The document contains four application notes:

A. How do I configure Virtual Server to allow external users' access to internal servers (Web, FTP, etc.) located behind the router?

Network Environment:

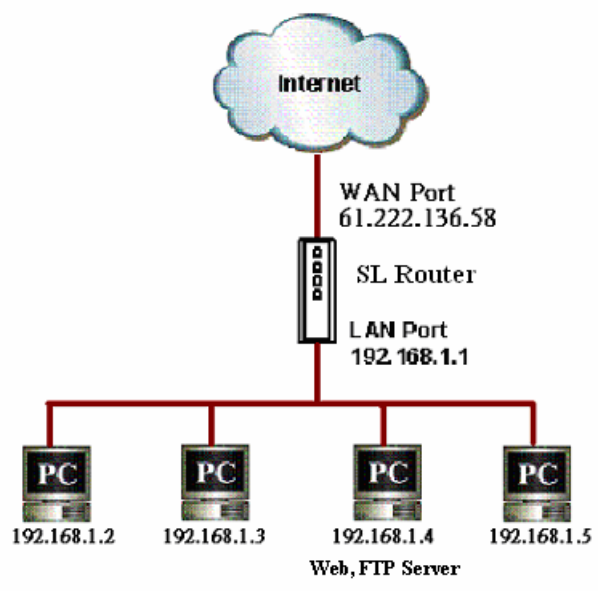
IP provided from ISP: 61.222.136.58 (fixed IP)

