MobileNAT : New technique for mobility across heterogeneous address spaces

Milind Buddhikot, A.Hari, K.Singh, Scott Miller

Presented By----Sandeep Davu

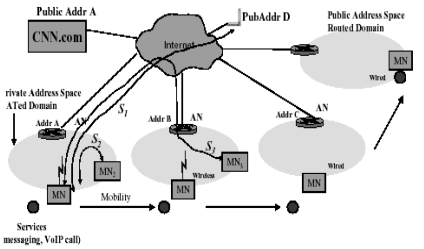
Abstract

- Use of two IP addresses – an invariant virtual ip address for host identification at application layer and an actual routable address at network layer that changes due to mobility.
- New DHCP enhancements to distribute the two addresses
- New signalling element called Mobility Manger(MM) to signal changes in packet processing rules to NATs in the event of mobility.

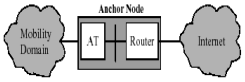
Introduction

- Network address translation(NAT) devices have been widely used to combat problem of address space depletion.
- Network will consist of large number of domains, each with its own address space.
- Mobility is an important characteristic of wireless networks that enable location transparent access to network services.

Network and Mobility model



Anchor Node(AN)

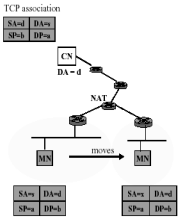


Anchor Node consists of two logically separate elements.

•Address translation(AT)which performs Network address translation(NAT) or network address porttranslation (NAPT).

•A traditional router.

Basic ideas in MobileNAT



TCP connection at the server is no longer valid and therefore, the connection is lost.

This results from the limitation of overloading the IP address with two functions

- host identification by TCP layer.
- network attachment information for routing.

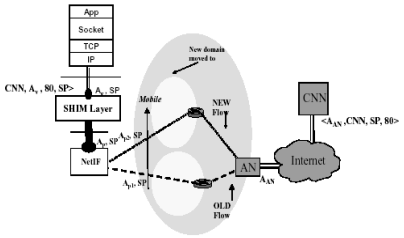
Two IP addresses for hosts

Dual functionality problem of IP address can be handled by providing two IP addresses.

- **Virtual IP (Av) address:** A fixed address is used for host identification that does not change on mobility. This is exposed to the TCP/IP stack and higher layer applications.
- **Physical IP (Ap) address:** This routable address identifies the *current* point of MN attachment to the Internet and is used for routing packets to the MN. Clearly, this address must change as the MN moves.

Both these ip addresses can be public or private addresses

Intra-domain mobility for Internet-sessions



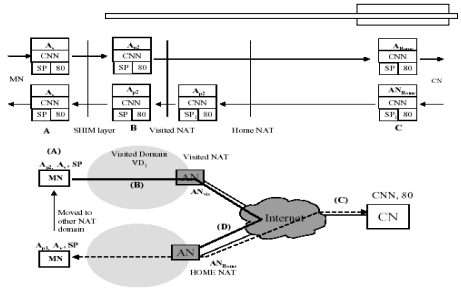
Intra-domain mobility for Internet-sessions

- Both Ap,Av are private addresses.
- TCP association at MN (TCP,Av,CNN,SP,80)
- Mobile Node
  - But Av is not routable—There is a sourceNAT (SNAT) which translates Av ->Ap in every packet and destination NAT (DNAT) changing the destination address from Av->Ap.
  - This is taken care by the SHIM layer between TCP/IP stack and the ethernet address.
- Anchor Node
  - Av is not a public address so the AN replaces Av with a publicly routable address Aan.
  - An maintains a address mapping rule Ap->Aan

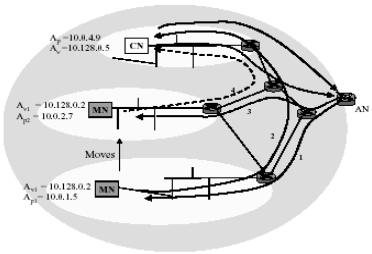
Summary of packet mapping rules at AN

	A_p	A_v	AN rules	
			Policy P_1	Policy P_2
case 1	Private	Private	$A_p \mapsto A_{AN}$	$A_p \mapsto A_{AN}$
case 2	Private	Public	$A_p \mapsto A_v$	$A_p \mapsto A_{AN}$
case 3	Public	Private	$A_p \mapsto A_{AN}$	$A_p \mapsto A_{AN}$
case 4	Public	Public	$A_p \mapsto A_v$	$A_p \mapsto A_{AN}$

Inter-domain mobility for Internet-sessions



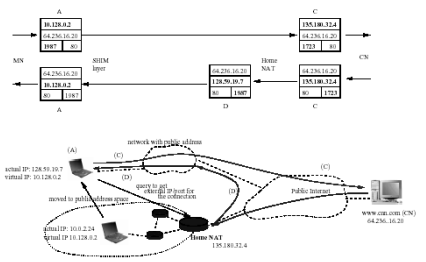
Intra-domain mobility for intra domain sessions



