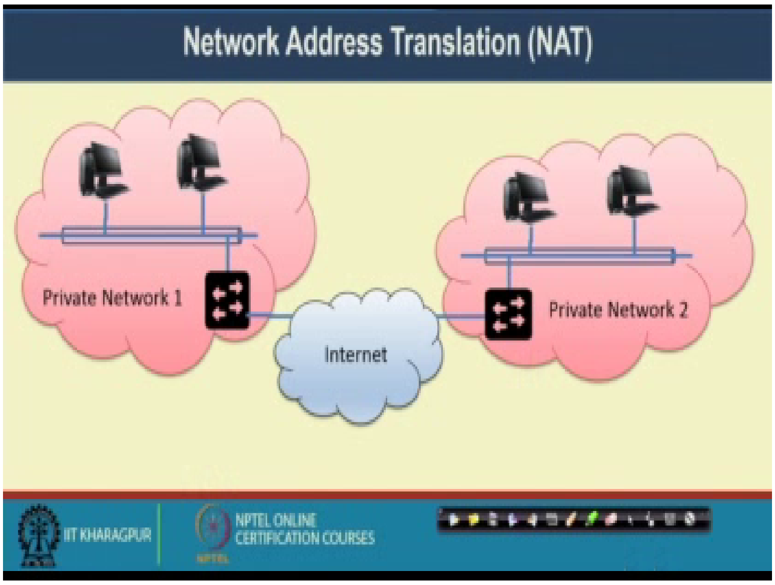
Computer Networks and Internet Protocol
Prof. Sandip Chakraborty
Department of Computer Science And Engineering
Indian Institute of Technology, Kharagpur

Lecture – 29
IP Addressing (IPv4) III – Network Address Translation (NAT)

Welcome back to the course on Computer Network and Internet Protocol. So, we are looking into the IPv4 Addressing schemes in details. So, now, we will look into a specific problems in IPv4 addressing and network layer protocol using IPv4 and we will look a possible solution about how we actually mitigating that problem in the current internet.

(Refer Slide Time: 00:45)


Network Address Translation (NAT)

So, the concept that we are going to discuss today it is called Network Address Translation on NAT which is actually a widely used concept which is used now a days for almost all the institute network. So, the problem which we have with IPv4 addressing is that the number of IPv4 address that we have they are very limited.

So, if you look into the address space which are there. So, this address space we have primarily class A, class B, class C. These 3 sets of a 3 classes of IP addresses and then class D, IP address is for a multi cast data transfer and class E IP address is for the reserve category. So, we are not able to use this class C IP address for our general internet data transfer whereas, class D data address because they are designated for multicast data delivery in today’s internet multicast are actually rarely used it is not used widely for data transfer.

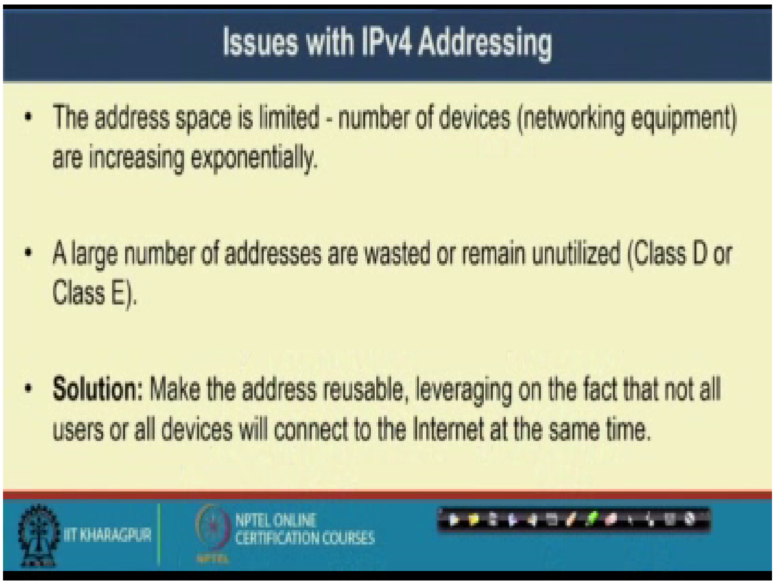
So, the address space that are reserved for the multi cast data delivery which are not use it for the normal data transfer, but that is actually being wasted or remaining underutilized. So, the 3 address, 3 classes of address that we have this class A class B and class C from class A class A, class B B or class C address. We have to allocate the address well, what we maximum do? We can apply concept of classless addressing or CIDR to combining multiple classes together or to break a single class into multiple subnets and then assign the address space to individual subnets.

But broadly if you just think of that the total number of available addresses that we have for combining class A, class B and class C although IP address is 32 bit, we are not getting 2 to the power 32 different number of addresses. We are only utilizing class A, class B class C, but inside also class this 3 classes we have this broadcast addresses, then this network addresses.

So, for every individual class A, class B or class C network, we are not able to use those broad cast address under network address to assign to a host. So, this further limits the number of available addresses that we have in the internet. And we this limitation if you just think of the number of devices that we have now a days that require an IP address, it is significantly getting boosted up. So, it is increased quite a few hundred fold from the time when IP was first introduced.