Subnet mask: 255.255.255.255

Default Gateway: 61.222.136.254

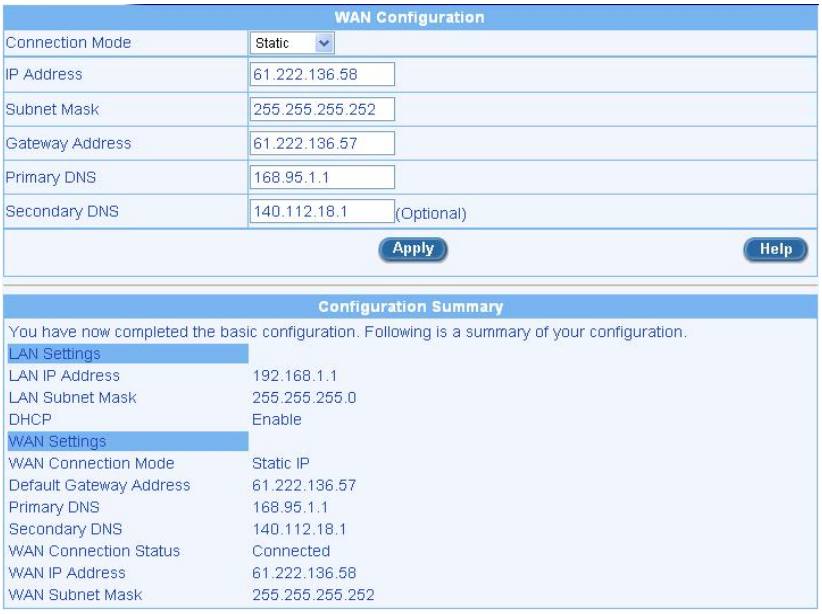
Router LAN IP: 192.168.1.1

Internal Server IP: 192.168.1.4



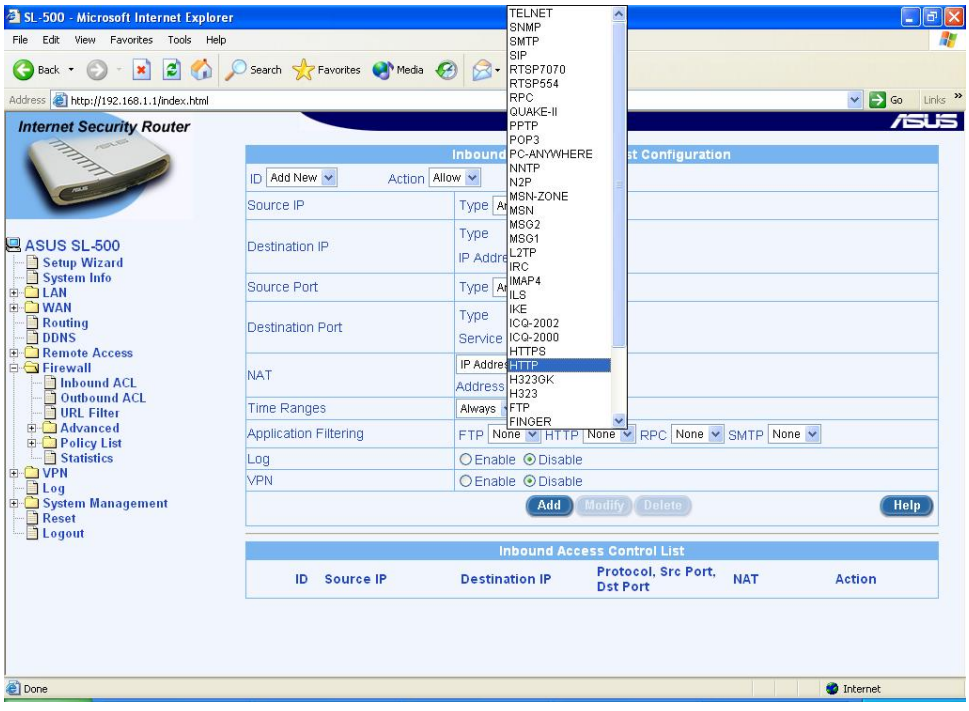
1. Configure WAN IP

   Login to Web management interface and enter **WAN>WAN.** Select **Static IP** and set 61.222.136.58 as the WAN IP. Fill in other fields according to the information provided by your ISP.



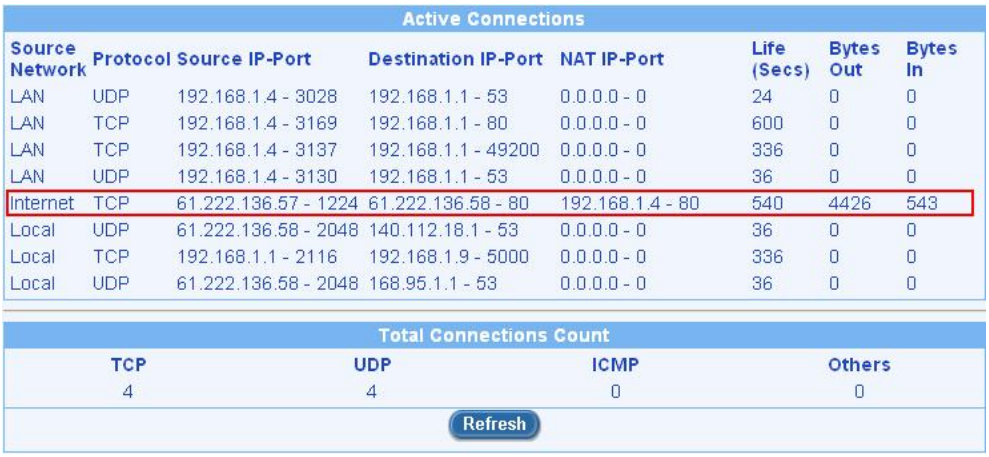
2. Configure an inbound ACL rule

   Click **Firewall>Inbound ACL** from function tree in left to configure an inbound ACL rule. Consider to set up a Web server in LAN, select predefined ”HTTP” from **Service** option for **Destination Port.** If you locate a FTP server, select “FTP”. The chosen option can be based on your actual requirement.



If the desired application is not listed, choose **Single** in order to define a specific port number or go to **Firewall>Advanced>Service** to define a service with related port number. A completed inbound ACL rule for a Web server is as follows:

