**IPV6 (internet protocol version six)**

**Internet is a network of network through which billions of devices are connected with each other and according to one estimates the size of internet becomes double after each nine month.**

**As discussed earlier in IPV4 we have 32 bit so the total number of IP addresses that can be used are about 4.8 billion that’s are not enough to support every device that is connected to internet .**

**The 32-bit Ip addressing scheme involves a two level addressing hierarchy**

1. **Network number/prefix**
2. **Host number**

I

In order to overcomes the shortages of IPV4(internet protocol version four) adddressing schemes IPv6(internet protocol version six ) was introduced.

The main features of IPV6 includes

* Large address space because it has 128 bits unline IPv4 which has 32 bit so the total number of IPV6 addresses that can be supporte are (2^128).
* Efficient backbone routing
* Security(Ip security Is enabled by default so when two devices using IPV6(inetrnet protocol version six) communicate a secure tunnel is formed among them .
* It has better support for quality of service.



IPv6 (internet protocol version six is consisting of 128 bits) and it has eight blocks each block is consisting of 16 bits and each block is separated with other block with  **:**  Symbol.

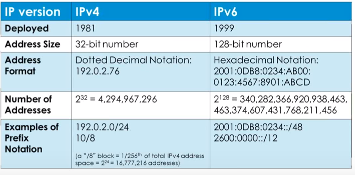


One rule that must be followed is that Leading Zeros will be removed and will be replaced with:: symbol

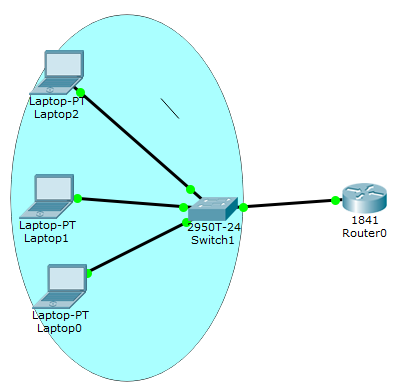
And remember it can be done only one in IPV6 address meaning that we cannot have (:: ) symbol two times.



**The Difference between IPv4 and IPv6**



**Link local address**

**Link local address is network address that can be used only inside the network it can’t be routed outside .The packets sourced from or destined to link local address are not forwarded out of layer two domains by the router. So if we are dealing with link local address these packets will remain inside the network in the above given example PC1, PC2, and PC3.**

**Types of IPV6 addresses**

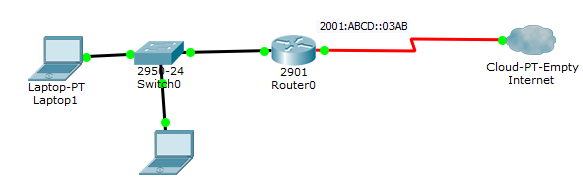
**IPV6 (internet protocol version six) has three types of addresses.**

* **Unicast –address (one to one) : A packet is delivered to only one interface.**
* **Multicast-address (one to many) : A packet destined to multiple interfaces.**
* **Any-cast (one to nearest) : A packet is delivered to nearest of multiples interfaces.**

**Unlike IPV4 (internet protocol version four) IPV6 (internet protocol version six) did not support broadcast address.**

**Global Unicast –addresses**

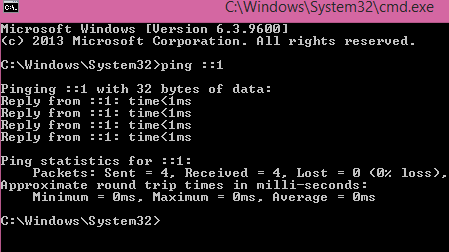
**The Global unicast address is globally unique on the internet this types of addresses starts with 2000 :: /3 .**

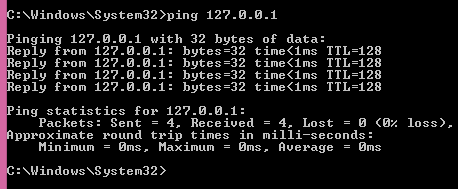


**The Global unicast addresses are assigned by ISP (internet service provider) two devices can’t have same IP address in the world.**

**Loopback address in IPv6**

**Like in IPV4 the loop back address is (127.0.0.1) in order to check the connectivity we use the command ping 127.0.0.1 to check the connectivity. In IPV6 the loopback address is 0000:0000:0000:0000:0000:0000:0000:0001 so it can be rewritten as ::1. To check your connectivity to your network interface card just ping ::1 in cmd.**



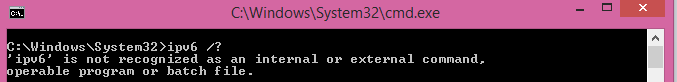


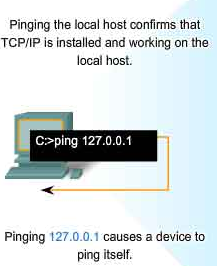
**In order to check the IPV6 (internet protocol version 6) address being used on your pc. Enter the command “ipconfig” without quote.**



**How to enable IPv6 (internet protocol version 6 ) on Windows Operating systems.**

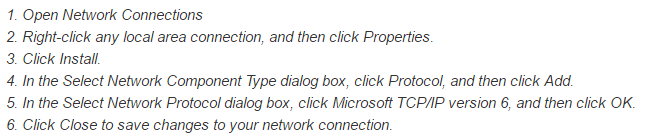
**In order to check either IPv6 (internet protocol version six) in window XP based systems is already enabled on your system type the command “ipv6 /?” in command prompt.**

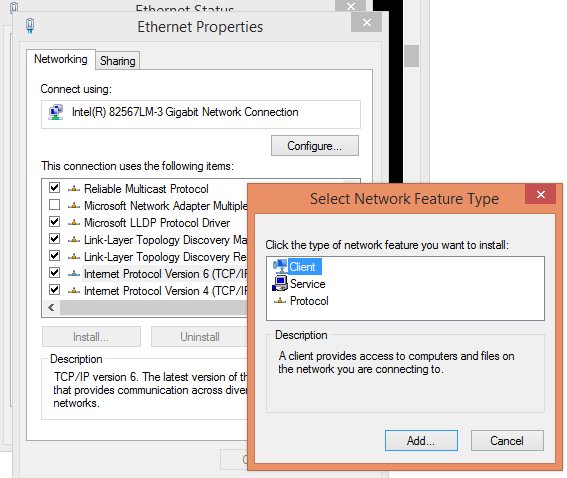




**The output shows ipv6 is not recognized because still we have not enabled IPV6 support on the PC.**

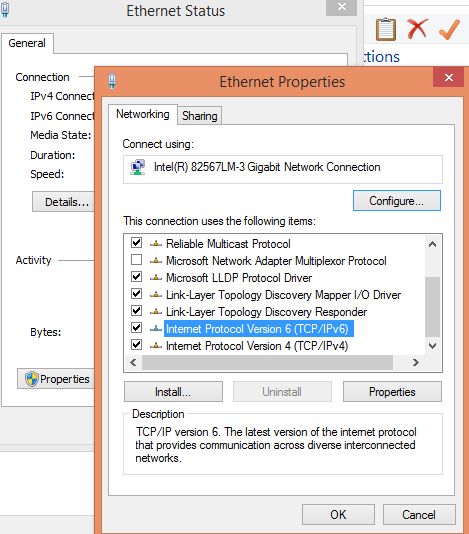
**In order to make your PC to support IPv6 (internet protocol version six) follow these simple steps**