So, if you think about a number of IP addresses that we actually require is again not equal to the number of devices that we have. Many of the devices that we have nowadays, they have multiple network interfaces and actually we require one IP address for every individual interfaces. And because of that we again require further more number of IP addresses from the available address space.

(Refer Slide Time: 03:54)



Issues with IPv4 Addressing

- The address space is limited - number of devices (networking equipment) are increasing exponentially.
- A large number of addresses are wasted or remain unutilized (Class D or Class E).
- **Solution:** Make the address reusable, leveraging on the fact that not all users or all devices will connect to the Internet at the same time.

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES

So, that is the major problem with IPv4 addressing scheme that the number of address space that we have it is limited. And the number of devices that is the networking equipment that we have, they are increasing exponentially. And the large number of addresses, they are either wasted or remaining underutilized like the class D or class E IP addresses.

So, what can be a possible solution? So, a possible solution is that if we can make the address reusable. So, ideally IP addresses are not developed to support reusability because, every individual device or every individual networking equipment with the network interface card should be uniquely identified in the network.

Now, the question comes that how will you apply this reusability. Here also we apply the concept from our normal day to day life. Say my name is Sandip Chakraborty, it is not necessary that in world I am the only person who are having the name Sandip Chakraborty. So, how do we actually disambiguate two person so, whenever we are sending postal mail? So, we see that what is the location of that particular Sandip Chakraborty is it inside IIT, Kharagpur or is it say inside some other place say IIT xyz.

So, if we want to send the postal mail to Sandip Chakraborty at IIT, Kharagpur, what I have to do? I have to use or address in way that Sandip Chakraborty inside IIT Kharagpur or Sandip Chakraborty inside IIT xyz. That way you can possible try to disambiguate between two person, but again if there can be two Sandip Chakraborty inside IIT, kharagpur. Then we want to or we will possibly disambiguate based on the department and even there are two Sandip Chakraborty in the department, then I do not know how that can be done, but at some level we require uniqueness.

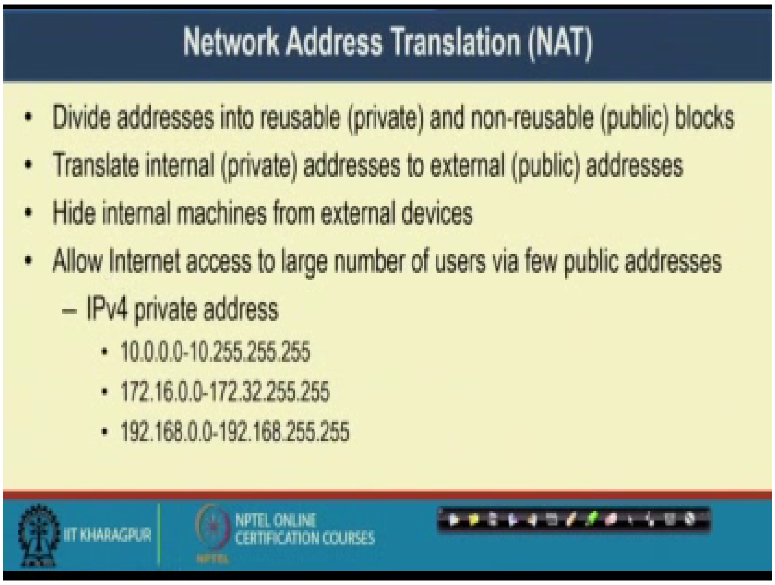
So, what we can do possibly that within an organization or within an institute possibly the name that we are using or the addresses the local addresses that we are using that can get reused. So, here by borrowing the similar kind of principle, we use the concept of reusability for IP addresses. So, what is it this reusability for the IP addresses? So, we have certain block of IP addresses which we call as the private IP addresses.

Now, this private IP addresses can be reusable. So, the private IP addresses can be put inside a IIT, Kharagpur at the same block of private IP addresses can be put in IIT Bombay or IIT Kanpur or IIT Hyderabad or any other institute in the globe. So, that way we will be possibly be able to disambiguate between two addresses by looking into whether that address is in IIT Kharagpur address or IIT Bombay address or IIT Hyderabad address or say some Stanford address.

So, that concept of reusability we need to bring in to the addressing concept. But whenever you are bringing this concept of reusability in the system, you still have a problem. That problem is that how will you route that packet or send that packet. Now to send that packet over the internet, ultimately you require an addresses which is unique in the globe. So, what you can possibly do that you can possibly disambiguate the things based on whether it is IIT Kharagpur or IIT Bombay or IIT Delhi. So, you have one address which is unique globally. So, this IIT Kharagpur it is unique globally, IIT Bombay it is unique globally, Stanford it is unique globally.

So, that way you first disambiguate whether you need to send the mail to IIT Kharagpur or IIT Delhi or a Stanford. Now once the mail is reaching there, then you send to the person concerned who is inside that institute whether it is Sandip Chakraborty or someone else inside that particular institute. So, we require a notion of publicly available name or publicly available unique address and then the private address inside that organization which can reused in multiple places.

