Date: ...../...../.....

CSE421 – Computer Networks – SEC

Lecture 12 – DHCP and NAT/PAT

DHCP – also a Network Layer protocol. (related to IPv4 Addressing)

↳ Dynamic Host Configuration Protocol

ISP – provides IP to your devices – assigned statically whereas DHCP assigns it automatically. DHCPv4 – functions w/ IPv4 addresses.

↳ assigns IPv4 addresses + other network configuration information dynamically.

There are a pool of IP Addresses (total available hosts) & DHCP works w/ these available IPs. DHCP can automatically assign these addresses to devices. Ex: wifi at a restaurant, 500 PCs in an office makes use of DHCP as well. [all available IPs under Network Address of that network]

↳ DHCP protocol is used in a dedicated DHCPv4 server. A cisco router can be configured to provide DHCP services w/out the need for a dedicated server as it is very expensive.

DHCP server – scalable + relatively easy to manage

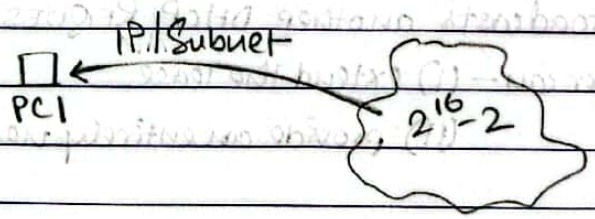
↳ DHCPv4 server dynamically assigns/leases an IPv4 address from a pool of addresses for a limited period of time chosen by the server/until the client no longer needs the address.

DHCP, works in c/s mode.

Manual connection stays forever.

* client can ask for an extension of the lease.

Ex: logging into your friend's wifi w/out password.



↳ The client connects to the network w/ that leased IPv4 address until the lease expires. The client must contact the DHCP server periodically to extend the lease.

Suppose, lease → 2 hours. but after 30 minutes the device is no longer using the IP address, DHCP server (after loosing an IP) keeps pinging the device to check if the IP is being used/waits for a reply. If not reply is found, then IP is returned to the DHCP pool.

Date: ...../...../.....

* lease mechanism ensures that clients which move out of the network / power off do not keep addresses that they no longer need.
* after lease expires → DHCP server returns the address to the pool.

DORA

(*) Steps to obtain a lease — ↑ type of packet / information

(I) DHCP Discover (Broadcast) – specific destn not known.
↳ finds the DHCP server on the network.
↳ can be >1

(II) DHCP Offer (Unicast) ↗ reply to step (I)
↳ contains an available IP address to lease.

unicast – you know who you are replying to so no need to broadcast; specific destn → unicast the DHCP offer

(III) DHCP Request (Broadcast) –> 1 DHCP servers; multiple offers
↳ serves as an acceptance notice to the selected server + an implicit decline to any other device.

} 1 DHCP ✓
} 2 DHCP ✗

one broadcast message performs both task.

(IV) DHCP Acknowledgement (Unicast)
↳ verifies the lease information.

confirmation

→ reply to step (III)

(*) Steps to renew a lease — ↑ before expiration

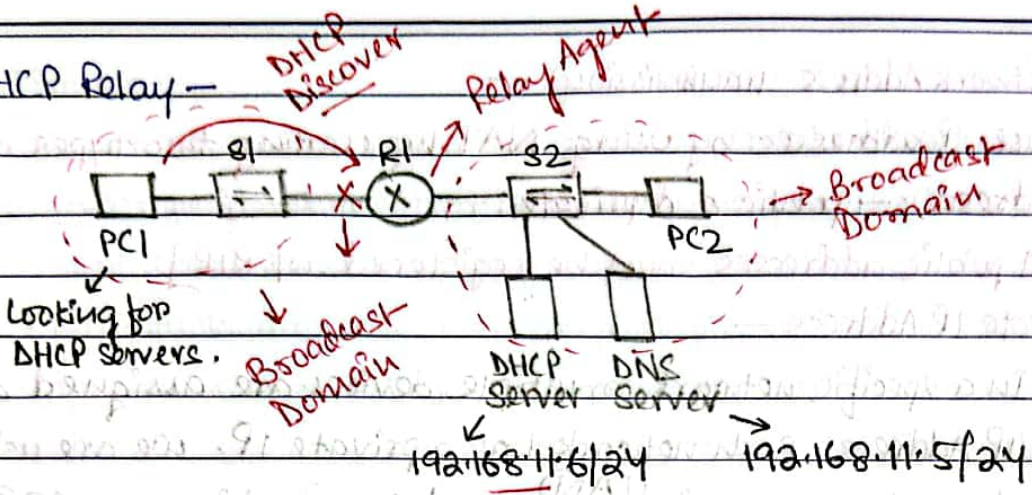
(I) DHCP Request
↳ before the lease expires, the client sends a DHCP Request message directly to the DHCPv4 server that it is connected w/. If a DHCP ACK is not received w/in a specific amount of time then the client broadcasts another DHCP REQUEST so that another DHCP server can – (I) extend the lease.
(II) provide an entirely new IP

If pool is divided, one server will not know IPs under same pool. ↑ renewal

(II) DHCP Acknowledgement
↳ on receiving the request message the server verifies the lease information by returning a DHCP ACK.