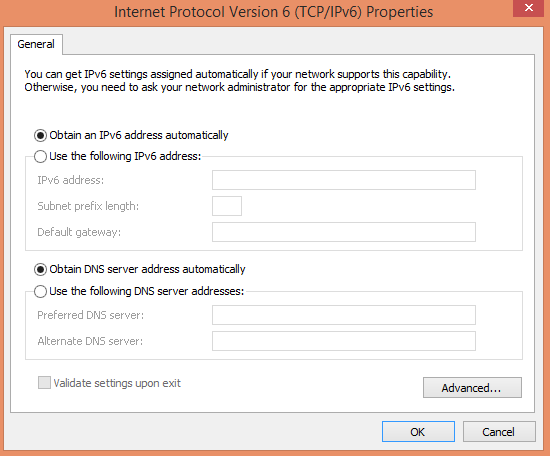


**If IPv6 (internet protocol) DHCP (Dynamic host configuration) is configured properly then follow these following steps to get the IPV6 address.**

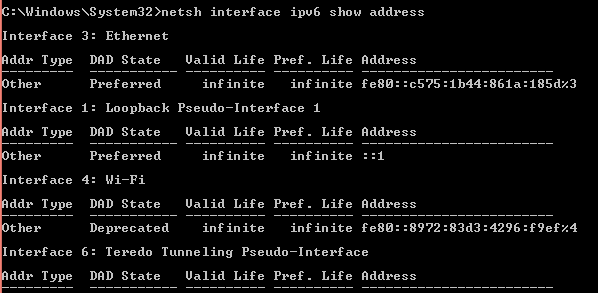
**Go to Ethernet Status then click on properties in the second window click on properties again.**



Select the Radio button “obtain ipv6 address automatically” and these addresses will be obtained from DHCP (dynamic host configuration protocol) or even can be configured manually.



**In order to get the IPv6 (internet protocol version six) information use this following command.**



**In order to get the information about the specific interface**



**Quick quiz**



**Answer: D**



**What is the usage of any cast address?**

1. For Load balancing
2. To communicate with a group of host.
3. It is same like broadcast address
4. None of Given option

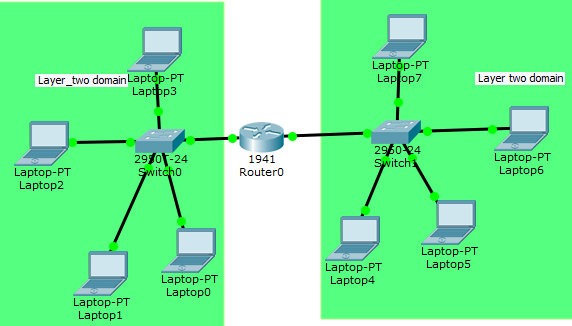
**Answer B: Any-cast is networking technique where the same IP prefix is advertised from multiple locations. The network then decides which location to route a user request to, based on routing protocol costs.**

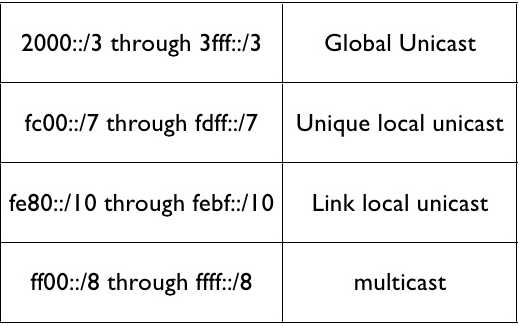


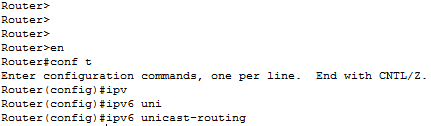
Link Local address

Link local addresses are mandatory in IPv6 (internet protocol version six) while loop back addresses are mandatory. It can be used within the context of single layer two domains Router divides layer two domain. Packets sourced or destined to link local address are not forwarded out of layer two domain by the routers.

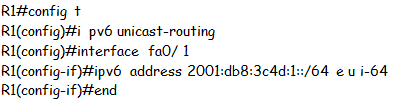
These addresses are useful for establishing the communication across the link in the absence of globally routable. Technically link local addresses are within the prefix of **FE80:: /10 .** On cisco IOS , an IPV6 enabled interface must be assigned with link local address . In Cisco routers Link local addresses can be manually assigned or they can be created by the Routers itself by using a technique known as EUI(extended unique identifier) .

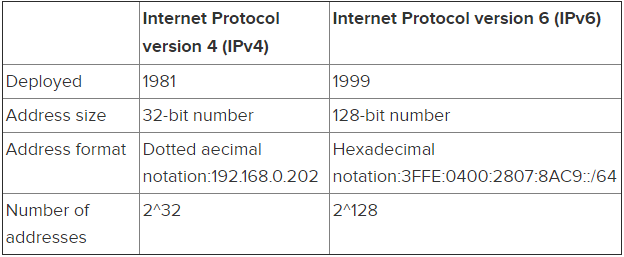


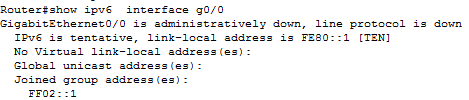


IPV6 feature is not installed by default on cisco router in order to enable the router to support IPv6 use the command “ipv6 unicast-routing” in router CLI(command line linterface).

And then in order to assign IPv6 address to interface follow use these simple steps

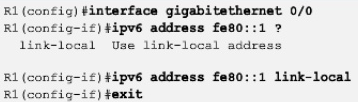




The link local address created by using this Technique can be viewed by using “show Interface fa0/1 ipv6 address”. Note after interface you have to put the respective interface number.

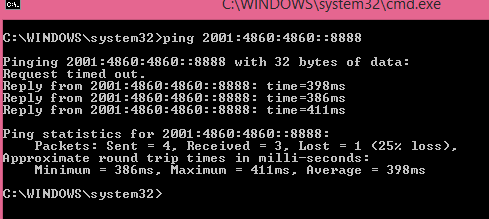
EUI (extended unique identifier) means link local address will be automatically generated or if you want to assign link local addresses from the range of

Or if you want to manually assign link-local address to all devices inside your network



**DNS (domain name system)**

Domain name system is used to convert Domain-name into IP address like in IPv4 (internet protocol version four) we usually use the public DNS of Google (8.8.8.8).Make sure you able to ping this address else DNS problem will occur . Likewise in IPV6 public DNS of Google **is 2001:4860:4860::8888.**



**DHCP (Dynamic host configuration protocol) services in IPv6**

Same like IPv4(internet protocol version four) in IPv6 enabled network we have to use the DHCP service to automatically assign Ipv6 addresses to all host connected in LAN.

But unlike IPV4 in IPV6 the DHCPV6 supports two different methods

* Stateful configuration
* Stateless configuration( also known as Stateless auto configuration SLACC)

The stateful version of DHCPV6 is pretty much the same as for IPv4. The DHCP enabled server or router will assign IPV6 address to all clients and will keep track of binding. If you are using cisco router as DHCP server this Binding can be seen by using the command “show ip dhcp binding”

DHCP (dynamic host configuration) enabled routers or server assigns IP(internet protocol ) address for a specific period and after that period client has to request again to DHCP router to assign IP address. Stateless Auto configuration is an important feature offered by IPV6 protocol. It allows various devices attached to IPv6 network to connect to internet using the **state less auto configuration** without having need of DHCP (dynamic host configuration protocol).

