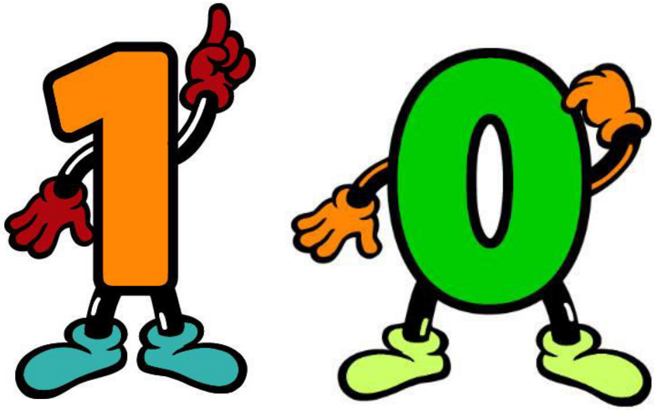
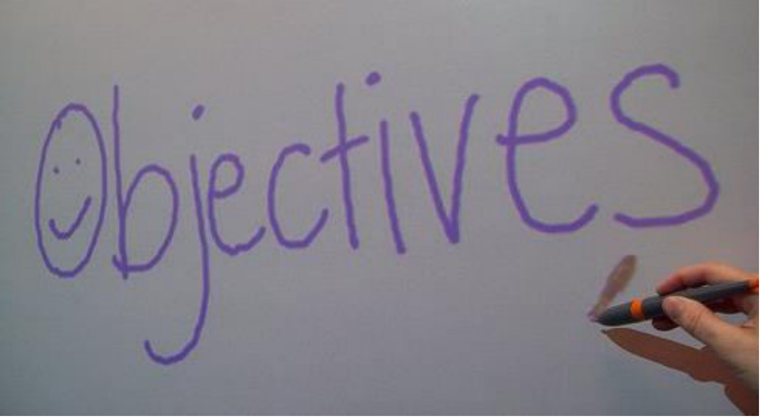


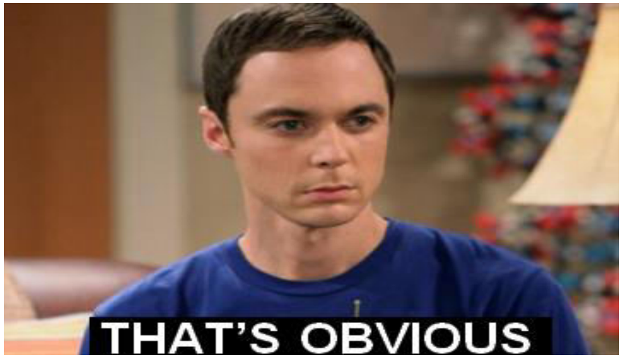
Domain Name Server (DNS)
Dynamic Host Configuration Protocol (DHCP)
Automatic Private IP Addressing (APIPA)
Network Address Translation (NAT)
Ports



1. DNS (Domain Name Server)
2. DHCP (Dynamic Host Configuration Protocol)
3. APIPA (Automatic Private IP Addressing)
4. NAT (Network Address Translation)
5. Ports

IP protocol connects computers based on their IP address (212.123.45.34)

212.123.45.34 is not www.cnn.com



If all the IP protocol cares about is IP addresses, where do these domain names come from?

e.g. www.cnn.com, server, PC1

www.cnn.com, server, PC1 do not mean anything to the computer.
Your computer only cares about the IP address

“BUT”

You care about www.cnn.com

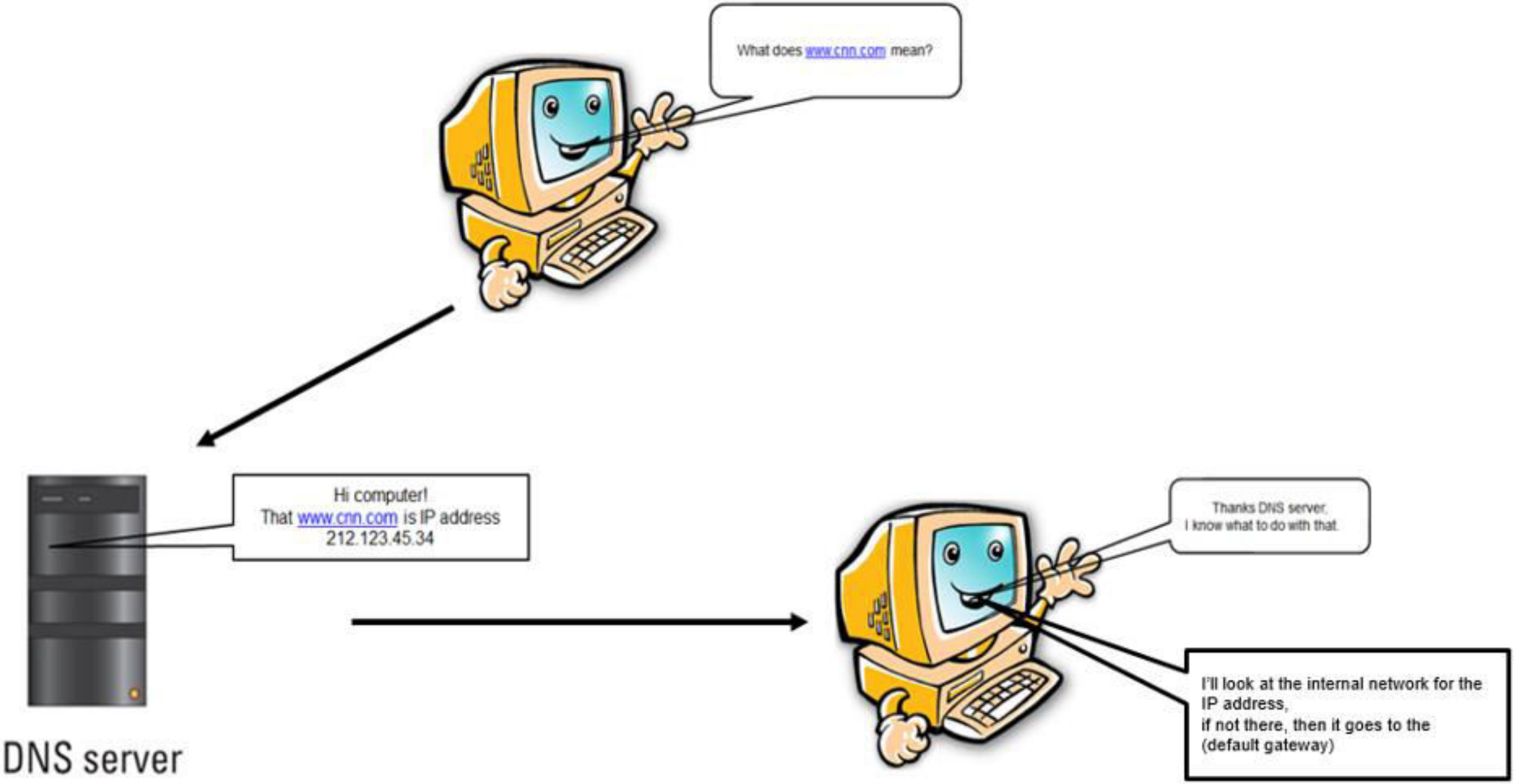
DNS (Domain Name Server) to the rescue

Domain Name System (DNS)

Server service that maps domain names to IP addresses e.g. 212.123.45.34 = www.cnn.com

(Humans can’t remember IP addresses)

Your computer will take cnn.com, goes and talk to the DNS server and asks it



What does www.cnn.com mean?

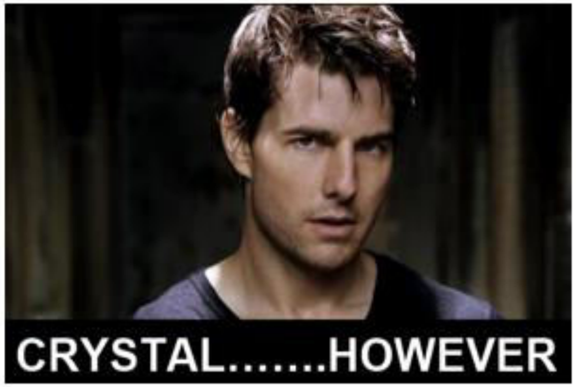
Hi computer!
That www.cnn.com is IP address
212.123.45.34

DNS server

Thanks DNS server,
I know what to do with that.