(Refer Slide Time: 08:33)



Network Address Translation (NAT)

- Divide addresses into reusable (private) and non-reusable (public) blocks
- Translate internal (private) addresses to external (public) addresses
- Hide internal machines from external devices
- Allow Internet access to large number of users via few public addresses
  - IPv4 private address
    - 10.0.0.0-10.255.255.255
    - 172.16.0.0-172.32.255.255
    - 192.168.0.0-192.168.255.255

So, what we do in Network Address Translation on NAT? We divide the available address space into reusable address and non reusable address. So, the reusable address are the private address and the non reusable address are the public address which are unique and which are used to send the packets globally.

Now, to transfer the packet, what you have to do? You need a translation mechanism to translate the internal or the private address to the external or the public address. So, this also hide the internal machines from the external device because the external people now, they are not able to see whether the mail is going to Sandip Chakraborty or the mail is going to Soumukh K Gosh rather they are just seeing that the mail is going to IIT Kharagpur.

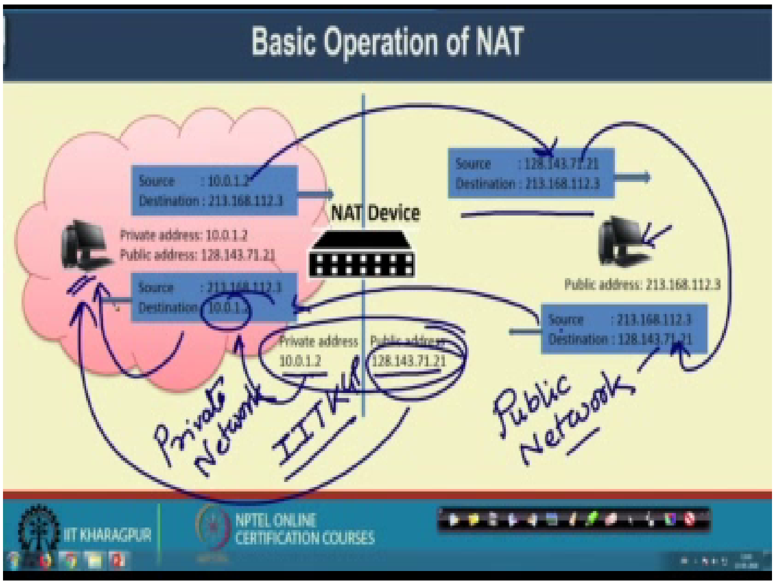
So, IIT Kharagpur is now becoming the identity the is public identity. Now once it reaches to the local people or the local postal center of IIT Kharagpur, then they disambiguate whether the mail need to be delivered to Sandip Chakraborty or that need to be delivered to Soumukh K Gosh that way we basically disambiguate the entire system.

So, you allow internet access you will be able to allow the internet access to a large number of users via few public address. Now, here is another interesting factor which is there while we are doing this private to public mapping. The interesting fact is there if you just think about the population of IIT Kharagpur the number of students or number of faculties, number of staffs who are there inside IIT Kharagpur not all of them access the internet simultaneously. Sometimes some a, students are accessing sometime the faculties are accessing or there is bounded number of users who are actually accessing the internet.

Now, the users who are accessing the internet at this moment for them, I require an IP addresses. The people who are just sleeping for them, I do not require an IP address at all. So, that way if you have a small set of pubic IP addresses, then I can possibly make a dynamic mapping between this private address that I am providing to them with this public IP; one of the public IP whenever they are waking up and trying to connect to the internet. So, that way we can ensure the reusability of the system.

Now, if you look into the IPv4 address block; the IPv4 address block gives a private addresses from individual classes of IP address pool. So, from class A we have 10 dot 0 dot 0 dot 0 to 10 dot 255 dot 255 dot 255 that is the private address range. From class B it is 172 dot 16 dot 0 dot 0 2 172 dot 32 dot 255 dot 255. From class C it is 192 dot 168 dot 0 dot 0 to 192 dot 168 dot 255 dot 255. So, from individual classes of IP addresses, you have taken one block of IP address or few block of blocks of IP addresses and designated them as the private IP address.

(Refer Slide Time: 11:45)



Basic Operation of NAT

Source : 10.0.1.2
Destination : 213.168.112.3

Private address: 10.0.1.2
Public address: 128.143.71.21

Source : 213.168.112.3
Destination : 10.0.1.2

NAT Device

Source : 128.143.71.21
Destination : 213.168.112.3

Public address: 213.168.112.3

Source : 213.168.112.3
Destination : 128.143.71.21

Private address	Public address
10.0.1.2	128.143.71.21

Now, this is the basic operation of a NAT. So, NAT is nothing, but a device a router or a gateway whatever you all it. So, in one site of the NAT, we have a private network. So, this is my private network; this is my private network and then I have my public network right. Now, in the private network, I have multiple machines who are identified by this private IP addresses. So, this is an internal machine inside the private network, you can just think of it as a IIT KGP network, say this is IIT KGP network. In the IIT KGP, network one machine is identified by this private IP address 10 dot 0 dot 1 dot 2.

Now, whenever this machine want to send the packet to the outside machine say this machine and this machine has a public address of to 13 dot 168 dot 112 dot 3. You want to send the message. So, what you do? You would prepare an IP packet and in that IP packet you have the source IP of 10 dot 0 dot 1 dot 2 the private IP of this machine and the destination is the public IP where you want to send the packet.