Quick Quiz

1. How many bits are in IPv6 address?
2. 128
3. 64
4. 32
5. 48

**Answer A**: in IPV6 we have 128 bits like (2001:0DB8:0FF2E: ABCD: 1).

1. What operating System currently support IPV6(internet protocol version six)
2. Linux
3. BSD
4. MAC
5. All of above

**Answer: D**

1. Which feature of IPv6 allows devices to assign IPv6 address to them selves
2. Stateless auto configuration
3. Stateful auto configuration
4. NDP( network discovery protocol)
5. None of the above

**Answer: A**

1. Which these of two statements are true about IPV6 (internet protocol version six) presentation.
2. The first 64 bits represent the dynamically created interface ID
3. A single interface can be assigned with multiple IPV6 addresses
4. Leading Zeros are eliminated
5. All of the above

**Answer: C**

1. What us the total number of IP addresses that can be supported by IPV6
2. 2^32
3. 2^48
4. 2^128
5. 2^64

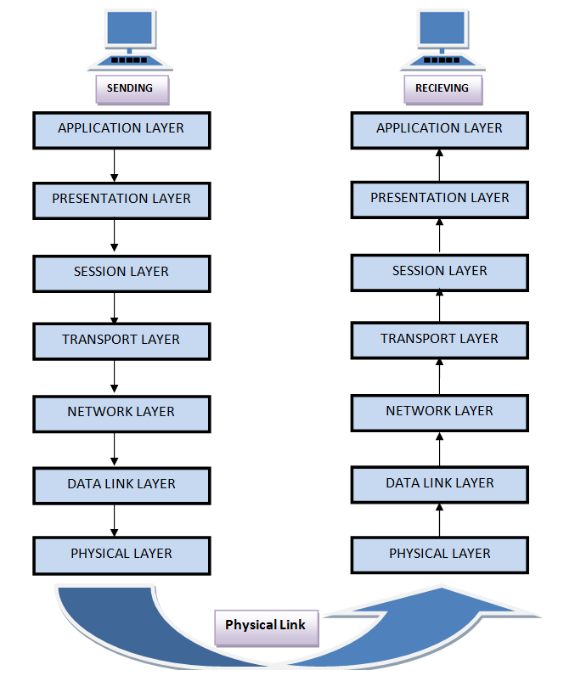
**Answer: C**

**Layer two (Data Link Layer) and Layer 3(Network Layer)devices**

**There are** billions of computer interconnected with computer network and are located over the world. So in order to ensure national and worldwide data communication, systems must follow a standard which is compatible to communicate with each other.

**In OSI (**open system interconnection model) is a conceptual model that characterize and standardizes the communication function of telecommunication or computing system.

In OSI (Open system interconnection) we have seven layer each layer has its own functionality



Layer one (Physical Layer) this layer performs the following functions

* It is lowest layer of OSI(open system interconnection model)
* It activates , deactivates , maintains the physical connection
* It converts the digital/analog data into electrical or optical signals
* Data Encoding is also done at this Layer

Layer two (Data link Layer) has the following responsibilities

* Data Link layer synchronize the information which is to be transmitted over the physical layer.
* The main function of this layer is to make sure data transfer is error free from one node to another node.
* Switches works at this layer and forwarding decision is made based on MAC (media access control) table.
* This layer is further divided into two sub-layer

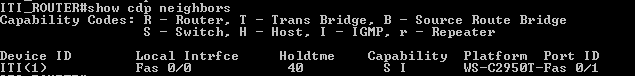
1. LLC(logic Link control)
2. Media Access control(MAC)

* Transmitting and receiving data sequentially is managed by this layer

**Logical Link control (LLC):** logical link control refers to the functions required by establishment and control of logical links between local devices on network. .

**Media Access control (MAC):** This refers to the procedure used by devices to control access to network.it is responsible for framing and de framing and collision detection.

In ipv6 enabled network we also use CDP (cisco discovery protocol) to check the layer two connectivity.

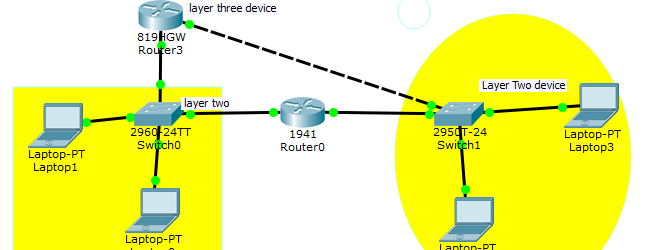


Although CDP(cisco discovery protocol) at data link layer but it also gives information about IP(internet protocol) address of connected devices which works at layer three(network layer).



**Layer 3: Network Layer**

The network layer is responsible for the followings

* It routes the signal through different channels from one to other.
* If there are multiple ways to reach the destination it the job the layer three to decide to choose which path should be taken to reach the destination
* It devices the outgoing messages into packets and assembles the incoming messages into packets for g higher levels.
* Routing is done at layer three (network Layer) in order to send packet from one network to another network Router must be there. It decides where to forward data based on routing table.
* On the router we have to configure any routing protocol that will enable router to make forwarding decision. There are two ways to configure router to use routing to make forwarding decision

(1) Static route

(2) Dynamic Route

In Static routing Paths are pre-computed by host and are loaded into routing table. The paths are fixed packets will be following that particular path. Static route is good when

* Network size is small
* Traffic load does not change variably
* Network topology is fixed and there is no need for router to perform any algorithm to determine the path.
* In dynamic routing each node computes the best path by communicating with its neighbor .Each node continuously learn the state of network by communicating with its neighbor. Path are not predefined they are determined by the router where to send the data. The example of Routing protocol includes RIP (Routing information protocol), OSPF (Open shortest path first) in IPV4. In IPv6 we have RIpng (RIP next generation) and OSPFV3 (open shortest path first version three).

**Configuring Static route between Routers**

Static route is form of routing that occurs when router uses a manually-configured routing entry rather than information from dynamic routing protocol.

(1) BY default port are shut down and in order to make the port open enter the command in configuration mode (“interface interfacee number”) and then put “no shut”.