I’ll look at the internal network for the IP address,
if not there, then it goes to the
(default gateway)

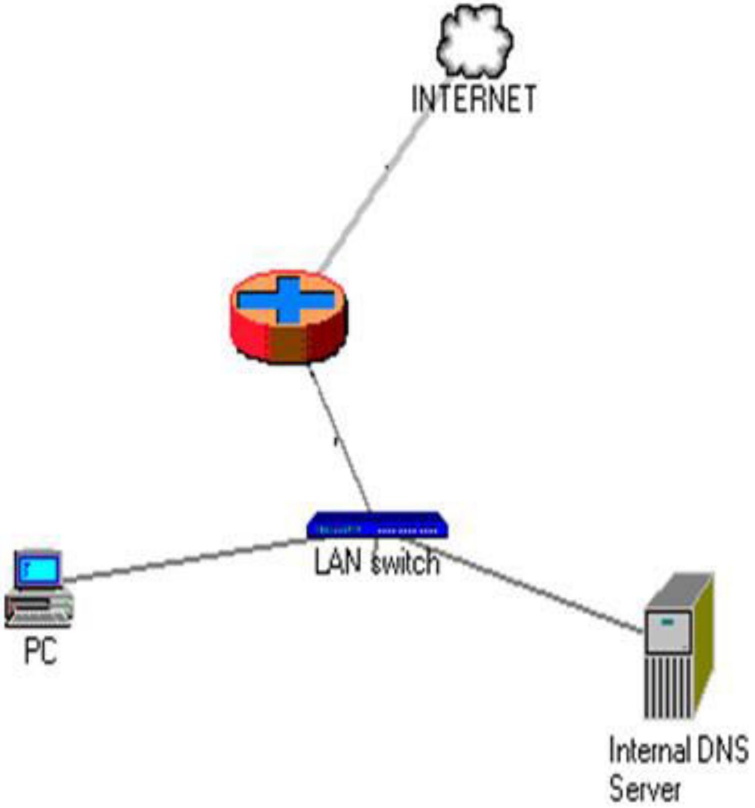
DNS maps these domain, computer names to the IP addresses



You can bypass a DNS lookup by entering the IP address

Local DNS server sitting in your building, only has records for the computers in your building.

It does not have the records for all the computers or websites out on the Internet.



When you want to access www.cnn.com, you go though the switch and that will go to you local DNS server.

If the local DNS server can not find the host/domain name in its records, it will have a DNS that it should look for.

Local DNS server has tables that have Host Names → IP Addresses

Has it’s own DNS servers that it will go query if there is no information within its tables

No single DNS server knows all the names and matching IP addresses

But

The information is distributed across many DNS servers.

So

DNS servers of the world work together

Forwarding queries to each other, until the server that knows the answer supplies the desired IP address information.

DNS is only 1 of the services that you use on a modern TCP/IP network

DHCP (Dynamic Host Configuration Protocol)

Dynamically assign IP addresses to client computers when they connect to the network

All computers/devices on a TCP/IP network require an IP address

Without an IP address, it can not receive communication and can not talk to anybody

↓

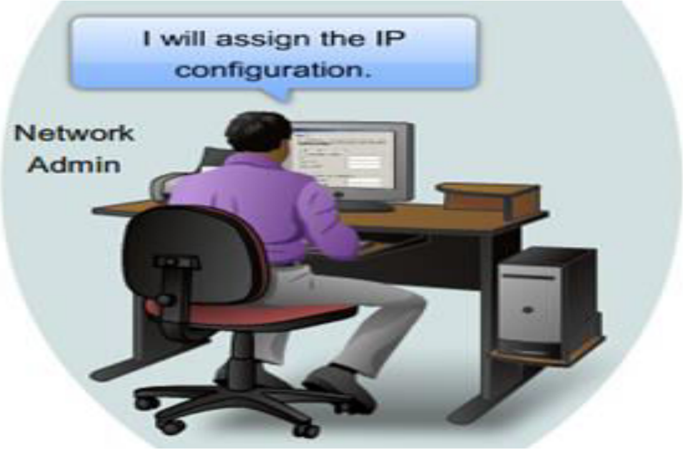
IP address can be configured manually or assigned automatically by another device

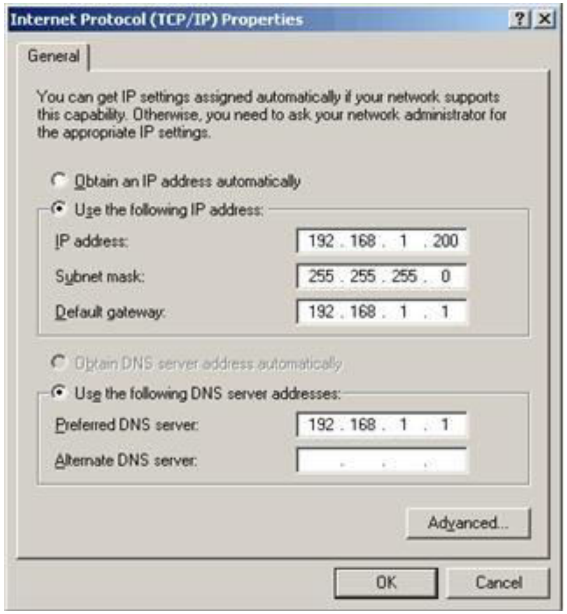
You opened the network configuration control panel and added in the IP address, SM, DG, DNS manually

Manual Configuration or Static Addressing

Values are entered into the computer via the keyboard

Static address and is permanently assigned to that device e.g. printer, server




Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 200

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

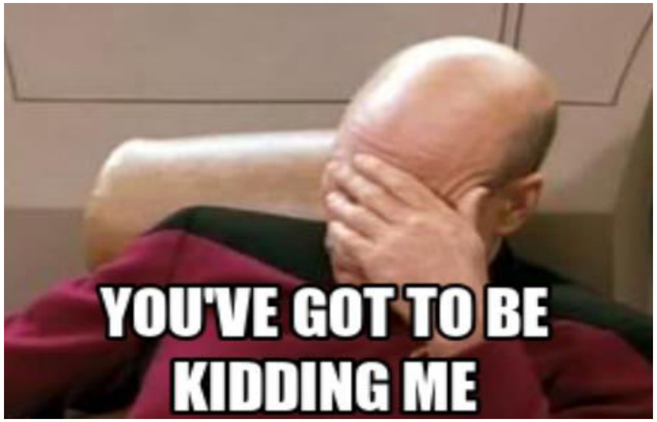
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 1

Alternate DNS server: . . .

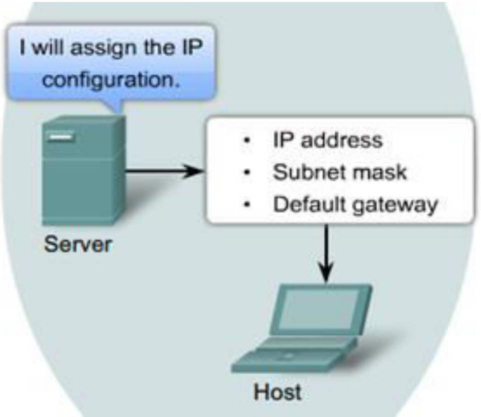
I have 500 computers that you need to configure manually

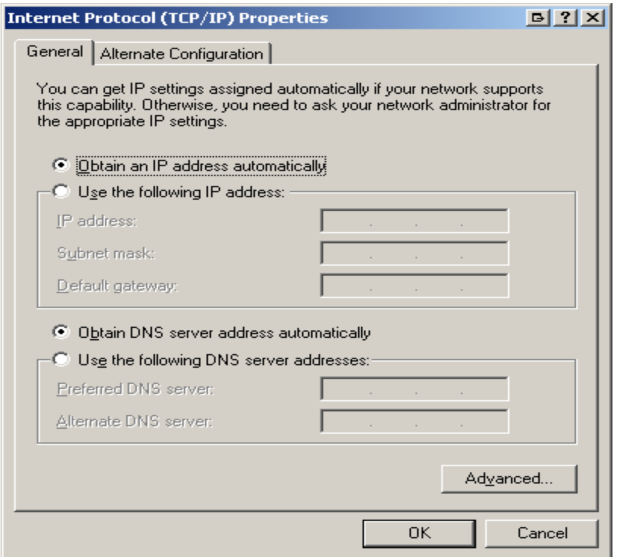


DHCP (Dynamic Host Configuration Protocol)

Dynamic Host Configuration Protocol (DHCP)

As soon as you connect your computer/printer into the network you are automatically given TCP/IP details via
DHCP server device (even a small router) located on the LAN




Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

TCP/IP details = IP address + SM + DG + primary and secondary DNS

IP address will be given dynamically whereas SM, DG and DNS Server (s) will be static
(plug the values into the server once and it will give that same info to all client computers)

DHCP allows **both** the permanent assignment of host addresses & the temporary lease of IP addresses.

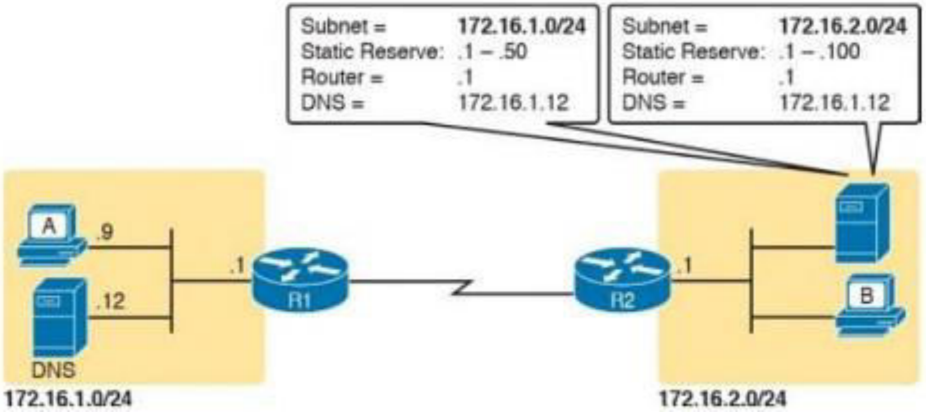
With these leases, DHCP can reclaim IP addresses when a device is removed from the network

↓

Image shows the concept behind the preconfiguration on a DHCP server for two LAN-based subnets, 172.16.1.0/24 and 172.16.2.0/24.