Now, with this private IP, you will not be able to send the packet to the outside world to the public network. So, whenever it is coming to the NAT device, what the NAT device does? It makes a mapping between the private address and the public address. So, this private address of 10 dot 0 dot 1 dot 2. It is mapped to one of the available public address which is 128 dot 143 dot 71 dot 21 and that public addresses is put to the packet which is going in the public network.

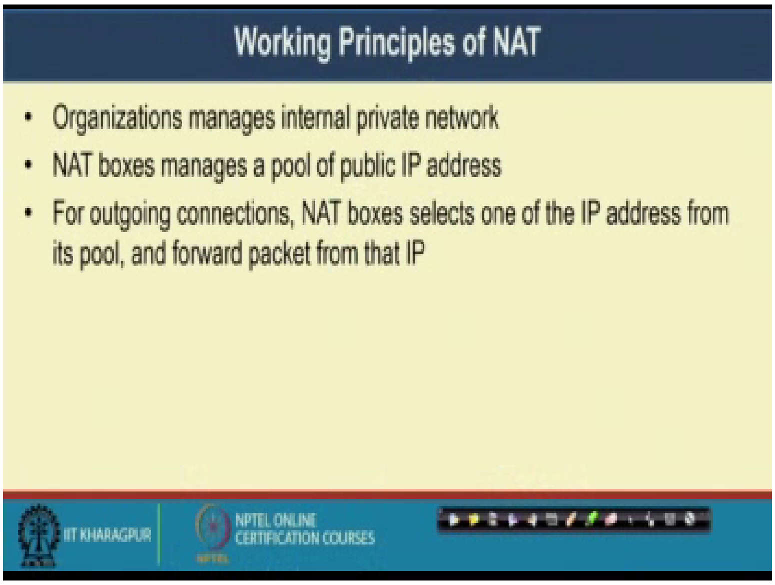
Now the NAT device is replacing this private IP with this public IP and sending the packet. Now the packet reaches to the destination. Once the destination receives that packet, it generates a reply back and in the reply it puts this source IP as the designation IP. Now, with this destination IP this 128 dot 143 dot 71 dot 21, this is an IP which is associated with this NAT device. So, this device is actually having a pool of IP addresses associated with them. So, any packet to those IP addresses will be delivered to that NAT device. So, the packet is delivered to the NAT device. When the packet is coming to the NAT device the NAT device is maintaining this NAT table where it has maintained a mapping between with the private address and the public address.

Now, what it does it finds out that well this public address has given to this machine. So, it replaces the source address; this particular destination address with the private address. Now whenever this packet is coming to the inside network, the address the destination address is replaced from the public address to the corresponding private address and with that private address the packet is delivered to this machine.

That is the way NAT works. So, now, you can see that every individual machine inside that network may have one private IP address and you do not require that many of public IP address because all the machines are not getting connected to the internet simultaneously. So, you require a small set of public IP addresses may be the number of users who are getting connected to the internet simultaneously. And then whenever a user request send the packet to the NAT, the NAT just make an address translation from a private IP to a public IP. Put that information to the local NAT table to the map and then transfer that packet to the outside world. And whenever the packet reaches to the destination machine, the destination machine reply back to you by using that public IP address; the source IP now become the destination IP.

So, that packet traverses to the network and reaches to the NAT device. Once the NAT device receives that packet, it again look into the NAT table to find the mapping the reverse mapping better to say. So, from the reverse mapping, it finds out that well this particular public IP was given to this machine with the private IP. It make a replacement in the destination IP and send it back to the internal network and the internal network forward that packet to the final destination. Well. So, that is the entire operation or the idea of NAT.

(Refer Slide Time: 16:27)

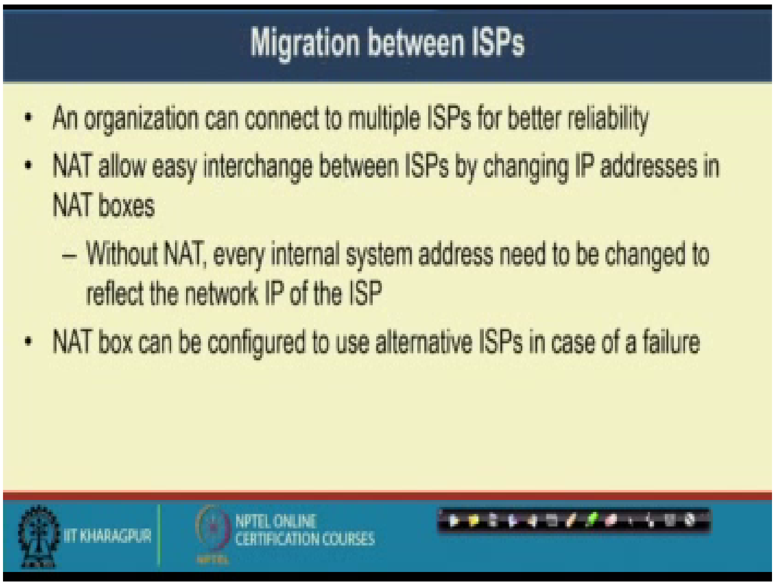


Working Principles of NAT

- Organizations manages internal private network
- NAT boxes manages a pool of public IP address
- For outgoing connections, NAT boxes selects one of the IP address from its pool, and forward packet from that IP

Now, in NAT the organization, they manages the internal private network and the NAT boxes. NAT boxes are nothing, but routers they manages a pool of public IP address, For outgoing connection the NAT boxes, they select one of the IP address from its pool and forward the packet from that IP.