After that have to use (**“ip route net hop address subnet mask Ip address of next Router ingoing interface”)**

**Enter the following command**

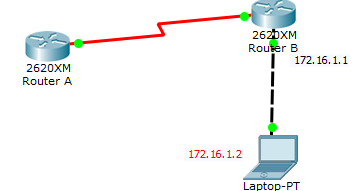


**This command will enable the Router A to redirect all traffic to (172.16.3.2) who is destined for (172.16.1.0 ) network.**

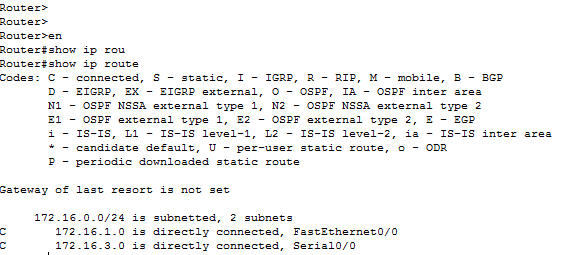
**If you want to configure Static route in IPV6 enable network same command will be used only the IP addresses will be changed .**

**Another simple way to configure static route is (“ip route next hop ip address subnet mask , outgoing interface number of Router A).**

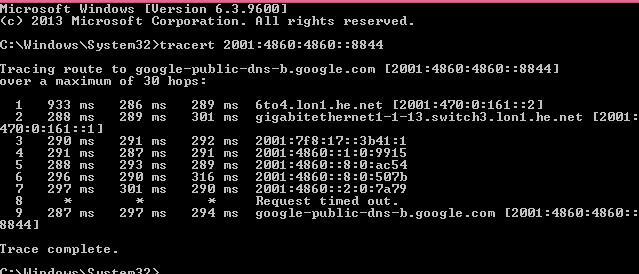




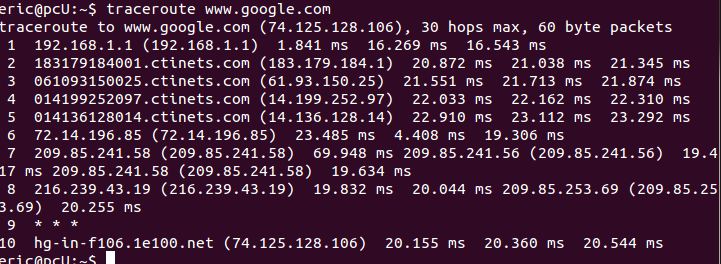
**And if you want to see the routing table enter the command “show ip route” it will list down the routing table that router is going to use in order to make forwarding decisions.**



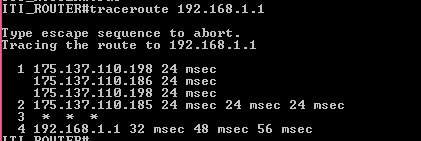
In order to determine which path is being followed by packets to reach the destination use the “tracert” command in window based system and “traceroute” in cisco Devices.



In Linux based system



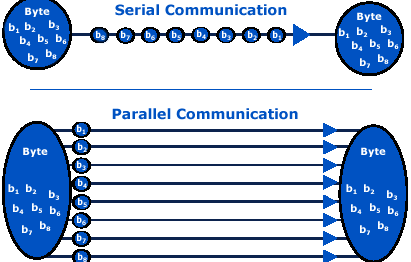
In cisco devices



Layer4: Transport layer

The transport layer has the following responsibilities.

* It decides if data transmission should be on parallel path or single path



* It receives messages from session layer above it , convert the message into smaller units and passes it to network layer.

Layer 5: Session Layer

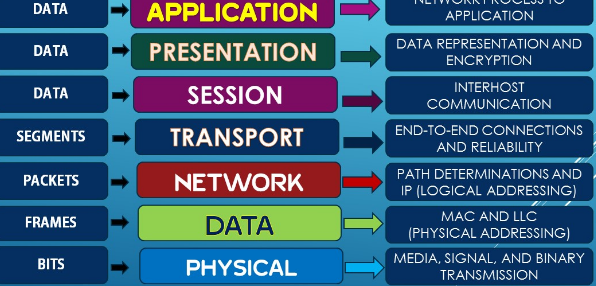
* Session Layer manages and synchronize the conversation between two different application
* It is responsible for establishing and teardown of connection

Layer6: Presentation Layer

* Presentation layer takes care that data is sent in such a way that receiver will understand the information (data) and will be able to use the data.
* It performs data compression, data Encryption m data conversion and etc.

Layer 7: Application Layer

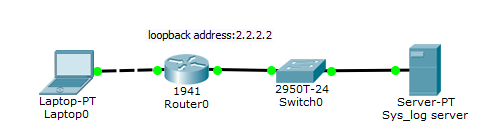
* It is the uppermost Layer in OSI( open system interconnection model)
* This layer mainly holds application program to act upon the received and to be sent data



Loop back interface in IPv4 and IPv6

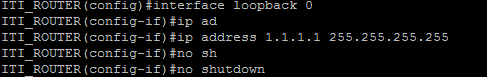
In computing localhost (loopback address) is the address is used to check the connectivity to network interface card. It is used to access the network services that are running on the host via it loopback network interface.

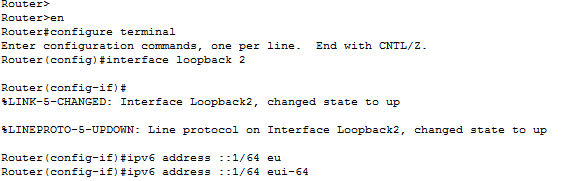
For example Sys log are used to keep track of activities going on inside the network so we can use loop back address on routers to uniquely identify each router, switch instead of IP address.



In cisco router and switches we can configure loopback in Ipv4 loop back address is 32 bit long. While in Ipv6 loopback by default is **0000:0000:0000:0000:0000:0001** and can be summarized as **::1.** In cisco router and switches one switch or router can have more than loopback address while for PCs there can be only loopback address that is (127.0.0.1) in IPv4 and in case of Ipv6 it is (::1).

In order to configure loopback address on cisco switch or router follows these basic steps





IPv4 (internet protocol version four) network standard reserve the entire 127.0.0.0/8 block for loopback purpose . That means any packet sent to one of these **16,777,214**  addresses (127.0.0.1 through 127.255.255.254) is a looped back. While IPv6 has just a single address **::1.**

Quick Quiz

1. Under what conditions static route is better than Dynamic routing protocol?

Answer: When we are dealing with simple network than static routes are better than Dynamic routes because in static routes there is no need for routers to perform any action in order to determine the path .But for complex and big network it is very difficult to configure static route.

2. Write two types of Dynamic routing protocols?

Answer: The most commonly used routing protocols in IPv4 are RIP (Routing information protocol) , OSPF(open shortest Path first) in ipv6 RIpng(Routing information protocol next generation) and OSP3(open shortest path first version three)

3. At which layer of OSI model encryption, compression is performed?

1. Application
2. Presentation
3. Transport
4. Physical
5. Network

Answer: presentation Layer

4. At which layer of OSI model Segments are used?

1. Transport
2. Network
3. Session
4. Presentation

Answer: Transport Layer

5. Which device makes the forwarding decision based on routing table ?

A. Switch

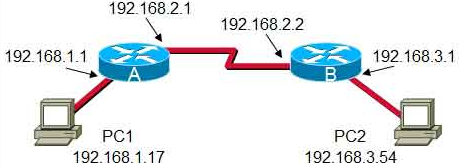
B. Router

C. Repeater

D. None of above

Answer: the router makes forwarding decisions based on routing tables

6. Host A is communicating with host B what Will be destination IP address when Packets reached at Router A?



(A) 192.168.3.254

(B) 192.168.3.1

©192.168.2.2

(D) 192.168.2.1

Answer: source and destination IP address never changes during the communication while MAC(media access control) address keep changing when they go through the routers.

(8) Which devices make the forwarding decision based on MAC (media access control) table?