For each subnet, the server defines all the items in the list.

In this case, the configuration reserves the lowest IP addresses in the subnet to be used as static addresses.



Subnet =	172.16.1.0/24
Static Reserve:	.1 – .50
Router =	.1
DNS =	172.16.1.12

Subnet =	172.16.2.0/24
Static Reserve:	.1 – .100
Router =	.1
DNS =	172.16.1.12

Router configuration can be a single command on many of the router's LAN interfaces, which identifies the DHCP server by its IP address.

OR

Router acts as the DHCP server

DHCP client does have knowledge of the DHCP protocol

So the client can use that protocol to 1) Discover a DHCP server and 2) Request to lease an IPv4 address

↓

DHCP process to lease an IP address uses the following 4 messages between the client and server

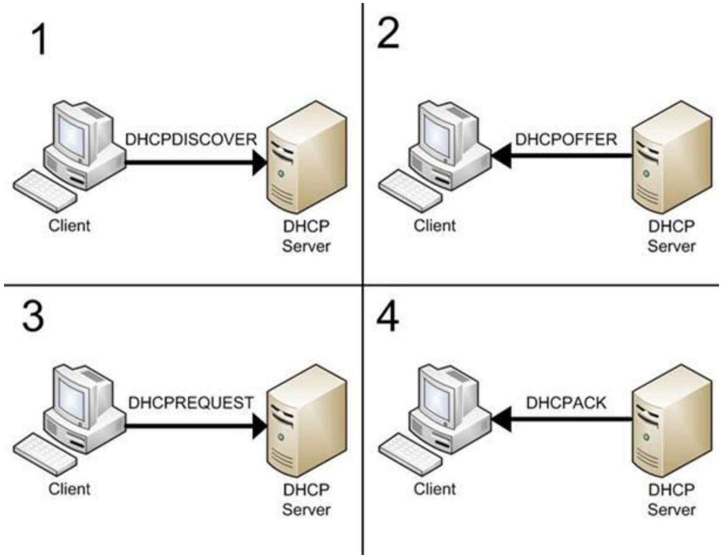
↓

Discover: Sent by the DHCP client to find a willing DHCP server

Offer: Sent by a DHCP server to offer to lease to that client a specific IP address (and inform the client of its other parameters)

Request: Sent by the DHCP client to ask the server to lease the IPv4 address listed in the Offer message.

Acknowledgment: Sent by the DHCP server to assign the address, and to list the mask, default router, and DNS server IP addresses



When you connect to the network, your computer will send a request to ask for an IP address
A **DHCP Discover** signal which says “I need an IP address, who can give me one”

↓

DHCP server hears the DHCP discover request & sends a **DHCP offer**
(DHCP offer = IP address, SM, DG, DNS)

↓

Client then sends a **DHCP request** saying ‘Thanks’ for all that stuff, I’ll keep it

↓

DHCP sends back a DHCP acknowledgement saying ‘okey dokey’

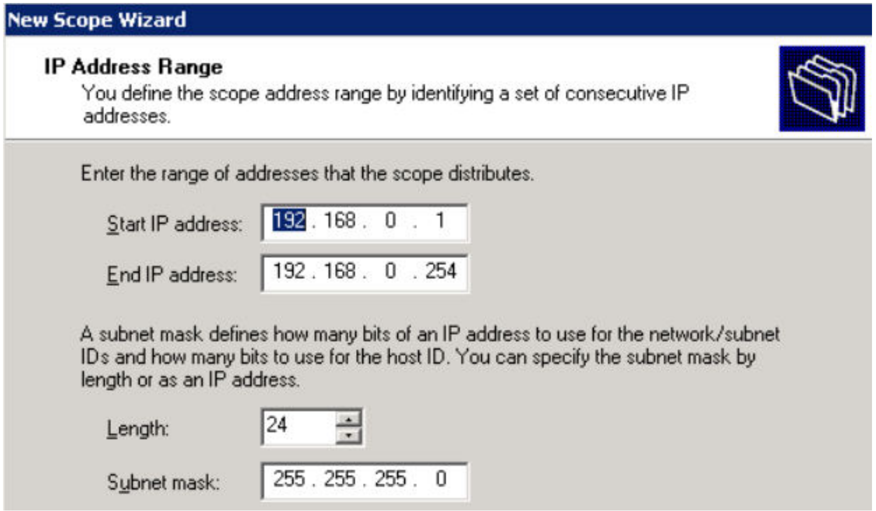
(Look at the notes section to read about how DHCP uses 3 allocation modes)

You configure in the DHCP server the scope or pool of IP addresses that the DHCP server can give out

Give out an IP address from the pool 192.168.1.100 – 192.168.1.254

In this case a scope of 154 IP addresses that it can give out

Scope: full range of IP addresses that the DHCP server can give out



New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 0 . 1

End IP address: 192 . 168 . 0 . 254

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

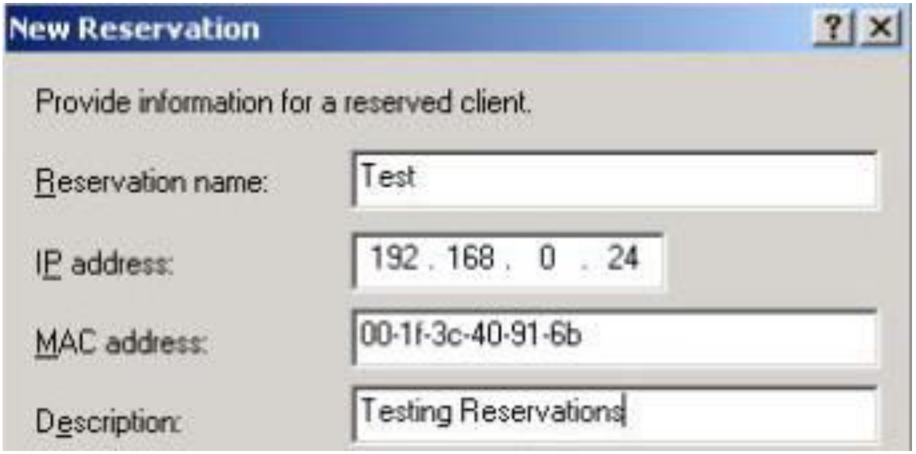
Length: 24

Subnet mask: 255 . 255 . 255 . 0

With DHCP you can create **reservations**

You create the scope but you can reserve a specific IP address within that scope e.g. 192.168.1.11 will be an access point

This IP address will not be issued by the DHCP as its been statically used



Provide information for a reserved client.

Reservation name: Test

IP address: 192 . 168 . 0 . 24

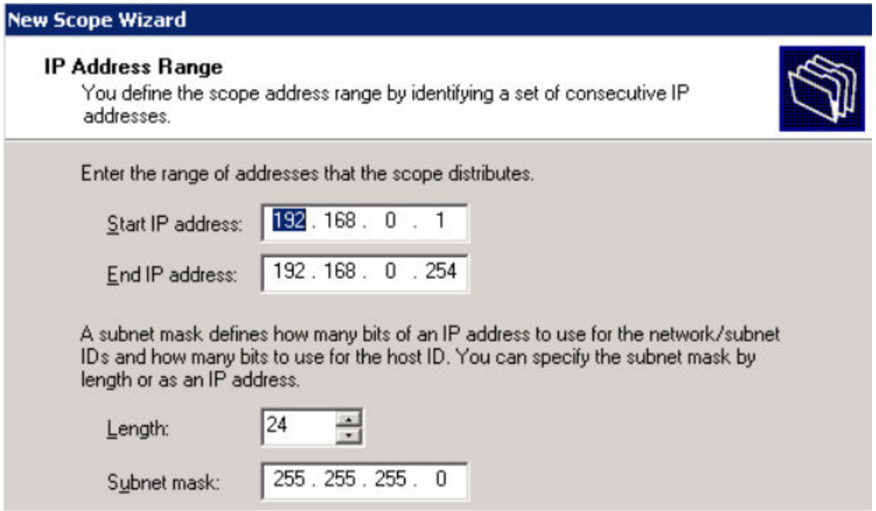
MAC address: 00-1f-3c-40-91-6b

Description: Testing Reservations

DHCP servers provide IP addresses for a limited time.

Network administrator can configure the actual length of time (usual of several days or a month).

If a **lease** expires, the IP address returns to the pool to be used by others



New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 0 . 1

End IP address: 192 . 168 . 0 . 254

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 24

Subnet mask: 255 . 255 . 255 . 0

Allows DHCP to recapture inactive IP addresses without humans updating the records.

An organization that lacks enough IP addresses for every user might use very short lease durations
so
That the addresses are reused during brief periods of inactivity.