(Refer Slide Time: 16:48)



Migration between ISPs

- An organization can connect to multiple ISPs for better reliability
- NAT allow easy interchange between ISPs by changing IP addresses in NAT boxes
  - Without NAT, every internal system address need to be changed to reflect the network IP of the ISP
- NAT box can be configured to use alternative ISPs in case of a failure

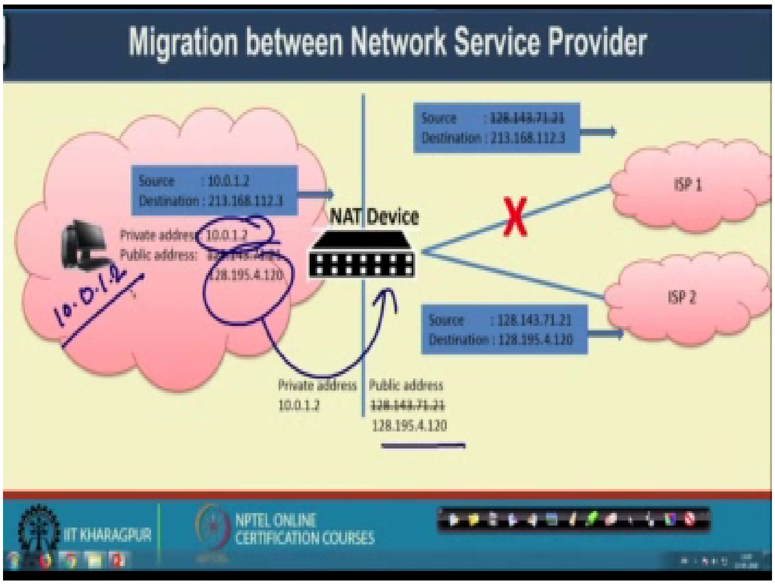
IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES

Now, NAT has multiple interesting use cases apart from supporting more number of users with the help of a limited public IP. One interesting fact is whenever you want to migrate between different ISP. Now an organization can connect to multiple ISPs for better reliability. So, for example, IIT Kharagpur network is connected to ERNET network as well as (Refer Time: 17:13) network. They have multiple outgoing network, we call it as a multi home network.

Now, this NAT it allows a easy interchange between the ISPs by changing the IP address in the NAT boxes. So, whenever you are making a change of the ISP your public address IP address pool is getting changed, but the internal machines you do not need to reconfigure the IP address for all the internet internal machines which are there inside IIT Kharagpur. They are having their fixed private IP address and only a mapping is being done to the corresponding ISP address to which the NAT box which is working like a gateway is currently connected.

So, without NAT what you have to do that every internal system address need to be changed to reflect the network IP of the ISP, but here you do not require that the net box will take care of that. So, you do not need to make a change into the internal machine.

(Refer Slide Time: 18:11)



Migration between Network Service Provider

Source : 10.0.1.2
Destination : 213.168.112.3

Private address: 10.0.1.2
Public address: ~~128.143.71.21~~
128.195.4.120

Source : ~~128.143.71.21~~
Destination : 213.168.112.3

Source : 128.143.71.21
Destination : 128.195.4.120

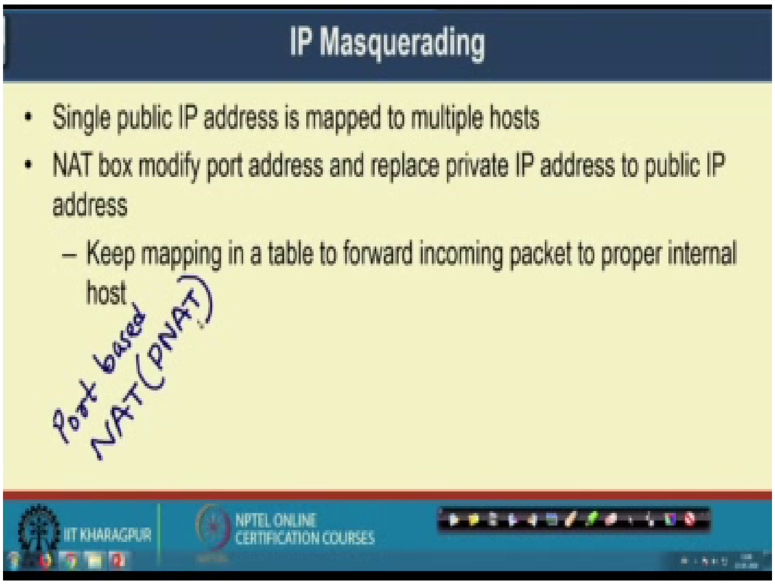
Private address 10.0.1.2

Public address ~~128.143.71.21~~ 128.195.4.120

So, here is an example like say initially the NAT device was connected to ISP 1 when it was connected to ISP 1 during that time you are giving the address from a pool of 128 143 dot 71 dot 21. The now the moment this ISP got a failure or something happened, then the NAT device gets connected to ISP 2. It start giving address from a different address pool say from 128 dot 195 dot 4 dot 120.