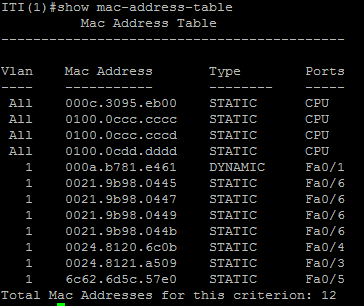
(A) Switch

(B) Routers

© Network interface cards

(D) Repeaters

Answer: Switch works at Layer two(Data link layer ) and they makes forwarding decision based on MAC address table and it can be viewed using the command “show mac-address table” in cisco switches.



(9) What the function of CDP (cisco discovery protocol)

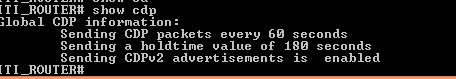
(A) It is used to check the layer two connectivity

(B) Is used to make remote access to network

© Is used to make secure web communication

(D) None of the above

**Answer: CDP works at Data link layer (Layer 2) and is used to Layer two connectivity.**



(11) Which command is used to enable IPv6 configuration on cisco devices?

1. *IPV6 unicast-routing*
2. *Show ipv6 interfaces brief*
3. *Show cdp neighbors detail*
4. *Show ipv6 route*

**Answer: IPv6 unicast-routing is a command which is used to enable ipv6 on cisco devices.**

**(12) Write down seven Layers of OSI model?**

**Answer:**

1. **Physical layer**
2. **Data link layer**
3. **Network layer**
4. **Transport Layer**
5. **Session**
6. **Presentation**
7. **Application**

**(13). OSI stand for?**

1. **Open source initiative**
2. **Open system interconnection**
3. **Open system integration**
4. **Optical storage international**

**Network troubleshooting**

Network troubleshooting is primary done by network engineer or administrators to repair or optimize the network. It is generally done to recover and establish network or internet connection on end nodes or devices. Network troubleshooting can be done manually or automatically by using network Diagnostic tools.

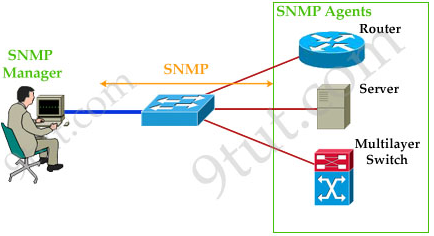


As a Good system administrator it is necessary to keep track of activities inside the network so in case if someone manages to penetrate inside the network system must be able to track it.

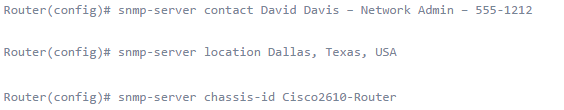
**SNMP (simple network management protocol)**

**The** simple network management protocol is a necessary toll for every network administrator it is the popular way to monitor the network performance of network devices including cisco routers, switches and PCs that are located inside your network. With an SNMP management station, you can graph the performance of network devices.

Further these devices can send alerts (trap) to management station if they found any unusual activity going on.



Once SNMP (simple network management protocol) is enabled on cisco Router or switch you may use any network monitoring tool like **CACTI** to see the flow of information and much more.



Next step is to configure SNMP so that it can be monitored by NMS(network management system). In order to use SNMP we have to create **community String** that as a password.

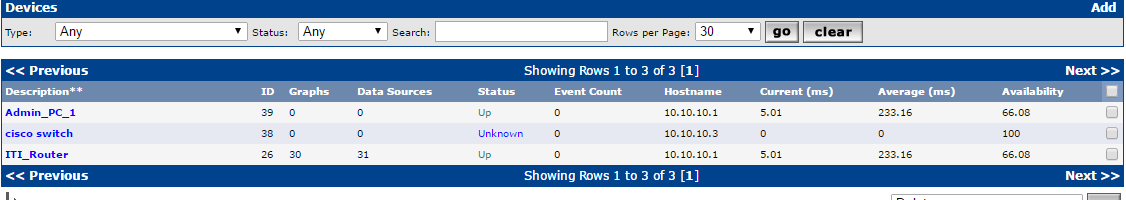


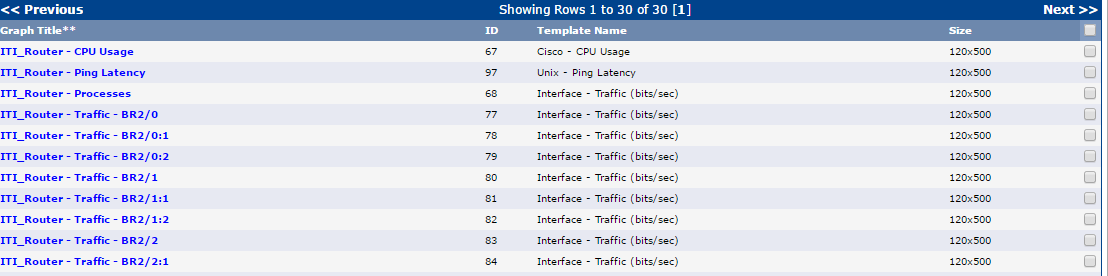
And then in order to send the notification to remote host the IP address of that host will be configured as.



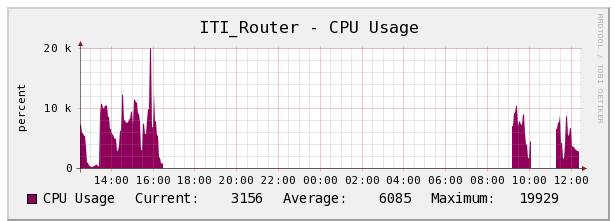
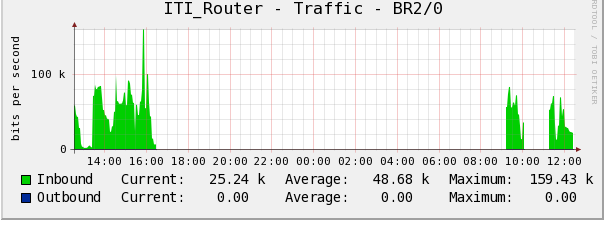
By enabling this all SNMP notification will be sent to **192.168.1.23**  host.

In CACTI now we can add The router that has be configured to send SNMP notification make sure you are using the right IP address of remote host that is running CACTI in this case it is **192.168.1.23.**



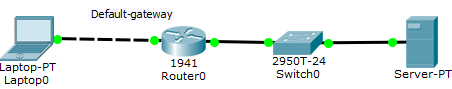
Following Graphs can be found by just clicking of devices that is added to use SNMP.

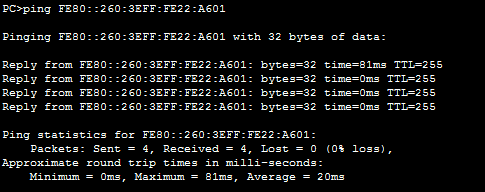
For example the CPU usage and traffic that is coming and going out looks like.



Checking connectivity to Default-gateway

Same like IPv4 network in IPv6 it is always good practice to check the connectivity to default-gateway .A default gateway is a point that acts as entrance to network and route the traffic of network station to outside network it must be configured properly in order for systems to communicate outside the network.



 And this connectivity can be checked by pinging from host to default-gateway Ip address.