Date: ...../...../.....

⊛ DHCP Relay –



Here, the client & the server are in different networks. The DHCP Discover/ Broadcast packet is dropped at the default gateway of the router (R1) as routers do not forward any type of broadcast packets. Therefore, the DHCP Relay concept is used. At the point where the broadcast message is being dropped, an "ip helper-address" is configured. Router then sees that it has a helper address configured so it takes the broadcast packet and delivers it to the DHCP server.

ip helper-address dest^{n} IP
↳ DHCP server

Q – PC1 is trying to contact a DHCP server/cisco router of another network for an IP address. But is unable to do so. Why? What is the solution?

* packet dropped
* DHCP relay needs to be configured.

⊛ Configuring DHCP Relay –

* allows R1 to relay DHCPv4 request/broadcasts to the DHCPv4 server.
* when R1 has been configured as a DHCPv4 relay agent, it accepts broadcast requests for DHCPv4 service and then forwards those requests as a unicast to the IPv4 address 192.168.11.6.

↳ commands –

default gateway (R1)
DHCP server

```
R1(config)# interface g0/0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1#
```

Date: ...../...../.....

NAT (Network Address Translation) —

* reuse IP addresses by using NAT by creating two types of addresses — public and private.
[all public addresses must be registered w/ RIR]

(I) Private IP Address —

In a specific network, multiple devices are assigned a single IP Address. Each network has a private IP. We are using IPv4 & we have already exhausted (LAN) these addresses (2^{32}); we cannot uniquely assign private IPs anymore.

* cannot route private IP over the internet

Problem — overlapping IP addresses for devices but it has to be unique in order to send packets across networks.

LAN1 PC1 — 192.168.10.1
LAN2 PC2 — 192.168.10.1

Same IP — server cannot differentiate who is the sender/receiver; cannot communicate w/ other networks.

∴ Private IP cannot be used to come out of a network.

* not enough public IP to allow org. to provide one to each of their hosts.

Soln — Public IP

Need to maintain uniqueness when you leave the network & move into the internet.

(II) Public IP Address —

Always unique over the entire internet; no overlapping

*** Need to translate/convert the private IP address at the default gateway of the router to public IP address.
↳ process is called NAT.

* public routing tables advertised globally

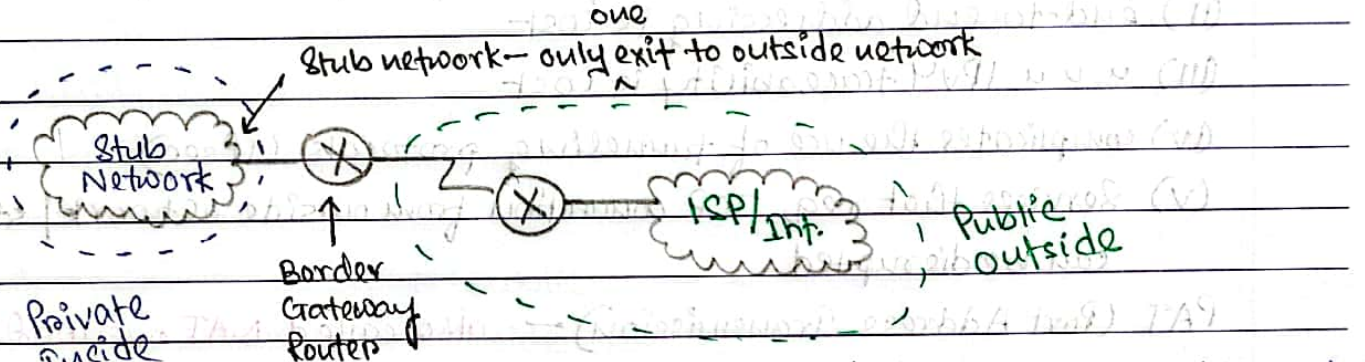
⊛ Classes of Private Addresses —

A	10.0.0.0 — 10.255.255.255
B	172.16.0.0 — 172.31.255.255
C	192.168.0.0 — 192.168.255.255

Date: ...../...../.....