A coffee shop has many people that come in with a laptop which are continually getting DHCP address but they soon leave

In this case your lease time of 1 day

If the host is powered down or taken off the network, the address is returned to the pool for reuse

Helpful with mobile users that come and go on a network

Client will try to renew the lease at about the 50% mark (1 day)

Client will re-contact the DHCP server and tell it that it wants to keep the IP address

DHCP says go ahead and keep that IP address for another 2 days

⬇

If your computer can not contact the DHCP server at the 50% mark

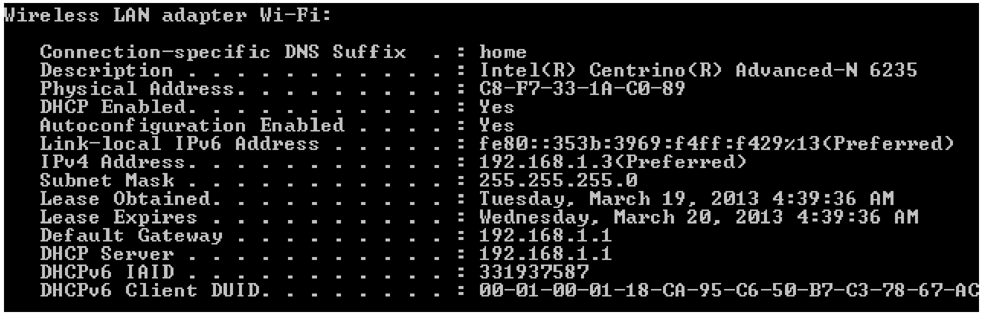
It will try again at the next 50% mark and so on

e.g. 2 days – 1 day – 12 hrs – 6 hrs – 3 hrs – 90 mins

⬇

If it can't contact the DHCP, then it gives up that IP address

To figure out how long your DHCP lease in Windows



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Intel(R) Centrino(R) Advanced-N 6235
   Physical Address. . . . . . . . . : C8-F7-33-1A-C0-89
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::353b:3969:f4ff:f429%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, March 19, 2013 4:39:36 AM
   Lease Expires . . . . . . . . . . : Wednesday, March 20, 2013 4:39:36 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 331937587
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-18-CA-95-C6-50-B7-C3-78-67-AC
```

Lease Obtained. . . . . : Tuesday, March 19, 2013 4:39:36 AM
Lease Expires . . . . : Wednesday, March 20, 2013 4:39:36 AM

When the DHCP Server goes down, that client can still use the allocated IP address for a limited period of time.

THINK ABOUT THIS !

Before a client communicates with the DHCP

They do not have an IP address yet, but they need to send IP packets.

To make that work

DHCP messages make use of two special IPv4 addresses

These addresses allow a host that has no IP address to still be able to send and receive messages on the local subnet

0.0.0.0: Address reserved for use as a source IPv4 address for hosts that do not yet have an IP address.

255.255.255.255: Local broadcast IP address.
Packets sent to this destination address are broadcast on the local data link, but routers do not forward them

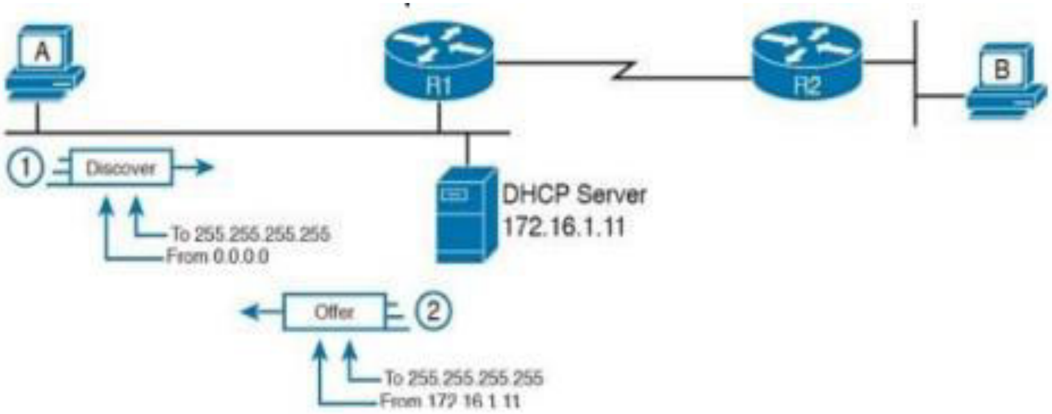
Host A, a client, sends a Discover message, with source IP address of 0.0.0.0 because host A does not have an IP address to use yet.

Host A sends the packet to destination 255.255.255.255, which is sent in a LAN broadcast frame, reaching all hosts in the subnet.

Client hopes that there is a DHCP server on the local subnet.

Why?

Packets sent to 255.255.255.255 only go to hosts in the local subnet; Router R1 will not forward this packet.

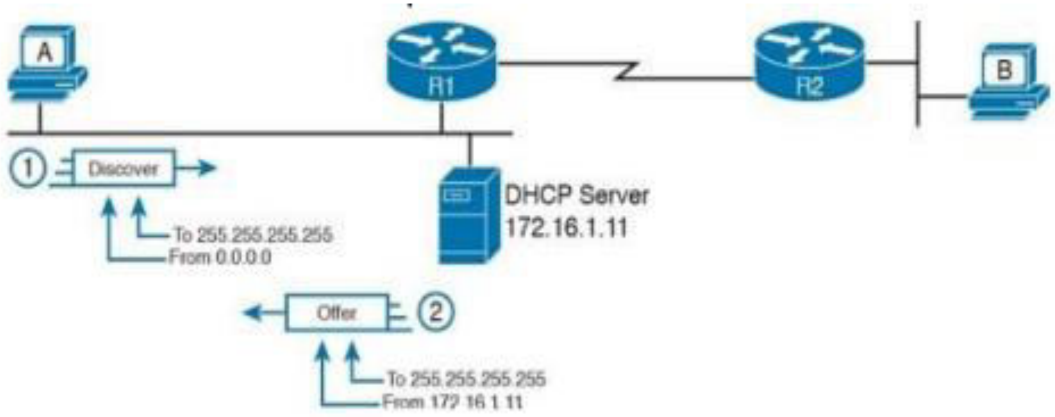


Offer message sent back by the DHCP server

The server sets the destination IP address to 255.255.255.255 again