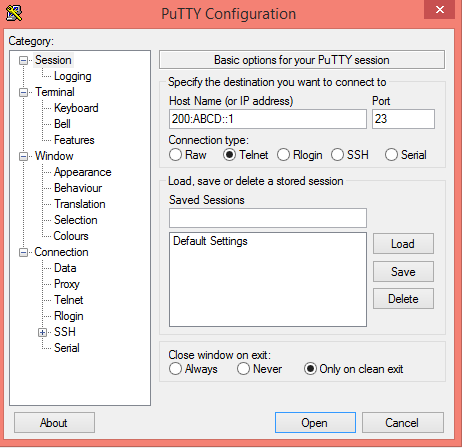
Making Telnet Access from Router

Same like IPv4 networks in IPv6 (internet protocol version six) telnet access can be made to remote access and to do that we can use command prompt (in window based operating system) Terminal(in Linux) ,CLI(command line interface in Cisco) and Putty. The procedure is same like IPv4 in the command line enter the command “**telnet ipv6 address”**



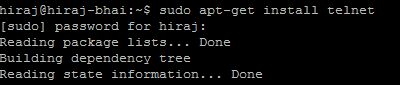
In case if you want to make telnet access from putty just put the IPV6 address of device with whom you want to make telnet connection and also from Linux terminal telnet access can be made.

In order to use the telnet services on cisco router or switches they must be enabled first the procedure will be same as discussed in previous chapters for Ipv4 (internet protocol version four)

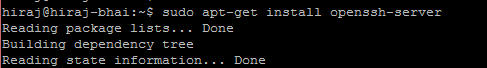


In order to enable telnet on Linux based system Go to terminal and enter the following command

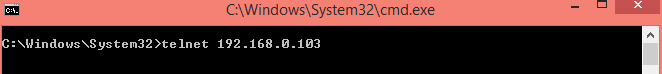
“Sudo apt-get install telnet” this command will install the telnet on the system and will enable the system to use the Telnet services.



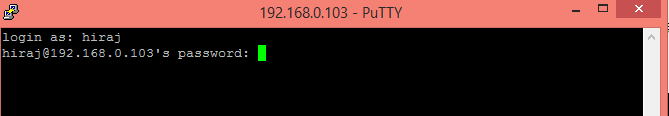
Or if you want to use the SSH (secure shell) services on Linux based system it can be enabled by entering these following command .

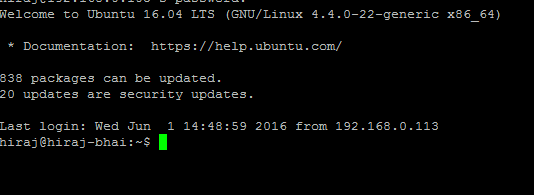


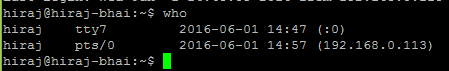
Once Telnet or SSH access has been enabled on Linux based operating system you can make remote access to the PC using any terminal and can install, uninstall , or can make changes remotely.



After making telnet or SSH connection it will ask about user name and password just provide the information and connection will be established.





If you are the one who is managing the network you must be able to keep track of who is having access to your Linux based Operating system or on cisco switch and Router. It can be checked by entering the “who” command. Thus by getting the information about devices that are having access these Devices can be blocked if they are un-authorized.

Domain Name system in IPv6

So with much information to be considered it is also import to consider DNS (domain name system) in IPv6 as in IPv4 if it is not properly configured you will not be able to have internet access because domain names will not be converted into IP addresses. There are two types of DNS server

1. **Primary DNS server**

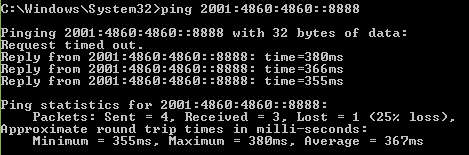
Primary DNS (domain name servers) reads data from the domain zone from a file located on the web server of hosting account. This server usually also sends information to secondary servers.

1. Secondary DNS server

Secondary DNS servers are also known slave server or simple slave receives zone data from primary server automatically.

A Secondary server can be configured inside the network all devices that are connected inside the network will make DNS query to that server that is located inside thus it will increase the efficiency and performance of network.

In order to check your connectivity to **Google DNS server** just use this command.

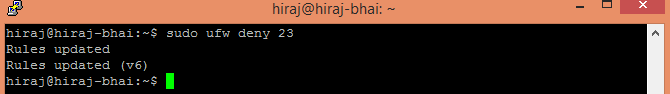


**Firewall in Linux based Operating System**

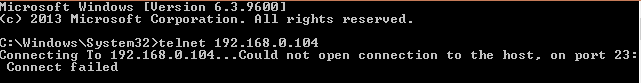
Same like in window based OS (operating system) in Linux based operating system it is always recommended to use Firewall in order to block un-intended traffic or to block certain type of traffic.in Linux UFW(un complicated firewall) is used it provides much more user friendly framework for managing net filter and command-line interface for working with firewall.

Other than that you can use command line as well some GUI(graphical user interface) that make its incredibly simple to use.

For example if you want to block telnet access to your Linux device enters the following command.



23 is port number that is used for Telnet access while port number 22 is dedicated for SSH connection. As from the above syntax Telnet is denied if you try to telnet the device connection will be refused by the remote host.



If want to allow Telnet access to remote host enter this command



The other basic available arguments for UFW (UN complicated firewall includes)

* Allow
* Deny
* Reject
* Limit

In order to enable UFW (uncomplicated fire wall) on your Linux device enter “Sudo ufw enable” without quote.



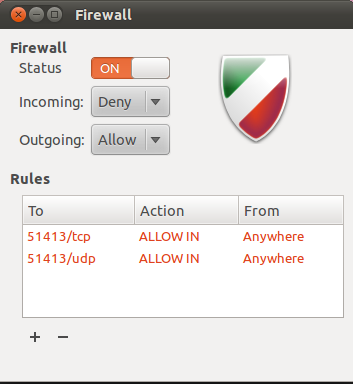
Or it can be disabled by the “Sudo ufw disable” command.



**GUFW is the GUI (graphical user interface) version of UFW that**  can also be used if you are newbie to Linux OS(operating system) . In order to install the GUFW just use this simple command

“**Sudo apt-get install gufw”**





Quick Quiz

1. SNMP is a protocol that is used for network management and it stand for?
2. **Simple network management protocol**
3. **Simply not my problem**
4. **Standard news management packet**
5. **Simple network message protocol**

Answer: A... SNMP stand for simple network management protocol

1. Which command is used to check how many connections are open on Linux machine?
2. Who
3. Whom
4. Sudo apt-get install
5. None of the above

The command **who** is used to check the connections.

1. In window based Operating we use **ipconfig**  to get IP address information in Linux which command is used to perform the same function?

1. Ifconfig
2. Ipconfig
3. Nslookup
4. Route

Answer: in Linux based Operating system “ifconfig” is interchangeable with ipconfig.

1. Can we enable Telnet and SSH both services on one device?
2. Yes
3. NO

Answer: Both services can be used at the same time.