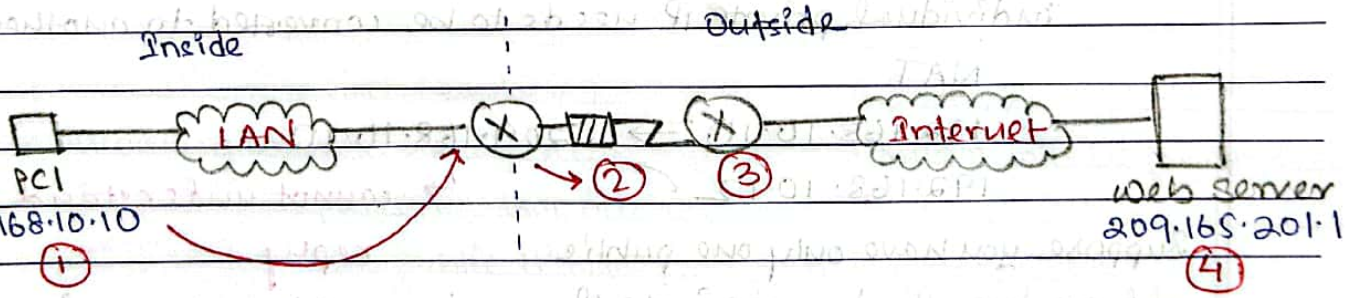
NAT-enabled routers

* NAT Process —
  - ↳ a router is used where NAT services are enabled.
  - ↳ router performs the translation at the edge of the network that works both ways.
  - ↳ NAT-enabled routers keep one/multiple valid IP addresses outside of the network and uses DHCP to provide private IPs to the users of the netwo
  - ↳ when C sends a packet out of the network, NAT translates the internal IP address of the client to an external address.
  - ↳ To outside users, all traffic to and fro the network has the same IP / is from same pool of addresses [cannot see the private IP]



→ performs the trans^{n} of inside private address to outside public address.

Inside network — LAN
Outside network — internet / another network



Inside local address — Private address — (1) (Source)
" global " — Public address (NAT translation) — (2) (Source)
Outside global " — Public address of router — (3) (Destination)
" local " — Private address of PC2 or server — (4) (Destination)

we do not know this address → in the internet we can only see the public IPs.

Advantages of NAT —

(i) Hides the IPv4 addresses of users & other devices
(ii) provides consistency for internal network addressing schemes
(iii) Increases flexibility of connections to public networks
(iv) conserves legally registered addressing by allowing privatization of intranets.
(v) conserves addresses via app^n port-level multiplexing
(vi) allows existing private IP address scheme to remain while allowing for easy & to a new public address scheme.

Disadvantages of NAT —

(i) increases forwarding delays
(ii) end-to-end addressing is lost
(iii) " " " IPv4 traceability is lost
(iv) complicates the use of tunneling protocols (IPsec)
(v) Services that req. TCP connection from outside network | stateless UDP can be disrupted.

PAT (Port Address Transmission) — also called NAT overload.

Why do we need PAT?

— In NAT, one private IP was mapped to one public IP. However, a network has more than one devices | private IPs so each individual private IP needs to be converted to another public IP.

NAT

192.168.10.10 → 209.168.10.10

192.168.10.12 ↗ ↳ cannot understand who to reply.

Suppose you have only one public address for all of your private IPs in your network. → Add port numbers — socket address → IP + Port Address

↳ one to one mapping
↳ private IPs are also expensive.
↳ public IP needs to unique

PAT ensures that devices use a different TCP port for each session it serves on the internet.

PAT

Private IP + Port Address of the device (S) → Public Address + Port Address (S)

One public address can satisfy multiple private IPs.

192.168.10.10 : 1555 → 209.168.10.10 : 1555
192.168.10.12 : 1575 → 209.168.10.10 : 1575

Date: ...../...../.....

Port Overlapping—

↳ PAT tries to use the source port but if source port is already used, PAT assigns the next available port.

↳ If there is no available ports left then go to another public address (if available) and if you have only one public then nothing can be done. NAT/PAT unsuccessful. → packet will not be forwarded

NAT v/s PAT—

NAT	PAT
* modifies IPv4 addresses.	* modifies IPv4+ port number.
* one-to-one mapping bet^n inside local + inside global.	* one public address can be mapped to multiple private address.
* uses IPv4 addresses during translation.	* uses IPv4 and TCP/UDP port numbers during translation.
* unique inside global (public) is required for each inside local (private) host accessing the outside network.	* a single unique inside global can be shared w/ many inside local hosts accessing the outside network.

Port forwarding—

Public IP : Port Number ← mentioned

* all incoming connections w/ matching port number will be forwarded to the internal computer w/ that address.
* a packet sent to the public IP and port of a router can be forwarded to a private IP address + port in the inside network.
* helps reach the servers w/ private addresses from outside networks.