Host A still does not have an IP address, so the server cannot send a packet directly to host A.

Server sends the packet to “all local hosts in the subnet” address (255.255.255.255).
All hosts in the subnet receive the Offer message.
Original Discover message lists a number called the client ID, based on the host’s MAC address, that identifies the original host.

As a result, host A knows that the Offer message is meant for host A.
Rest of the hosts will receive the Offer message, but see the message lists another device’s DHCP client ID, so other hosts ignore the Offer message



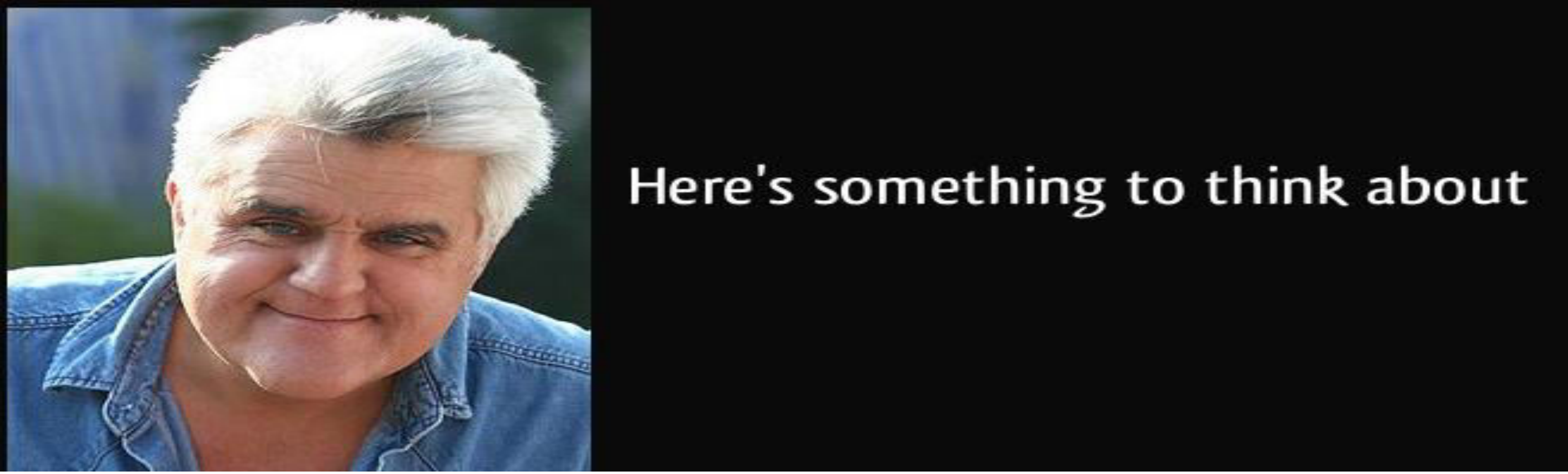
PUT IT IN YOUR BACK POCKET

DHCP server keeps status (state) information about each DHCP client that leases an address.

It remembers the DHCP client ID, and the IP address leased to the client.

So an IPv4 DHCP server can be considered to be a stateful DHCP server.

This is NOT the case with IPv6!



Assigning IP addresses with DHCP when another host tries to statically configure that same IP address.

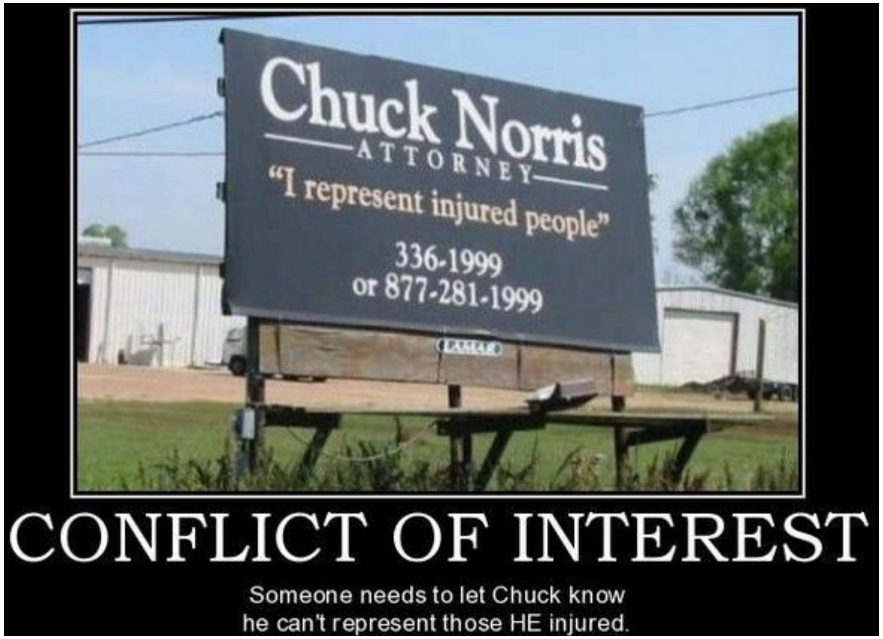
Although the DHCP server configuration clearly lists the addresses in the pool, plus those to be excluded from the pool,

Hosts can still statically configure addresses from the range inside the DHCP pool.

Simply, no protocols prevent a host from statically configuring and using an IP address from within the range of addresses used by the DHCP server

Knowing that some host might have statically configured an address from within the range of addresses in the DHCP pool

Both DHCP servers and clients try to detect such problems - **conflicts**


Chuck Norris
ATTORNEY
"I represent injured people"
336-1999
or 877-281-1999
LAMAR
CONFLICT OF INTEREST
Someone needs to let Chuck know
he can't represent those HE injured.

DHCP servers detect conflicts by using pings

Before offering a new IP address to a client, the DHCP server first pings the address.

If the server receives a response to the ping, some other host must already be using the address, which lets the server know a conflict exists.

Server notes that particular address as being in conflict, and the server does not offer the address, moving on to the next address in the pool

DHCP client detect conflicts by using ARP

When the DHCP client receives from the DHCP server an offer to use a particular IP address

Client sends an Address Resolution Protocol (ARP) request for that address.

If another host replies, the DHCP client has found a conflict.

BATMAN
WHAT HAPPENS IF A CLIENT IS UNABLE TO CONNECT TO A DHCP SERVER

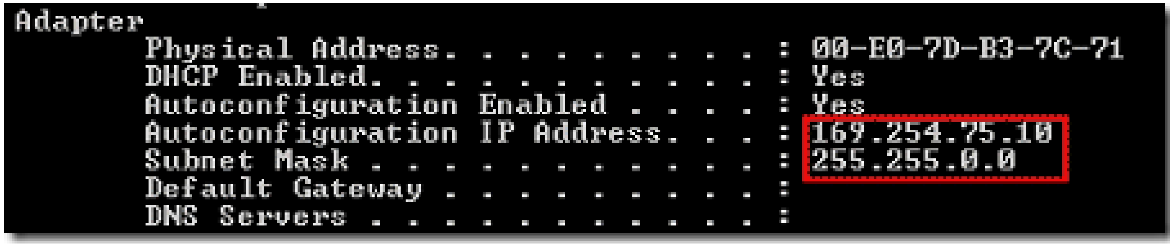
Computer default action is to use an '**Automatic Private IP Addressing (APIPA)** 'address

Automatic Private IP Addressing (APIPA)

Feature of all versions of Microsoft Windows (except Windows NT)

DHCP failover mechanism (when DHCP servers are nonfunctional)

Allows computers on same LAN to communicate

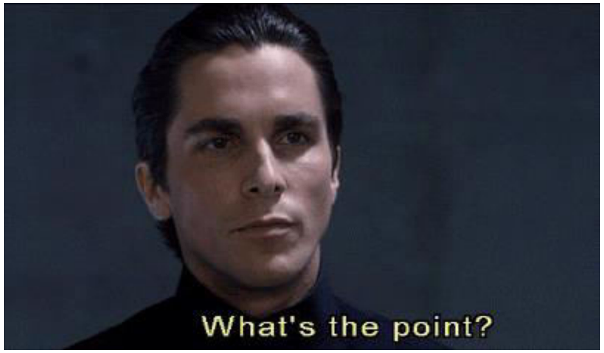