1. Which command is used to install telnet on Linux?
2. Sudo apt-get install telnet
3. Sudo apt-get install talnet
4. Sudo apt-get add telnet
5. Sudo apt-get purge telnet

Answer: **Sudo apt-get install telnet**

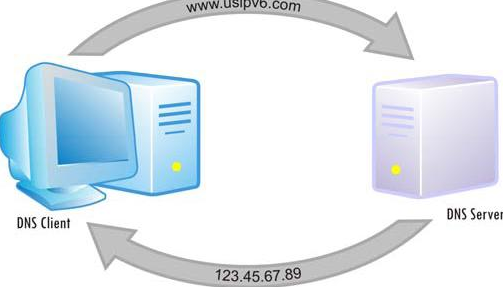
1. Which command is used to enable SSH service on Linux based operating system?
2. Sudo apt-get install openssh
3. Sudo apt-get install openssh-server
4. Sudo apt-get install SSH
5. None of the above

Answer: Sudo apt-get install openssh-server

1. Write down two types of DNS (Domain name system)?
2. Primary DNS
3. Secondary DNS

1. Write down three Differences between Primary and secondary DNS (domain name system)?

|  |  |
| --- | --- |
| **Primary DNS** | **Secondary DNS** |
| It is Authoritative server for the zone. | It is backup DNS server. |
| It can read/write copy of DNS server | It can only read the copy of DNS server |
| One DNS server can have one primary DNS server | There can be up to 255 secondary DNS servers. |



1. Write dow the three advantages of OSI(open system inter conenction model) ?
2. It prevents changes from one layer to take affect on other layers
3. Standardrization of network components allows multiple vendor development
4. It allows different types of hardware and software to communicate with each other.
5. **Write down the advantages of each Layer in OSI model ?**



**Build in features of IPV6 (internet protocol version six)**

* **Very large address space**

As IPV6 (internet protocol version six) uses 128 bits so the total address spaces is much higher than IPv4 because in IPV4 the total number of bits =16.

Remember The format of IPV6 address : **Eight set of four hexadecimal numbers**  if you have successive filed of zeros in IPv6 they can be replaced with (**::)**

* **Security**

In IPV6 (internet protocol version six) IP-sec is build-in so the link between devices using iPV6 secure tunnel is formed without any configuration.

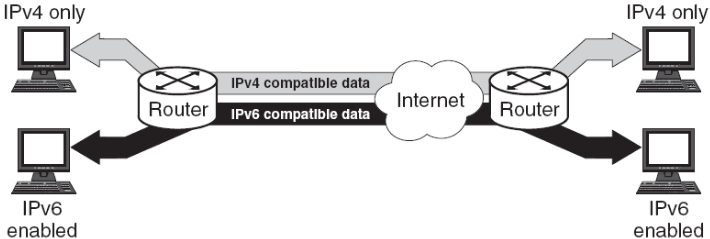
* **Stateless and stateful address configuration**

IPV6 supports both stateful address configuration such as DHCPV6 and stateless auto configuration where IP address is generated by it own.

* **Transition capabilities**

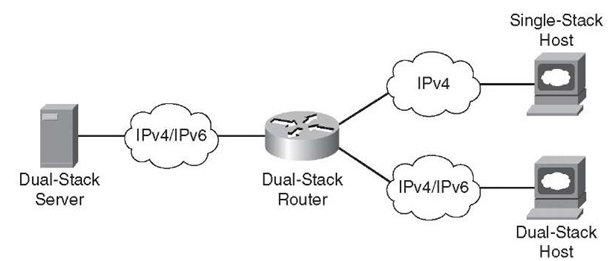
There are cases where there is need for IPv6 packets to travel on IPv4 network and migration between each other. One method is dual stack that allows devices to run both IPv4 as well IPV6 at the same time. Second method is by forming tunnel in a way that IPv6 packets will be encapsulated in Ipv4 packets and they can travel on Ipv4 network such as internet.

Cisco supports a third method referred as **Network address translation-Port translation(NAT-PT).**



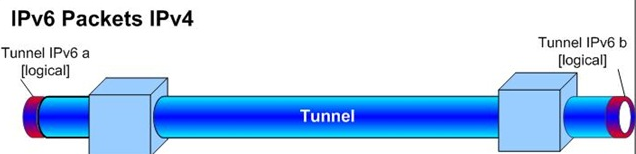
**IPV4 to Ipv6 Transition Options**

* **Dual stacking**

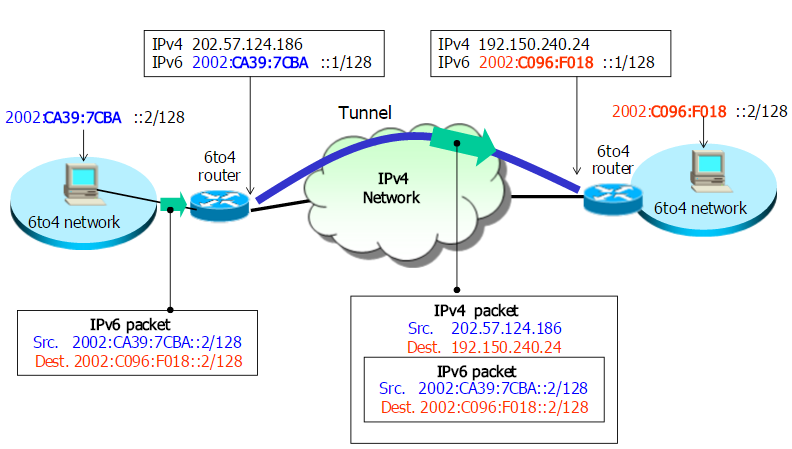
 Devices such as PC’s and routers run both IPV4 and IPv6 and thus have two set of addresses.

* **Manual IPv6-over-IPv4 (6 to 4)**

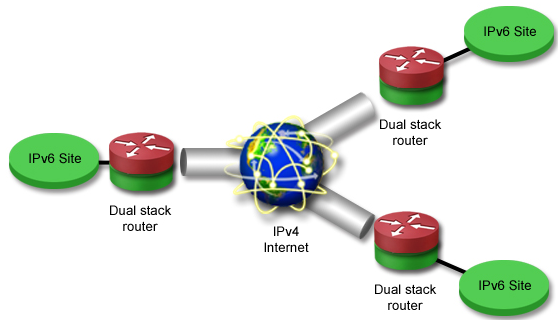
In this method IPV6 packets are tunneled across an IPV4 network by encapsulating them in Ipv4 network. It requires routers configured with dual –stack.



* **Dynamic 6 to 4 Tunneling**

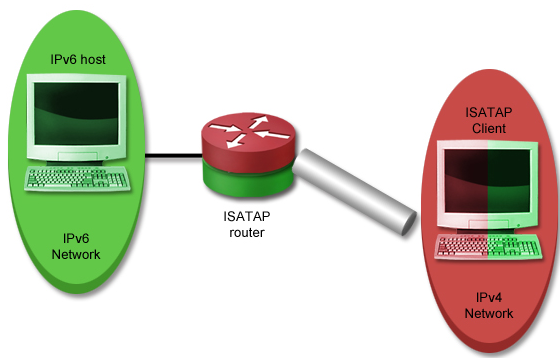
This method allows IPv6 (internet protocol version six) localities to connect IPV6 localities across IPv4 backbone such as internet automatically .This method applies a unique IPV6 prefix to each locality without having to retrieve IPV6 addressing information from addressing registries or ISP(internet service providers)

**During the transmission of packets the packets begins as a normal ipv6 packet with IPv6 source and destination address and these addresses never changes.**



**Intra –site automatic tunnel addressing protocol (ISATAP)**

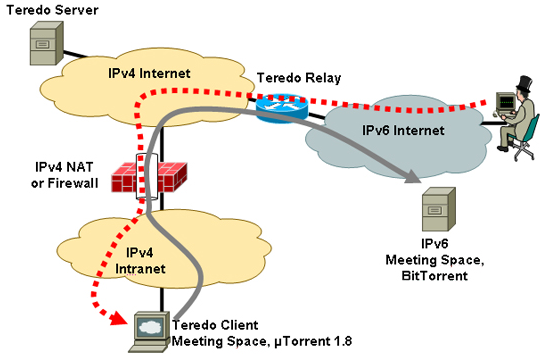
Uses virtual links to connect IPV6 localities together within a site that is primarily using IPv4. Boundary Router between the two addressing types must be configured with dual stack.