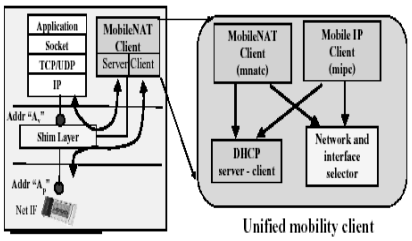
Virtual address aliasing

- When the MN moves to the new NAT-domain, it attempts to renew its Av and obtain new Ap;new.
- It might happen that there is an Av already existing in that NAT domain. This is called Virtual Address Aliasing.
- the new AN uses Av -> Ap SNAT or DNAT rules for some other node's Ap, such aliasing results in ambiguity in data forwarding.
- Although Av may not be unique, (Ap;Av) pair is always unique in a domain. So the MN can obtain a new Av;new and Ap;new during address renewal if it discovers Av conflict.
- choice is given to the user before getting Av;new
  - Continue with the old sessions, and not establish new sessions, or
  - close all the existing sessions and start afresh.

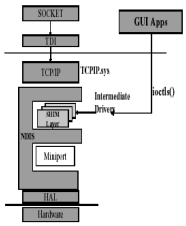
Moving between a NAT-domain and the public Internet



PROTOTYPE IMPLEMENTATION



PROTOTYPE IMPLEMENTATION



Shim-layer is located between the TCP/IP stack and the network interface and acts as an intermediate driver.

the application level entity called mnatc processes the DHCP client messages and interacts with the shim-layer.

Discussion

- ***Fast hand-off and DHCP latency.***
- ***Route optimization for intra-domain sessions.***
- ***Co-existence with Mobile IP and Hawaii.***
- ***IPv6 in NAT domain.***
- ***Mobility to 3G network.***
- ***Multiple NAT for load balancing.***

Security Considerations

- MOBILENAT should work with IP security (IPSec). The AH (authentication header) mode is not possible with networkaddress translator devices in the network, however the ESP (encapsulated security payload) should be allowed. IPsec is used in VPNs (virtual private networks).
- MOBILENAT should work with transport layer security (TLS) like secure socket layer (SSL).
- The inter-domain mobility requires packet flow between two different NATs in two different domains, i.e., the Home-NATforwards the packets to the Visited-NAT. The system should also allow reverse tunneling from Visited-NAT to Home-NAT

  so that the Visited-NAT does not have to spoof the source IPaddress.
- The mobile nodes subscribed to some independent service provider with appropriate AAA infrastructure should be allowed to roam in the MOBILENAT domain.

RELATED WORK

- ***Cellular IP (CIP)*:** One big problem with Cellular IP is that it usesproprietary non-IP protocol within the domain and can not inter-operate with other IP endpoints in the domain.
- ***Hawaii*:** Hawaii uses IP within the domain, however the intradomain routers must maintain per-host routing information. This is not scalable with increasing number of mobile nodes in the domain.
- ***Hierarchical mobile IP (HMIP)*:** A domain wide gateway foreign agent (GFA) manages host mobility within the domain. When the MN moves to a new location the global HA is informed.
- ***Intra-domain mobility protocol (IDMP)*:** IDMP [6] is similar to hierarchical mobile IP, except that it also allows multiple mobility agents (similar to GFA in HMIP) for load balancing, and can use DHCP for signaling. IDMP is also well suited for NAT domains where the mobility agent also interacts with the NAT device for IP address translation.

Critique on the paper

Advantages

- The paper provides a very good explanation of the work along with the possible alternatives that could be employed.
- It discusses the possibilities of combining this with other research to have even better results.

Disadvantages

- Did not provide with the performance analysis of the work.

Overall the paper provides a exhaustive vies of the technique they have implemented.

CONCLUSION

- For most of these devices, transiently allocated IP addresses instead of permanently assigned Home IP addresses will be efficient under most common circumstances.
- MOBILENAT supports efficiently the micro and macro mobility of devices across private and public heterogeneous address spaces.
- fixed unique virtual IP address for host identification and a dynamic, unique actual IP address for routing within the domain.
- The biggest advantage of our scheme
- is that unlike several micro-mobility schemes it does not require any change in the routing infrastructure in the domain or does not need any foreign agent.
- It co-exists with MobileIP and is easy to deploy.

Questions????

- What is virtual address aliasing and how can it be handled?
- Describe how can you obtain the mapping rules that anchor node maintains in each of the four cases?
- What are the two main functionalities of IP address and which address takes care of which function?
- What is shim layer and how is it useful?
- What are the functions of an Anchor node?