```
Adapter
        Physical Address. . . . . . . . . : 00-E0-7D-B3-7C-71
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        Autoconfiguration IP Address. . . : 169.254.75.10
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :
        DNS Servers . . . . . . . . . . . :
```

Does not provide a default gateway, so clients using APIPA cannot access the Internet

Client will assign itself an IP address of the form 169.254.x.y/16 (169.254.0.1 – 169.254.254.254)

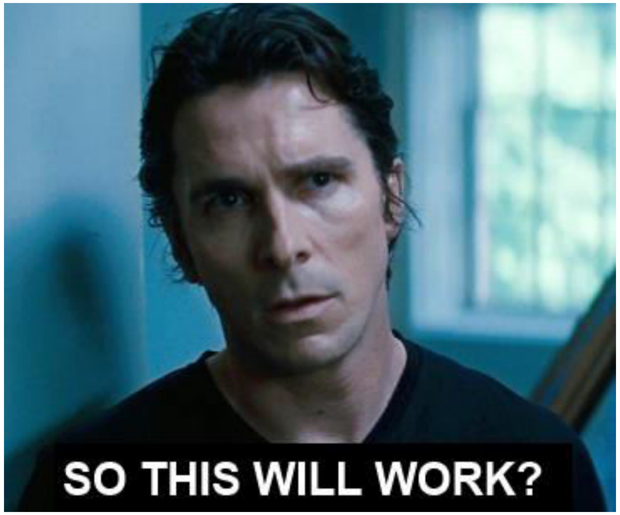
To go to the Internet we need to get an public IP address which is unique all over the world



Given this scenario, the world would have run out of IPV4 address years ago which are expensive to lease

Private IP addresses are valid only within that LAN, not recognized on the public Internet

By using **Network Address Translation (NAT)** we can save tons of IP addresses



NAT allows a host that does not have a valid registered IP address to communicate with other hosts through the Internet

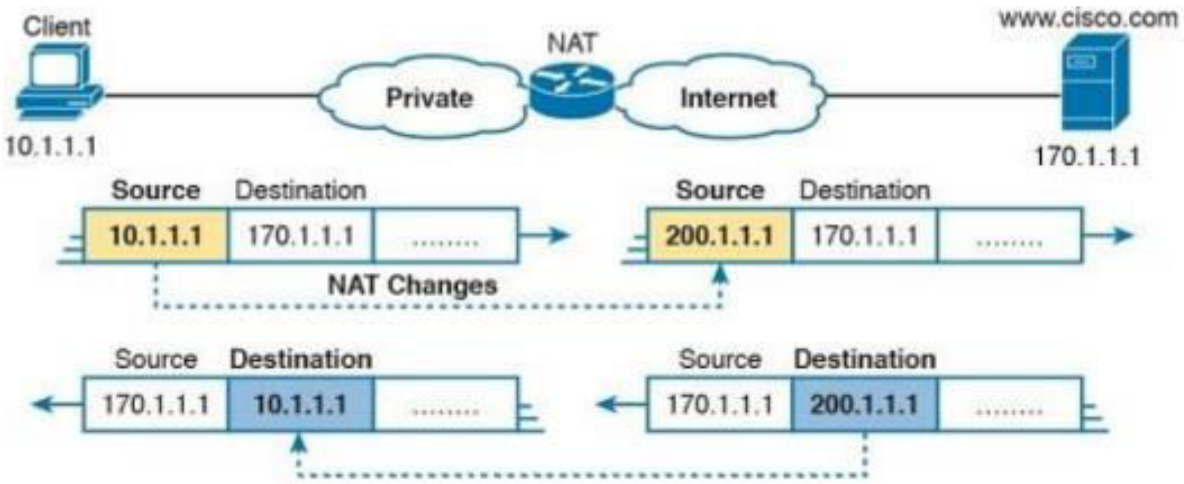
↓

NAT allows a small pool of public addresses or even a single public address, to be shared by an entire private network.

Router uses NAT to translate the private IP address to a public (global) address for routing over the internet

NAT function changes the private IP addresses to publicly registered IP addresses inside each IP packet

Only packets destined for other networks need to be translated



NAT translates (changes) datagrams that travel **in either direction**.

↓

Router performing NAT, changes the packet’s source IP address when the packet leaves the private organization

Router performing NAT also changes the destination address in each packet that is forwarded back into the private network

NAT Disadvantages

Adds small delay into network as NAT router has to create/maintain a NAT table

(table of inside addresses and associated outside addresses)

End to end traceability is lost

Some applications fail due to NAT (not common now)

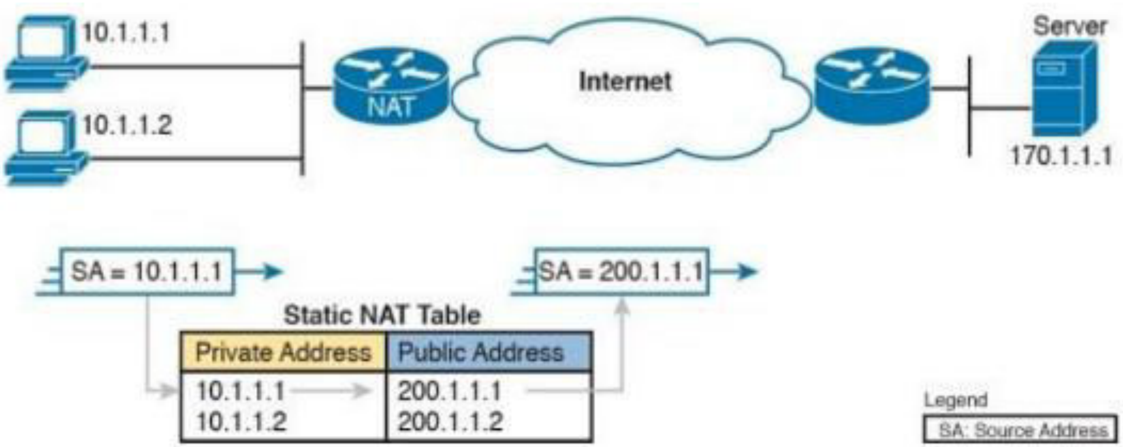
Static NAT (SNAT)

Allows permanent one-to-one mapping between private and global addresses. e.g. 10.1.1.1 → 200.1.1.1

Guarantee that a particular device is always associated with the same public IP address

Requires you to have one real Internet IP address for every host on your network

NAT router must maintain a table in memory of address mappings.



Private Address	Public Address
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

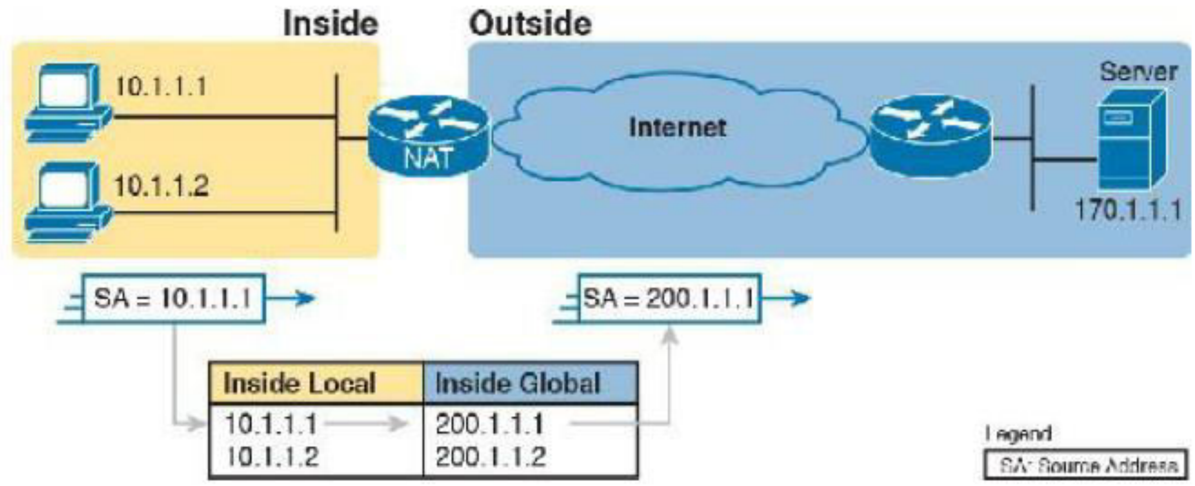
Cisco uses the term **inside local** for the private IP addresses and **inside global** for the public IP addresses

Inside local

Address used for the host inside the enterprise i.e. address used locally versus globally.

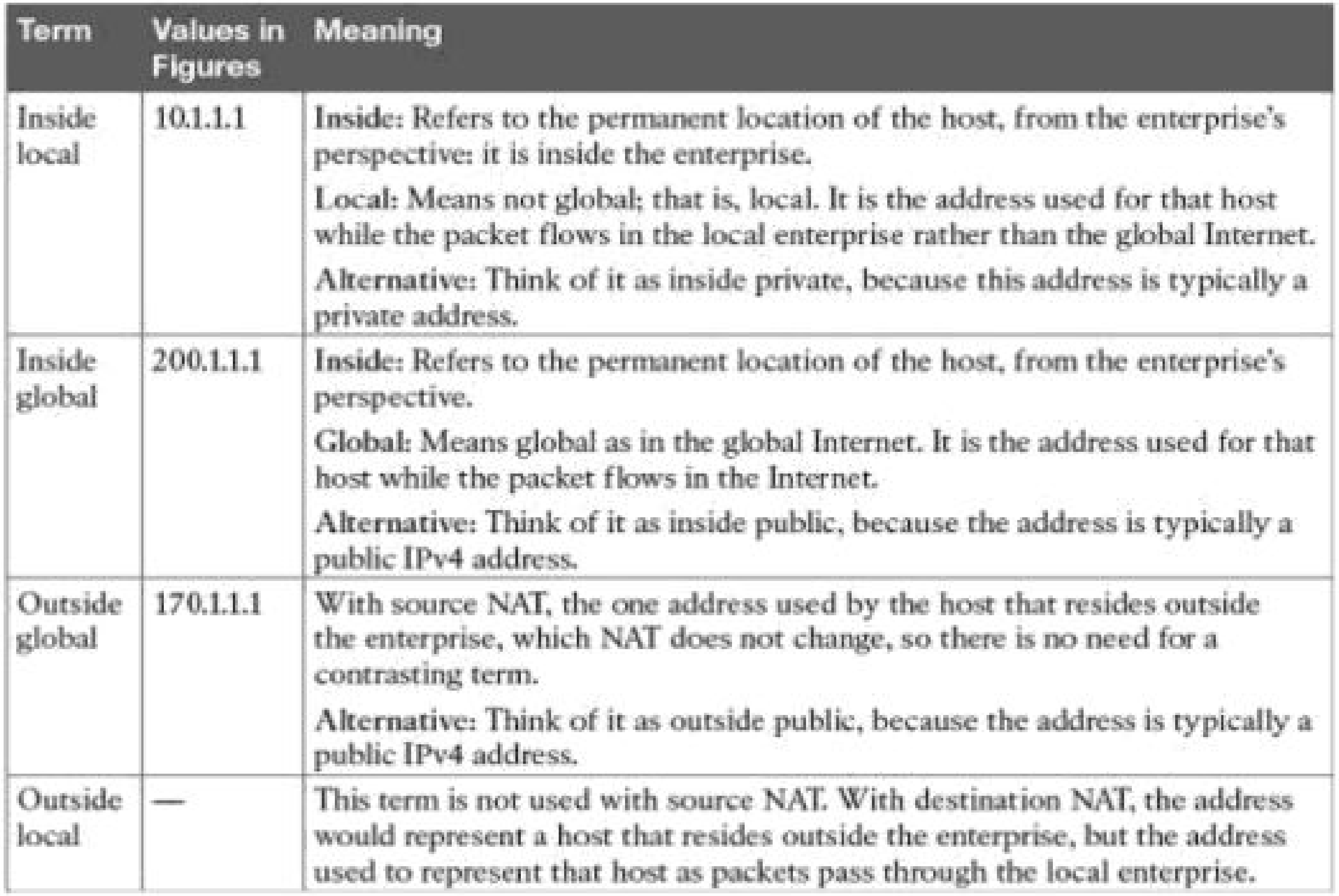
Inside global

Address used for the host inside the enterprise, but it is the global address used while the packet flows through the Internet

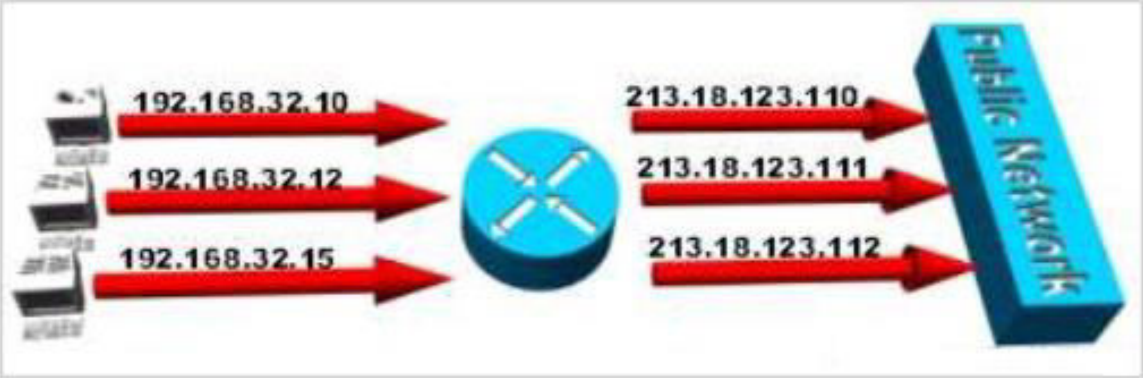


Inside Local	Inside Global
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

NAT feature destination NAT uses similar terms **outside local** and **outside global**



Term	Values in Figures	Meaning
Inside local	10.1.1.1	**Inside:** Refers to the permanent location of the host, from the enterprise's perspective: it is inside the enterprise. **Local:** Means not global; that is, local. It is the address used for that host while the packet flows in the local enterprise rather than the global Internet. **Alternative:** Think of it as inside private, because this address is typically a private address.
Inside global	200.1.1.1	**Inside:** Refers to the permanent location of the host, from the enterprise's perspective. **Global:** Means global as in the global Internet. It is the address used for that host while the packet flows in the Internet. **Alternative:** Think of it as inside public, because the address is typically a public IPv4 address.
