop** tab, then open **MIB Browser**.



On the opened MIB browser page, click **Advanced** tab to open the **Advanced** page.
Enter the information like the screenshot or below table.

Address: 192.168.10.1. This is the R1 IP address.

Read Community: R1. It has taken from read only (ro) community name.

Write Community: R1rw, it is the name of read and write (rw) community.

From the **SNMP Version**, select **V3** and click **OK**.

The screenshot shows the MIB Browser application interface. At the top, there is a header bar with the title "MIB Browser" and a close button. Below the header, there are input fields for "Address" (192.168.10.1) and "OID" (.1.3.6.1.2.1.2.2.1.2), along with "Advanced..." and "Operations: Get" buttons. A "GO" button is highlighted with a red dashed box.

The main area is divided into two panes. The left pane, titled "SNMP MIBs", shows a hierarchical "MIB Tree" with the following structure:

- router_std MIBs
 - .iso
 - .org
 - .dod
 - .internet
 - .mgmt
 - .mib-2
 - .system
 - .sysDescr
 - .sysObjectID
 - .sysUpTime
 - .sysContact
 - .sysName
 - .sysLocation
 - .interfaces
 - .ifNumber
 - .ifTable
 - .ifEntry
 - .ifIndex
 - .ifDescr
 - .ifType
 - .ifMtu
 - .ifSpeed
 - .ifPhysAd...
 - .ifAdminS...
 - .ifOperSta...

The right pane, titled "Result Table", displays the following data:

| Name/OID | Value | Type |
|-------------------------|--------------------|-------------|
| .1.3.6.1.2.1.2.2.1.1... | Vlan1 | OctetString |
| .1.3.6.1.2.1.2.2.1.1... | GigabitEthernet0/0 | OctetString |
| .1.3.6.1.2.1.2.2.1.1... | GigabitEthernet0/1 | OctetString |
| .1.3.6.1.2.1.2.2.1.1... | GigabitEthernet0/2 | OctetString |

Below the result table, there is a detailed view for the selected OID (.ifDescr):

Name: .ifDescr
 OID: .1.3.6.1.2.1.2.2.1.2
 Syntax: DisplayString
 Access: read-only
 Description: A textual string containing information about the interface. This string should include the ...

At the bottom of the window, the path ".iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr" is visible.

Now on the MIB browser page expand **MIB tree** to **system** and select each value then hit the **GO** button to display the exact information on Router1.
 That's all, configure SNMP Protocol on routers or switches.

Career in networking field & Global exams in Networking

Job Titles in Networking is as follows:

- System administrator
 - Network Engineer
 - Technical Support
 - IT administrator
 - Network administrator
 - Security Database development and administration
-

Duties of Network Engineer

- Monitoring the network performance and security.
 - Perform network maintenance and ensure networks are running smoothly and efficiently.
 - Maintain system back up.
 - Support network and computing infrastructure.
 - Configuring and installing various network devices (e.g., routers, switches, firewalls, load balancers, VPN, QoS).
-
-

Recruiters

Here are the names of some renowned companies that recruits hardware and networking professionals:

- Intel Corporation
 - CISCO
 - Acer India (Pvt) Ltd
 - Dell
 - Casio India Company
 - HCL
 - TCS
 - Infosys
 - Wipro
 - Accenture
 - Many more.....
-
-

Best Computer Networking Certifications

IT pros skilled in the many areas of networking are in high demand in today's job market. Those serious about their IT careers should consider one or more of these best-of-breed networking certifications to set themselves apart from their competitors.

When it comes to the care and feeding of modern networks, there's quite a lengthy list of tools and technologies that qualified IT professionals must master – especially those who aspire to work as network administrators. In addition to the servers and clients that make up the endpoints in such environments, there's a lot of network infrastructure to worry about. This includes switches and routers (both physical and virtual), plus a raft of appliances and services, such as unified threat management (UTM), next-generation firewalls (NGFs), software-defined networking (SDN) and network functions, virtualization (NFV) components and WAN optimization, as well as spam, email, and content filtering.

Wrapping your head around all these certification options and specialties can be challenging, but knowing where to start can help. We looked at five networking certifications (in their order of appearance in the job boards table that follows) that we consider leaders in the field of networking for 2019 and beyond.

To pick our leaders, we looked at the state of networking certification, examined various market and salary surveys, and performed an informal job board survey that revealed the number of job posts across the U.S. in which our featured certifications were mentioned on a given day.

Making its first appearance on the leader board this year is the SolarWinds Certified Professional (SCP). It replaces the Juniper Enterprise Routing and Switching, Expert (JNCIE-ENT) credential. While the JNCIE remains a great credential, job board numbers for the SCP were stronger, earning it a slot in the top five. The other featured credentials include the [Cisco Certified Internetwork Expert](#) (CCIE), [Cisco Certified Network Professional](#) (CCNP), [CompTIA Network+](#) and [WCNA Certification for Wireshark](#) (WCNA).