So, only thing is that the public address gets changed and these public address are managed by the NAT device. But the private IP that 10 dot 0 dot 1 dot 2 which was assigned to this particular machine that remains as it is. So, that address do not need to change. So, you do not need to reconfigure every machine independently to reflect these changes.

(Refer Slide Time: 19:12)



IP Masquerading

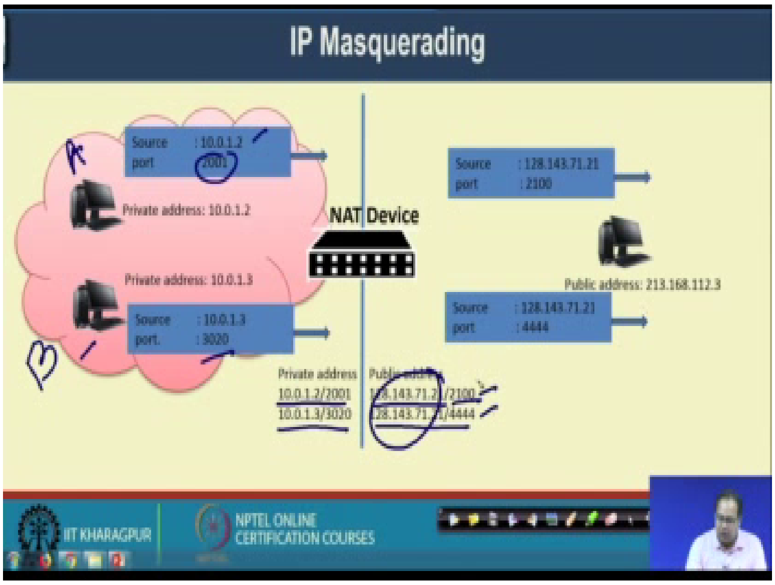
- Single public IP address is mapped to multiple hosts
- NAT box modify port address and replace private IP address to public IP address
  - Keep mapping in a table to forward incoming packet to proper internal host

Port based NAT(PNAT)

Now another interesting thing is in NAT is that you can utilize something called IP masquerading. So, what is IP masquerading it is like that, you have a single public IP address which you can map to multiple host. Now how you can do that? You can actually use the port address along with the IP address. So, this concept is interesting in the context of in the context of NAT. So, what you are doing here that. So, it is basically an extension of NAT which is sometime called as a port based NAT or PNAT.

Now, in PNAT what happens that one? So, ultimately if you think about the communication the communications are basically a process to process communication one process at the source machine is communicating with another process at the destination machine. So, these process system are in identified the IP address of the machine plus a port number. So, this port numbers are used to uniquely identify a process which is running inside a machine. Now, you can use this IP port pair actually together to make this mapping. So, how you can do that?

(Refer Slide Time: 20:48)



IP Masquerading

Private address	Public address
10.0.1.2/2001	128.143.71.21/2100
10.0.1.3/3020	128.143.71.21/4444

So, let us see one example here. So, this is the thing say assume that one application is running to this machine at port 2001 that has a private IP of 10 dot 0 dot 1 dot 2. There is another machine say this is machine A, this is machine B. In machine B, it is using a different private address 10 dot 0 dot 1 dot 3 and the application is running at port 3020.

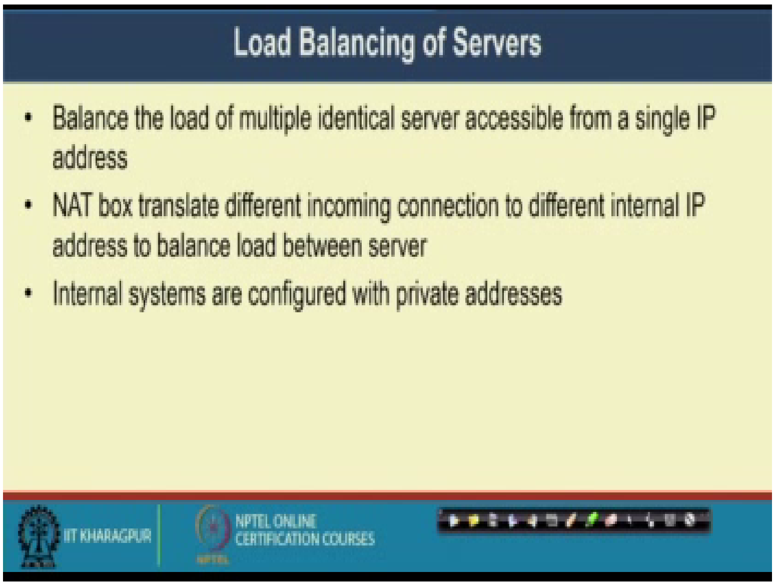
Now, whenever these packets are going outside and they are trying to communicate to some public machine same or different that is immaterial to us. So, whenever these things are being happen during that time, what the NAT device now do? NAT device makes a mapping of this IP port to another IP port. So, what happens here that this particular private IP and the port number is being mapped to a public address and one port. The second private IP and the port is mapped to another public IP and the port.

Now, here I can use the same public IP for both the machine because this port number is actually making the differentiation. So, whenever I will get a response, if I am getting a response at port 2100 of the IP 128 dot 143 dot 71 dot 21, I know that in the reverse mapping that will be mapped to 10 dot 0 dot 1 dot 2 at port 2001. Similarly if you are receiving a packet at the NAT device at port 4444 from this particular mapping you know that this IP port pair will be mapped to 10 dot 0 dot 1 dot 3, it port 3020.