Outside global	170.1.1.1	With source NAT, the one address used by the host that resides outside the enterprise, which NAT does not change, so there is no need for a contrasting term. **Alternative:** Think of it as outside public, because the address is typically a public IPv4 address.
Outside local	—	This term is not used with source NAT. With destination NAT, the address would represent a host that resides outside the enterprise, but the address used to represent that host as packets pass through the local enterprise.



computer with the IP address of 192.168.32.10 will always translate to 213.18.123.110

↓

In real life, not all of your employees uses internet at the same time

Dynamic or Pooled NAT

Like static NAT, the NAT router creates a one-to-one mapping between an inside local and inside global address,

+

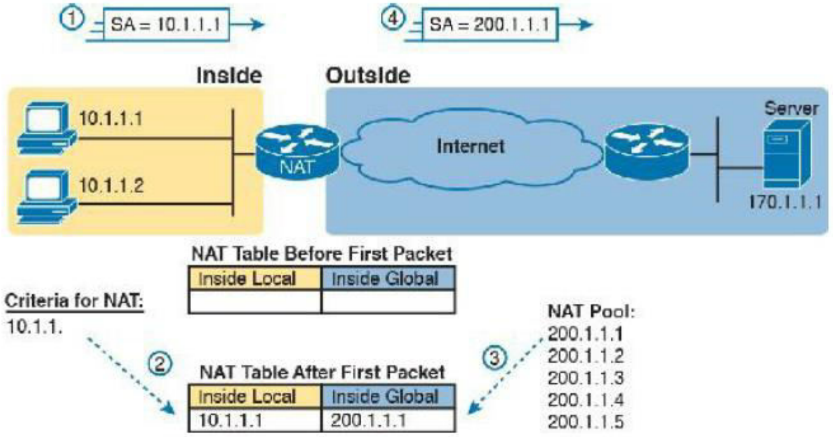
Changes the IP addresses in packets as they exit and enter the inside network.

Sets up a pool of possible inside global addresses

Dynamically assign these 50 public IP addresses to those who really need them at that time i.e.

Many → Many

Any private IP address will automatically be translated to one of the available Internet IP addresses by that router



NAT Table Before First Packet

Inside Local	Inside Global

NAT Table After First Packet

Inside Local	Inside Global
10.1.1.1	200.1.1.1

A pool of five inside global IP addresses has been established: 200.1.1.1 through 200.1.1.5.

NAT has also been configured to translate any inside local addresses that start with 10.1.1.

Step 1

Host 10.1.1.1 sends its first packet to the server at 170.1.1.1.

Step 2

As the packet enters the NAT router, the router applies some matching logic to decide whether the packet should have NAT applied.

As the logic has been configured to match source IP addresses that begin with 10.1.1

The router adds an entry in the NAT table for 10.1.1.1 as an inside local address.

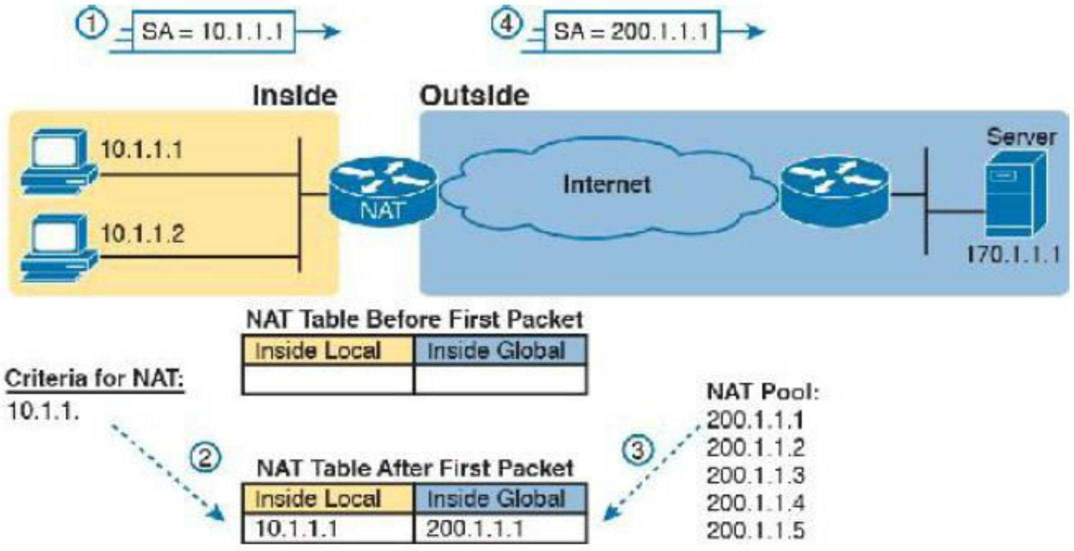
Step 3

NAT router needs to allocate an IP address from the pool of valid inside global addresses.

It picks the first one available (200.1.1.1, in this case) and adds it to the NAT table to complete the entry.

Step 4

The NAT router translates the source IP address and forwards the packet.



NAT Table Before First Packet

Inside Local	Inside Global

NAT Table After First Packet

Inside Local	Inside Global
10.1.1.1	200.1.1.1

goodtoknow

Dynamic entry stays in the table as long as traffic flows occasionally

You can configure a timeout value that defines how long the router should wait
having not
Translated any packets with that address, before removing the dynamic entry.

If a new packet arrives from yet another inside host, and it needs a NAT entry, but all the pooled IP addresses are in use, the router simply discards the packet.

e.g. only the first 50 people can access internet, others must wait to their turns until a NAT entry times out

Inside global pool of addresses needs to be as large as the maximum number of concurrent hosts that need to use the Internet

↓

Port Address Translation (PAT)

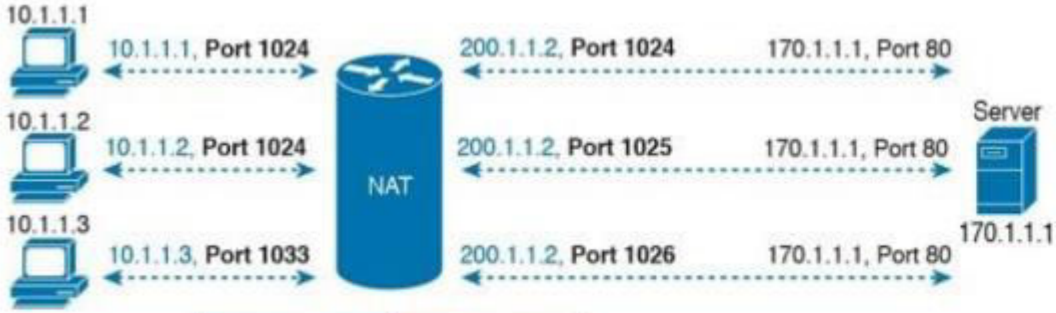
PAT (NAT Overloading)

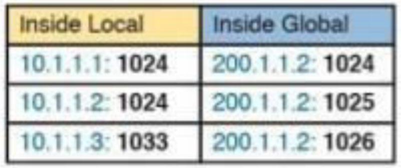
Most popular type of NAT

Overloading allows NAT to scale to support many clients with only a few or 1 public IP address (es)

When PAT creates the dynamic mapping, it selects not only an inside global IP address but also a unique port number

Maps multiple private IP addresses to a single public IP address (many-to-one) by using different ports



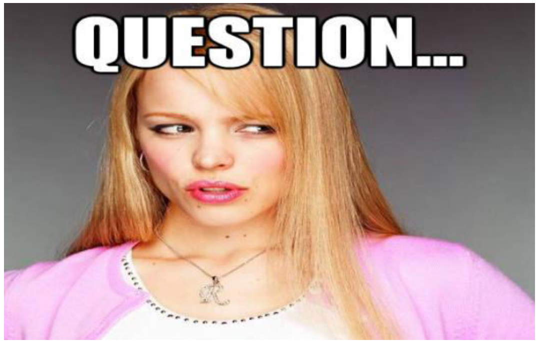


Inside Local	Inside Global
10.1.1.1: 1024	200.1.1.2: 1024
10.1.1.2: 1024	200.1.1.2: 1025
10.1.1.3: 1033	200.1.1.2: 1026

Dynamic NAT Table, With Overloading

NAT router keeps a NAT table entry for every unique combination of inside local IP address and port
with