What Are the Exams Like?

- Exams are proctored, timed, and delivered in a secure environment. Most exams last approximately one to two hours. Lab exams typically last eight hours.
- Candidates must acknowledge the [Cisco Certifications and Confidentiality Agreement](#) online at the authorized testing center prior to taking any Cisco Certification exam. Candidates will not be able to proceed with the exam and a refund will not be provided. Signing this legal agreement is required to be officially certified.
- Exams can be very challenging, going beyond simple recall and requiring candidates to engage in on the job types of problem solving. Questions include multiple-choice single answer, multiple-choice multiple answers, drag and drop, fill in the blank and simulations. An [Exam Tutorial](#) is available to demonstrate the various question formats.
- Exams other than CCIE lab exams are delivered online, with questions in sequence, and do not allow a candidate to "mark" and return to an exam question.
- Candidates will be provided with an erasable note board and marker for notes and calculations to assist them as they answer the questions.
- Exams may contain non-scored items to collect performance data on new items. Non-scored items are not used in determining the passing score nor are reported in a subsection of the score report. All non-scored items are randomly placed in the exam with sufficient time calculated and given to complete the entire exam.
- At the completion of computer-based exams, candidates receive a score report along with a score breakout by exam section and the passing score for the given exam. Lab exams are Pass/Fail and results are available online (using login) within 48 hours.
- Cisco does not publish exam passing scores because exam questions and passing scores are subject to change without notice.

Do certification exams expire?

- Exams required for CCENT, Associate, and Professional certifications are valid for three years from the date the exam was passed. Exams for the Specialist certifications are valid for two years from the date the exam was passed.
- Placing expiration dates on exams ensures that candidates starting a multi-exam certification such as CCENT, CCNA Routing and Switching, or CCDP, for example, complete the program within a specified time frame. By passing all of the required exams within the specified time period as noted above, candidates demonstrate that they are tested on current content. In situations where the period exceeds three years, candidates will need to retake those exams that expire.

What Do I Get When I Pass My Exams?

- After a candidate passes all exams required for a certification and signs the required agreements, Cisco will send a Cisco Certifications certificate identifying the candidate's Cisco Certification ID and valid certification dates. Allow 3-5 business days for electronic certificates and 6-8 weeks from the date the certificate was mailed for printed certificates.
- Certified candidates are authorized to use the appropriate Cisco Certifications logos indicating certification status. Prior to use, they must read and acknowledge the Cisco Certifications Logo Agreement. Logos can be ordered through the Cisco Certifications Tracking System.
- The [Cisco Certifications Tracking System](#) provides a record of both exam and certification status. Candidates and certification holders are expected to keep contact information up to date for receiving notifications from Cisco.

CCIE: Cisco Certified Internetwork Expert

An evergreen and high-value networking certification is the [Cisco Certified Internetwork Expert \(CCIE\)](#), which comes in several tracks. The annual production of CCIEs remains small enough that Cisco can still claim itself able to hire all of them itself, with demand and appreciation for this difficult and rewarding certification always stratospheric. Over the past few years, the Storage Networking credential gave way to Collaboration, and a Data Center credential made its debut, as well as other new certification tracks.

Although the road to obtaining a CCIE is long and hard, it is well worth the effort, time, and money. This credential opens doors to plenty of job opportunities and high salaries for networking professionals.

CCIE facts and figures

| | |
|---|--|
| Certification name | <u>Cisco Certified Internetwork Expert (CCIE)</u> |
| Prerequisites and required courses | None.
Cisco recommends eight years of relevant job experience. |
| Number of exams | <p>Every CCIE track requires both a written and lab exam. Written exam scores are valid for 18 months. Lab exams must be attempted within 18 months of the written exam. CCIE candidates may not schedule a lab exam until receiving a passing score on the written exam. Candidates must retake the written exam if they do not pass the lab exam within three years. All written exams are 90 to 110 questions, 120 minutes.</p> <p><u>CCIE Collaboration:</u></p> <ul style="list-style-type: none"> • CCIE Collaboration Written Exam 400-051 • CCIE Collaboration v2.0 Lab Exam <p><i>Note:</i> New CCIE Collaboration Written and Lab Exams will be utilized beginning on Feb. 24, 2020, though candidates' progress to date before the cutover will be</p> |

transferred to the new program.

CCIE Data Center:

- CCIE Data Center Written Exam: 400-151
- CCIE Data Center Lab Exam

Note: New CCIE Data Center Written and Lab Exams will be utilized beginning on Feb. 24, 2020, though candidates' progress to date before the cutover will be transferred to the new program.