**It does not require the underlying IPV4 network infrastructure to support multicast.ISATAP defines a method for generating a link-local IPV6 address from an IPv4 network and a mechanism to perform Neighbor discovery protocol on top of IPV4.**

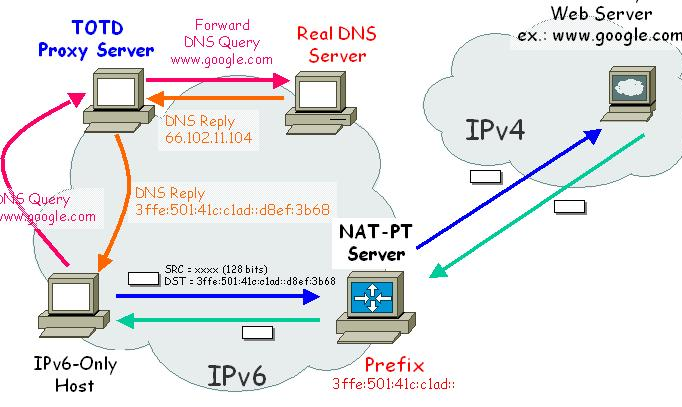
**Teredo tunneling**

Instead of using routers to tunnel the packets in Teredo tunneling has the hosts perform tunneling. It requires the host to be configured with dual stack. It is commonly used to move packets through an IPV4 address translation device.



**NAT –Proxying and translation (NAT-PT)**

**Hs an address translation device translate address between IPv6 and IPv4 network and vice versa.**



**Quick Quiz**

1. **IPV6 address are ---------------- bits in length**
2. **128**
3. 64
4. 32
5. 1

**Answer :128**

1. Which of following best describe any cast address?
2. One to all
3. One to many
4. one to one
5. single interface

**Answer: one to one**

1. Which of the following is Global address?
2. 2001:FFFF:ABCD::1
3. FE80::1
4. ::1
5. None of above

**Answer: A(2001:FFFF:ABCD::1)**

1. Which IPV6 command must first be entered on cisco router to enable IPv6 ?
2. Ipv6-unicast routing
3. Ipv6 address
4. Ipv6 support enable
5. Router ipv6-unicast

**Answer: A (**ipv6 unicast-routing)

1. What are the three IPV6 transition mechanisms?
2. **6to 4 Tunneling**
3. **VPN Tunneling**
4. **Teredo tunneling**
5. **ISATAP tunneling**

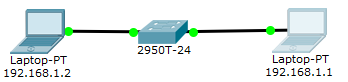
Answer:A,C,D

1. ISATAP stand for?

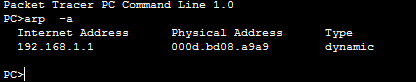
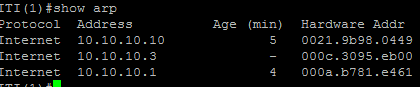
Answer: **intra site automatic tunnel address protocol**

**IPv6 Neighbor discovery protocol (NDP)**

Internet protocol version six (IPV6) Neighbor discovery protocol is a set of messages and processes that determine relationship between neighboring nodes in IPV6 networks. In IPV4(**internet protocol version four)** we use the ARP(Address resolution protocol) in order to map between MAC(media access control) and IP address .

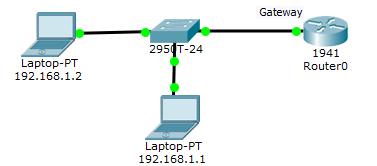


In order to determine the ARP (address resolution protocol) table on CISCO router, switches o enter the command “**show arp” without quote.** On PC’s use **“arp –a” command.**

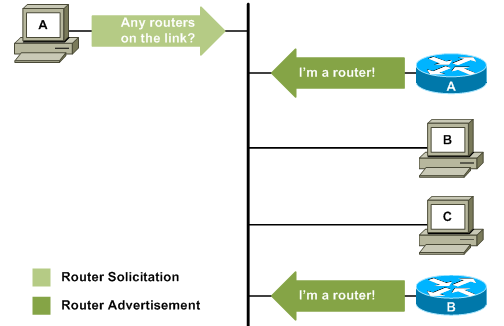


IPV6 (internet protocol version six) did not support Arp (Address resolution protocol). So ND (network discovery) protocol replaces ARP (address resolution protocol), ICMP (internet control message protocol) router discovery, and ICMP redirect message used in IPV4 networks.

IPV4 hosts must rely on manual configuration or DHCP (dynamic host configuration protocol) to provide the address of default-gateway.

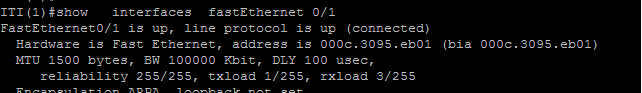


**But IN IPV6** networks hosts can automatically locate default routers on the links. This is accomplished through the use of two ICMPV6 (**internet control message protocol version six)** messages **Router solicitation and Router advertisement.** when first joining the link IPV6 host multicast router solicitation to all the routers multicast group and each router active on the link responds by sending router advertisement with its address to all nodes that are inside the multicast group.

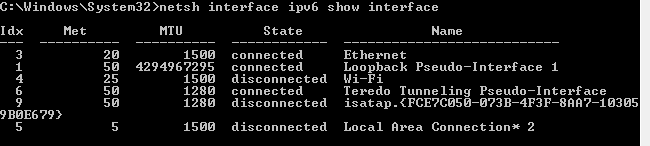


MTU (Maximum transmission limit): **MTU** is the number of bytes in largest IPv6 packet that can be sent of the link.

Because MTU (maximum transmission unit) also includes header and trailer so MTU is not same as frame size of link.



In order to get the information the actual interface ID’s and MTU (maximum transmission unit) on your PC.



**Quick Quiz**

**(1) What is the total address space in IPv6 ?**

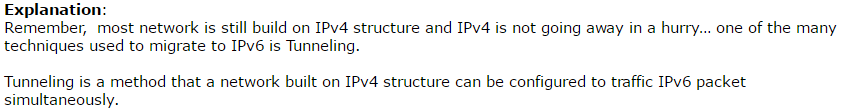
1. **2^32**
2. **2^64**
3. **2^128**
4. **2^16**

**Answer: C**

**(2)** In practical IPV6 application, the encapsulation of IPV6 packets inside IPv4 packets is called ?

1. Tunneling
2. Hashing
3. Routing
4. NAT

Answer: Tunneling



(3) 