Translation to the inside global address and a unique port number associated with the inside global address

Note: As the port number field has 16 bits, NAT overload can use more than 65,000 port numbers, allowing it to scale well without needing many registered IP Addresses i.e. just 1 required



How does a server know which application/service an incoming packet should be directed to?

e.g. a server running both web server s/w and file transfer s/w can serve up web pages and transfer files

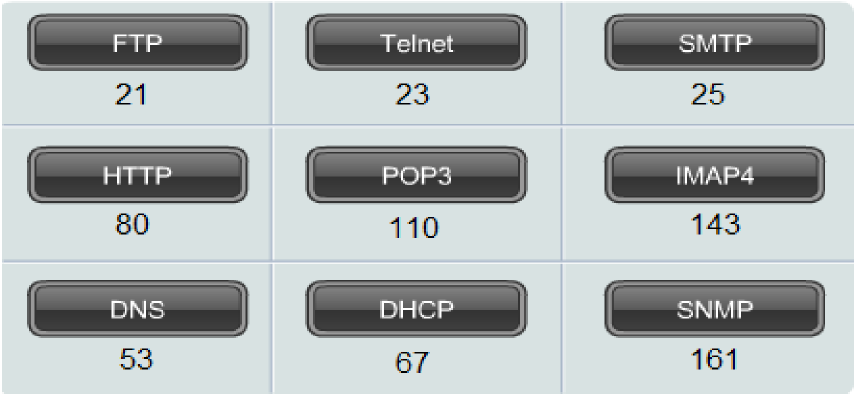
↓

Port Numbers & Sockets

Port Numbers

Virtual Ports as opposed to physical ports

Indicates which application is to be used to process a packet sent by a client request to a specific destination port.



FTP	Telnet	SMTP
21	23	25
HTTP	POP3	IMAP4
80	110	143
DNS	DHCP	SNMP
53	67	161

Similar to apartment numbers.

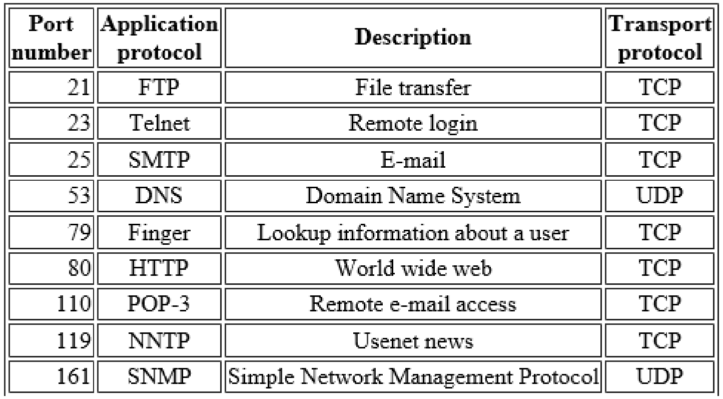
Street address (IP address) of an apartment complex takes you to the correct building

Apartment number (port) is required to identify the correct location within the building

Incoming packet requesting a web page will contain not only an IP address of the web server,

but

Also contain the port number it expects the web server s/w to be listening on.



Port number	Application protocol	Description	Transport protocol
21	FTP	File transfer	TCP
23	Telnet	Remote login	TCP
25	SMTP	E-mail	TCP
53	DNS	Domain Name System	UDP
79	Finger	Lookup information about a user	TCP
80	HTTP	World wide web	TCP
110	POP-3	Remote e-mail access	TCP
119	NNTP	Usenet news	TCP
161	SNMP	Simple Network Management Protocol	UDP

How does a packet know which port number to use?

↓

Already setup e.g. web servers listen on port 80

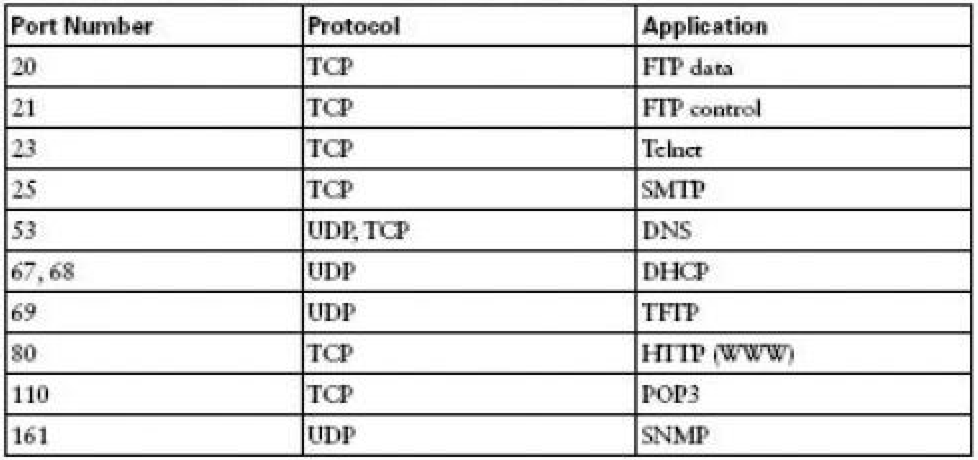
↓

When a web server is started up, it immediately begins listening on port 80.

When the web server detects a packet with port number set to 80, it extracts the packet payload and processes the data

Ports are broken into three categories and range in number from 1 to 65,535

1. **Well-Known Ports:** destination ports that are associated with common network applications i.e. range of 1 to 1023.
2. **Registered Ports:** Ports 1024 through 49151 can be used as either source or destination ports.
3. **Private Ports:** Ports 49152 through 65535, often used as source ports.



Port Number	Protocol	Application
20	TCP	FTP data
21	TCP	FTP control
23	TCP	Telnet
25	TCP	SMTP
53	UDP, TCP	DNS
67, 68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP

Port 80 is reserved only for computer running web server s/w (not web browser s/w)

Source host does not use does not use port 80 when requesting a web page. Client uses ports from 1024 – 4096

Destination Port

Client places a destination port number in the segment to tell the destination server what service is being requested

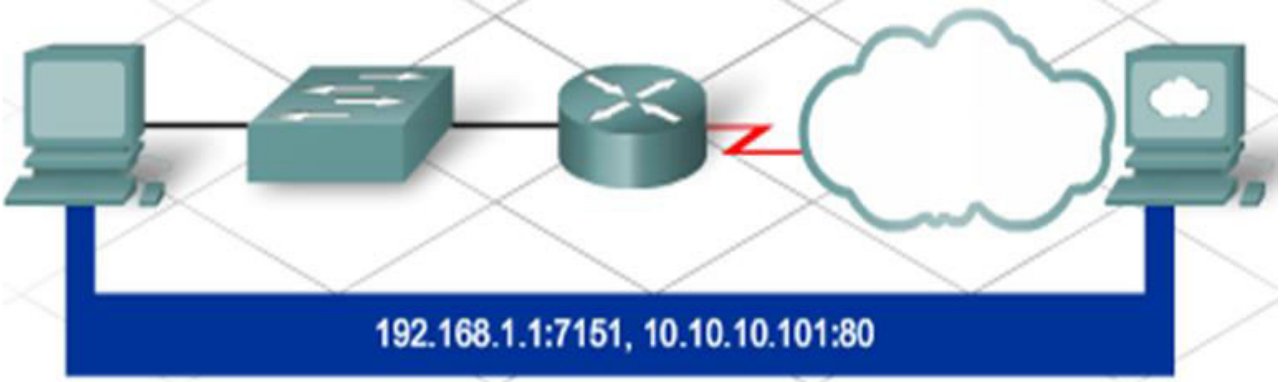
e.g. Port 80 refers to HTTP or web service.

Server that receives the message knows that web services are being requested.

A server can offer more than one service simultaneously e.g. web & ftp services

Source Port

Randomly generated by the sending device to identify a conversation between two devices

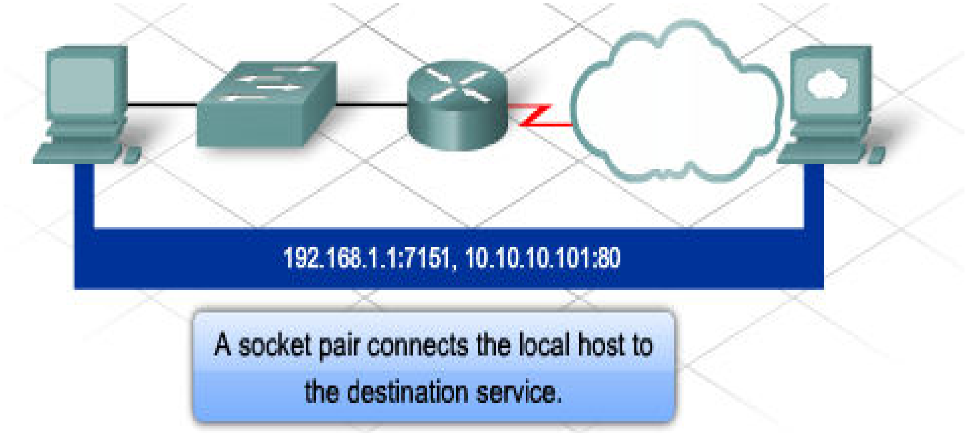


Transport Layer Port Number + Network Layer IP address of the host (either source or destination) = **Socket or Endpoint**

Sockets: help identify a specific host along with the port a particular application is listening on

Socket = IP address + transport protocol + port number e.g. (10.1.1.2, TCP, port 80)

Socket Pair = Source + Destination IP addresses + port numbers
(unique and identifies the specific conversation between the two hosts)


192.168.1.1:7151, 10.10.10.101:80
A socket pair connects the local host to the destination service.

Client socket = 192.168.1.1:7151
Web server socket = 10.10.10.101:80

Client socket + Web server socket = socket pair (192.168.1.1:7151, 10.10.10.101:80)

GOOD AFTERNOON

GOOD EVENING

AND

GOOD NIGHT