CCIE Enterprise Wireless:

- Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR 300-401)
- CCIE Enterprise Wireless v1.0

CCIE Security:

- CCIE Security Written Exam: 400-251
- CCIE Security Lab Exam

Note: New CCIE Security Written and Lab Exams will be utilized beginning on Feb. 24, 2020, though candidates' progress to date before the cutover will be transferred to the new program.

CCIE Service Provider:

- CCIE SP Written Exam: 400-201
- CCIE SP Lab Exam

Note: New CCIE Service Provider Written and Lab Exams will be utilized beginning on Feb. 24, 2020, though candidates' progress to date before the cutover will be transferred to the new program.

CCIE Wireless:

- CCIE Wireless Written Exam: 400-351
- CCIE Wireless Lab Exam

Note: New CCIE *Enterprise* Wireless Written and Lab Exams will be utilized beginning on February 24, 2020, though candidate's progress to-date before the cutover will be transferred to the new program.

| | |
|-----------------------------|--|
| Cost per exam | Written exam: \$450 or equivalent worldwide
Lab exam: \$1,600 or equivalent worldwide
Exam rates vary based on exchange rates and local taxes (VAT, GST). |
| URL | https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/expert.html |
| Self-study materials | CCIE learning opportunities include study documents, recommended reading, test examples, training opportunities, online communities and study groups, all available through the Cisco Learning Network . |

CCNP: Cisco Certified Network Professional

The [Cisco Certified Network Professional](#) (CCNP) takes aim at platforms and products from a leading networking equipment vendor found at most communications and internet service providers, not to mention enterprises and businesses of all sizes, including government, research, and academia. It's hard to go wrong with Cisco certification nowadays, and the CCNP is its most important midrange credential across a wide variety of specialties.

Cisco offers several flavors of the CCNP: Cloud, Collaboration, Data Center, Routing and Switching (the most popular), Security, Service Provider, and Wireless. The [Cisco Certified Network Associate](#) (CCNA) is a required steppingstone to the CCNP. What usually comes after the CCNP for networking professionals could be another CCNP (different specialty), one or more Cisco Specialist certifications, or the advanced [Cisco Certified Internetwork Expert](#) (CCIE), also available in numerous specializations.

CCNP facts and figures

| | |
|---|--|
| Certification name | <p><u>Cisco Certified Network Professional</u> (CCNP) certifications:</p> <ul style="list-style-type: none"> • CCNP: Certified DevNet Professional • CCNP: Collaboration • CCNP: Data Center • CCNP: Enterprise • CCNP: Security • CCNP: Service Provider |
| Prerequisites and required courses | <p>A valid CCNA or CCIE credential is required.</p> <p>The primary CCNP certification (Enterprise) requires the core exam plus one of the concentration exams below:</p> <ul style="list-style-type: none"> • 300-401 ENCOR Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) <p>Concentration Exams:</p> <ul style="list-style-type: none"> • 300-410 ENARSI Implementing Cisco Enterprise Advanced Routing and Services (ENARSI) • 300-415 ENSDWI Implementing Cisco SD-WAN Solutions (ENSDWI) • 300-420 ENSLD Designing Cisco Enterprise Networks (ENSLD) • 300-425 ENWLSD Designing Cisco Enterprise Wireless Networks (ENWLSD) • 300-430 ENWLSI Implementing Cisco Enterprise Wireless Networks (ENWLSI) • 300-435 ENAUTO Automating and Programming Cisco Enterprise Solutions (ENAUTO) |
| Number of exams | |

Other CCNP certifications require four exams.

| | |
|-----------------------------|---|
| Cost per exam | \$300 |
| URL | https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/professional.html |
| Self-study materials | Recommended training is listed online for each CCNP Certification track. Self-study materials include books, flash cards, practice tests, and virtual and physical labs. |

CompTIA Network+

There aren't that many entry-level networking IT certifications around, probably because [CompTIA's Network+ credential](#) more or less owns this niche. Many IT and certification pundits, including us, believe the Network+ to be an important early checkbox element in any savvy IT professional's basic certification portfolio. If you're just starting out, this is a certification for you.

CompTIA Network+ is also a vendor-neutral certification and a steppingstone to a variety of more advanced networking credentials. Some vendor-specific certification programs even include it as a prerequisite.