So, that way now you can support more number of users with a very limited number of IP addresses because any way you have around 65000 more than 65000 different number of ports. If I even remove the reserve port address, still you have some port numbers in the order of 10000 even it is something similar to 50000 that many different unique port number you have.

So, that is why if you have a very few public IP addresses. With that very few public IP addresses by making a mapping with IP port pair, you can actually support a large number of users in the private network. And for them you can use the same public IP, but with different port number and the mapping is basically done based on the IP port pair ok. So, that is the concept of IP masquerading to which you can support again large number of users inside the private network.

(Refer Slide Time: 23:31)



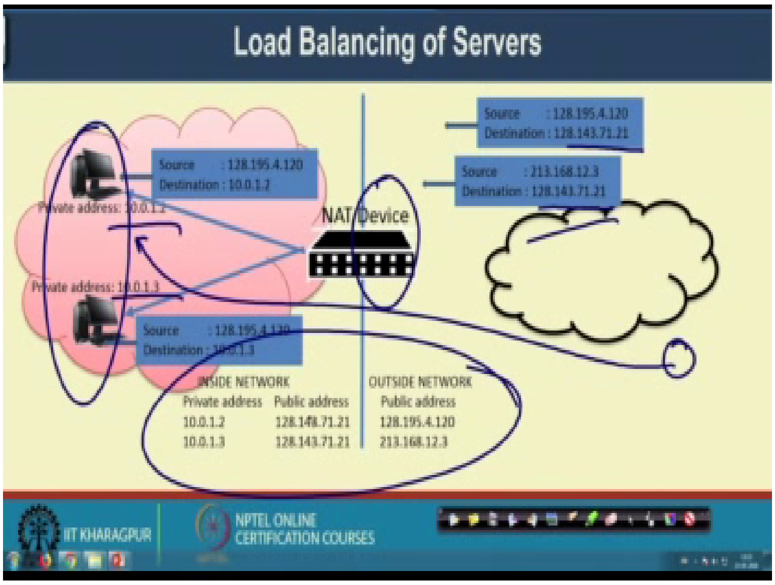
Load Balancing of Servers

- Balance the load of multiple identical server accessible from a single IP address
- NAT box translate different incoming connection to different internal IP address to balance load between server
- Internal systems are configured with private addresses

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES

And well another use case in NAT is that it can help in doing a load balancing of servers. So, balances of load of identical server, they are accessible from a single IP address. So, the NAT box it translate the different incoming connections to different internal IP addresses to balance the load between the server and the internal systems are now configured with private address.

(Refer Slide Time: 23:57)



Load Balancing of Servers

INSIDE NETWORK		OUTSIDE NETWORK
Private address	Public address	Public address
10.0.1.2	128.143.71.21	128.195.4.120
10.0.1.3	128.143.71.21	213.168.12.3

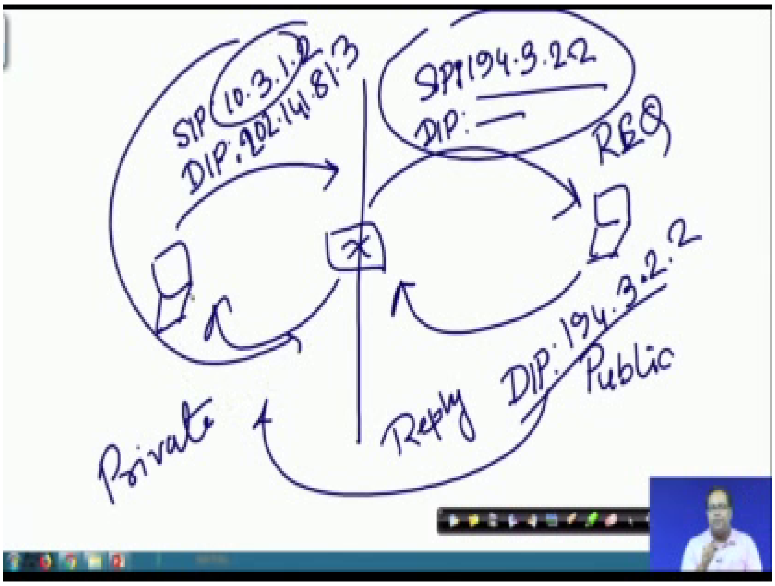
So, an example is something like this that whenever you are getting the request, you are getting the request to the same destination IP; that means, 128 dot 143 dot 71 dot 21. And the whenever this particular request are coming to the NAT device based on the load the NAT device can redirect some of the machines some of the request to one machine at 10 dot 0 dot 1 dot 2 and some of the request to a different machine at 10 dot 0 dot 1 dot 3.

So, that way the same public IP is mapped to multiple private IP and the NAT can do actually the load balancing by distributing the requests to the multiple private IP addresses. Now, you can think of this machine such the web servers and you have to different copies of the web server. And whenever the web request are coming to this particular IP address 128 dot 143 dot 7 dot 21. So, you are making a mapping to one of the private address either 10 dot 0 dot 1 dot 2 or 10 dot 0 dot 1 dot 3 based on the availability. And or based on the load balancing principle and then send the request to those particular machine.

Now, this is the broad idea of NAT. Now one limitation of NAT is that see, you need to show to have someone from outside to communicate with this particular machine, they need to have this particular mapping in the NAT device. So, unless you have this mapping in the NAT device, you will not be able to serve a outside request. So, that is why if you are behind the NAT during the time, someone from outside will not be able to directly connect to you unless they have the information of the public IP of the NAT box.

So, whenever you are making a connection from inside, during that time you are actually allowing the outside machine to get a information about the public IP address through this source destination IP pair.

(Refer Slide Time: 25:59)

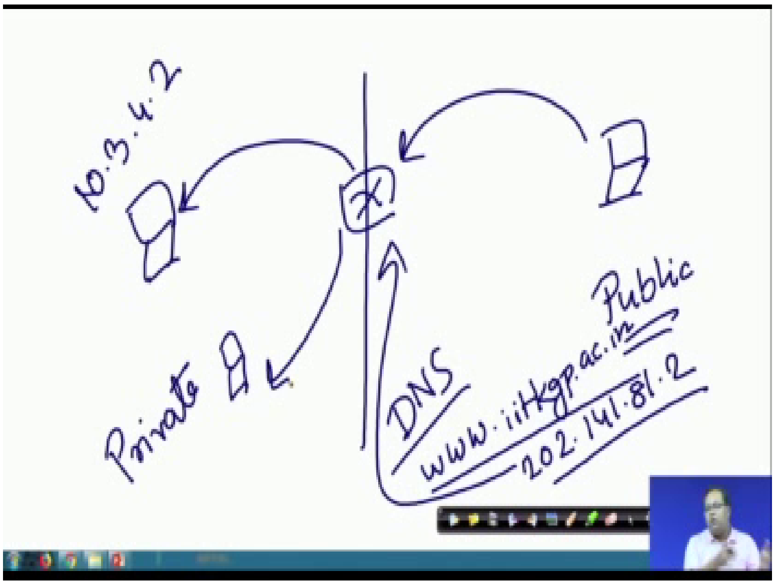


So, assume that this is your NAT boundary and you have the NAT box. One machine is there inside and this is the machine at the public domain. So, this is my public domain and this is my private domain.

Now, whenever you are sending the packet if the connection is initiated from inside, then you have the source IP as a private IP say 10 dot 0 dot 1 dot 2 and destination IP as a public IP say 202 dot 141 dot 81 dot 3. And whenever the packet is going outside, the NAT box is making a change to this source IP source IP to some public IP say 194 dot 3 dot 2 dot 2 and the destination IP as earlier. And then this machine whenever it is receiving this particular message from this IP, it can comes to know that well this should be my destination IP the source IP in the request. So, that was the request message.

The source IP at the request should be the destination IP at the reply. So, it uses destination IP in the reply message. It uses the destination IP as this is 194 dot 3 dot 2 dot 2 and send that packet back. When it is comes to NAT, then the NAT makes an change makes this destination IP, change to this source IP and the packet as forwarded to the internal machine.

(Refer Slide Time: 28:24)



But if the internal machine is not initiating the connection, during that time the life is difficult. During that time, what you have to do that say, this is my internal machine in the private domain and this is the machine at the public domain. Now, in that case here is the NAT box now, this public machine does not cannot send the packet to this internal IP of 10 dot 3 dot some 4 dot 2. It need to know the public IP of the NAT box. So, unless you have a information of the public IP of the NAT box, this machine in the public domain will not be able to initiate a connection.

Now, to solve this problem people use DNS. So, in that case of DNS, you have a mapping so, rather than naming these things the example that I have given as a web server. So, for IIT Kharagpur, we have these dub dub dub dot iit kgp dot ac dot in. And whenever you are accessing a machine with this DNS name, the DNS actually has the IP of corresponds to which is mapped to dub dub dub dot iit kgp dot ac dot in say something like 202 dot 141 dot 81 dot 2 and this particular IP is mapped to a IP of the NAT box.

So, whenever the request comes, so we have multiple web servers multiple copies of the web servers. Based on the load balancing principle, it forwards the request to one of the machines which are internal to the private network. So, that way by using DNS, we sometime resolve this problem whenever we require this kind of load balancing. But in general unless you have the IP of the NAT box, you will not be able to initiate a connection from the outside world or from the public world. You need to initiate the connection from the private network or from the internal network.

So, that is all about this concept of network address translation which is actually a very useful mechanism to support large number of nodes with the help of IP version 4. And the in the next class, we look into IP version 6. Although IP version 6 is not a very successful protocol and although the network design understood long back that IPv 6 is required, but till now people are not able to successfully deploy IPv 6 globally for every purpose.

IPv 6 provides more number of address space compared to IPv4 and it has nice mechanism of managing the IP protocol. Although that is not a success, but in many of the places in Iceland wise IPv 6 are being used recently people are exploring IPv 6 for internet (Refer Time: 31:28) communication. So, in the next class, we will briefly look into the basic principles of IPv 6 protocol and look in to the way people are trying to make a mapping or make a compatibility between the IPv4 addressing mechanism and the IPv 6 addressing mechanism.

Thank you all for attending the class today, see you in the next class.