CompTIA Network+ Cert

Network+ facts and figures

| | |
|---|--|
| Certification name | <u>CompTIA Network+</u> |
| Prerequisites and required courses | None
CompTIA A+ plus 9-12 months experience is recommended, but not required. |
| Number of exams | One exam: N10-007 (maximum 90 questions, 90 minutes) |
| Cost per exam | \$319 |
| URL | https://certification.comptia.org/certifications/network |
| Self-study materials | Exam objectives and sample questions can be downloaded from the certification page (URL listed above). Visit the CompTIA Store for study guides (\$50-plus), classroom and online training, and the CertMaster online learning tool. Study books include: <ul style="list-style-type: none"> • <i>CompTIA Network+ N10-007 Exam Cram (6e)</i> by Emmet Dulaney • <i>CompTIA Network+ All-in-One Exam Guide: Exam N10-007</i> by Mike Meyers • <i>CompTIA Network+ Study Guide: Exam N10-007</i> by Todd Lammle Practice exams are available through Certification.CompTIA.org and ProProfs.com . |

SolarWinds Certified Professional

Our sole newcomer to the top five this year is the [SolarWinds Certified Professional](#) (SCP). Headquartered in Austin, Texas, [SolarWinds](#) makes simplicity its business. At SolarWinds, businesses and IT professionals will find tools, products, and solutions to improve performance and monitoring and to solve real-world problems easily and efficiently. SolarWinds offers solutions across six areas: network management, system management, security, database management, IT help desk and the cloud.

SolarWinds currently offers a single credential, the SolarWinds Certified Professional (SCP), designed to validate a candidate's skill, knowledge and expertise in using either the SolarWinds system management or network management product portfolio. Candidates can choose to test for the SCP on either the Network Performance Monitor (NPM) or Server and Application Monitor (SAM) path. Either way, a single exam is required to earn the credential.

SolarWinds is committed to ongoing education and ensuring that SCP credential holders maintain skill currency as new products and technologies are released. To accomplish this, SolarWinds requires SCP credential holders to maintain a SolarWinds subscription and attend events and training. The subscription provides SCPs with webcasts, online training, invitations to in-person and online events, enhanced support, opportunities to study with SolarWinds experts, and more. An annual subscription fee of \$200 is required. Credentials expire after three years if a candidate fails to maintain a subscription and attend training.

SolarWinds Certified Professional

SCP facts and figures

| | |
|---|--|
| Certification name | <u>Solar Winds Certified Professional</u> (SCP) |
| Prerequisites and required courses | None listed |
| Number of exams | One exam (75 questions, 90 minutes) |
| Cost per exam | \$200
Exams administered by PSI Exams, but you register on the SCP certification site. |
| URL | https://support.solarwinds.com/Success_Center/SolarWinds_Academy/Solarwinds_Certified_Prof |
| Self-study materials | SolarWinds maintains links to various documentation and exam prep guides on the exam webpage. Opportunities and classes can be found at the SolarWinds Academy . On THWACK , candidates will find the SolarWinds IT community, library, support, blogs, webinars and more. |

WCNA: Wireshark Certified Network Analyst

Founded in 2007 by major networking geeks Gerald Combs and Laura Chappell, Wireshark University offers only a single certification but makes it worth your while. The WCNA for [Wireshark Certification](#) (WCNA) recognizes knowledge of network packet and protocol sniffing and analysis using Wireshark, as well as TCP/IP network communications, network troubleshooting, and network security. To achieve this credential, candidates must pass one multiple-choice exam, which is DoD 8570-certified.

The WCNA is good for three years, but certification holders must obtain a total of 20 continuing professional education (CPE) credits each year to maintain their credentials in good standing. These CPE credits must focus on activities related to the WCNA exam objectives (sniffing, analysis, etc.) and not be tied directly to job tasks. For example, attending a Sharkfest or Black Hat conference, or even reading the Wireshark Network Analysis Study Guide, can net some CPEs.

Along with administering the WCNA program, Wireshark University offers self-paced, instructor-led and customized training options for anyone who wants to learn about Wireshark and packet analysis. An All-Access Pass is a one-year subscription to all [WCNA for WireShark](#) training courses and costs \$699.

Wireshark Certified Network Analyst

WCNA facts and figures

| | |
|---|--|
| Certification name | WCNA Certification for WireShark |
| Prerequisites and required courses | None |
| Number of exams | One exam: WCNA-102.x Exam (100 questions, two hours) administered by Kryterion |
| Cost per exam | \$299
Practice exams available for \$29. |
| URL | https://www.wcnacertification.com/ |
| Self-study materials | Online self-paced training, instructor-led training, customized training and exam prep books available at the WCNA for WireShark Training . One site for practice exams is Udemy . |

Beyond the top five: More networking certifications

There are lots of other choices for networking professionals to investigate and pursue outside of these five. Another interesting and upcoming Open Linux Networking focused credential comes from Cumulus Networks – namely the Cumulus Networks Open Networking Professional ([CCONP](#)). While it didn't make the top five this year, the Juniper Enterprise Routing and Switching-Expert (JNCIE-ENT) remains an excellent credential for candidates interested in Juniper technologies.

Many other major networking vendors, including [F5](#) and [HPE](#), offer networking-focused credentials that ascend all the way to advanced or expert credentials. Serious network professionals will also want to check out the certifications from Avaya, [Citrix](#) and Extreme Networks.