3. After the inbound connection is established, you can check connection and NAT information in **Firewall>Statistics**.

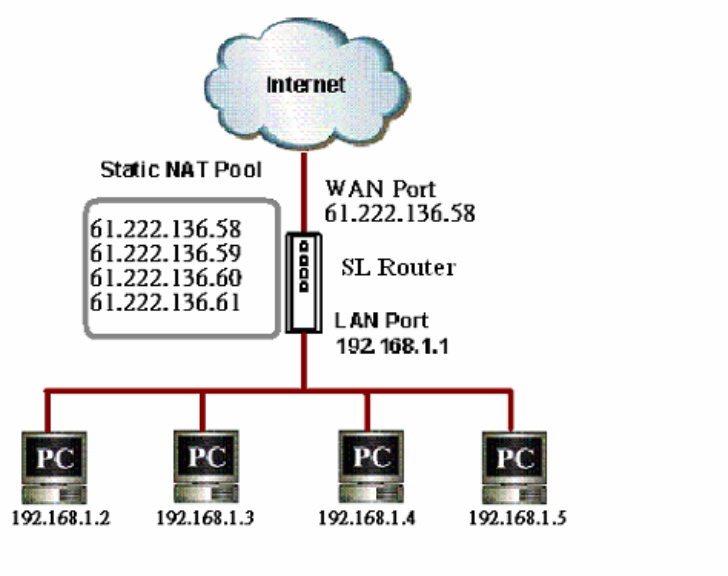


B. How do I open Port Mapping in order to allow users from Internet bypass the firewall and connect to internal hosts?

Please refer to the instructions in Part A.

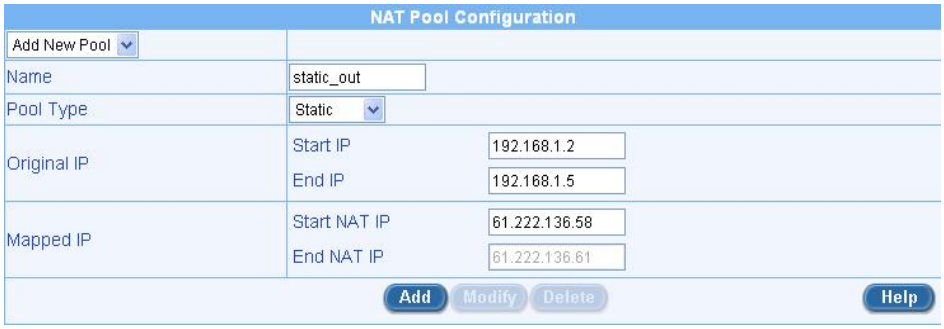
C. Only one static IP can be set to WAN interface in "Static" mode. How do I configure the router for multiple and static IP mapping between internal and external networks?

Network Environment:
IP provided from ISP: 61.222.136.58~61
Subnet mask: 255.255.255.248
Default Gateway: 61.222.136.57
Router LAN IP: 192.168.1.1
Internet Hosts: 192.168.1.2~5 (manually configured IP with default gateway as the Router LAN IP: 192.168.1.1)

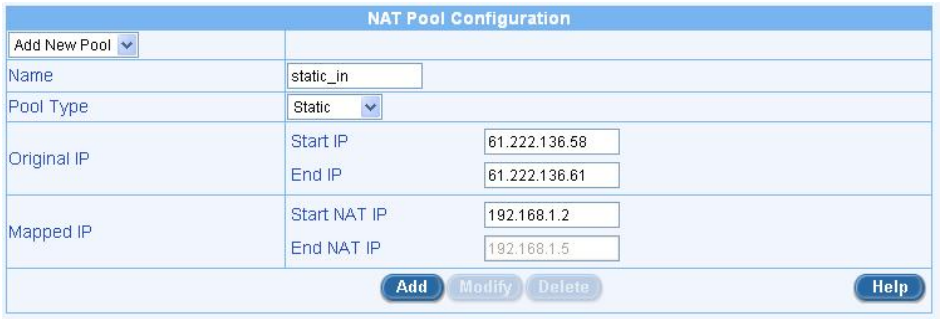


1. Configure WAN IP:
   Login to Web management interface and enter **WAN>WAN.** Select **Static IP** and set 61.222.136.58 as the WAN IP. Fill in other fields according to the information provided by your ISP.

2. Configure a static NAT Pool (internal->external):
   Click **Firewall>Policy List>NAT Pool** from function tree in left, select **Static NAT.** Set IP range of LAN hosts in **Original IP** and set IP range of WAN to **Mapped IP,** click **Add**. It's a static NAT mapping from internal network to external network.
   192.168.1.2 → 61.222.136.58
   192.168.1.3 → 61.222.136.59
   192.168.1.4 → 61.222.136.60
   192.168.1.5 → 61.222.136.61



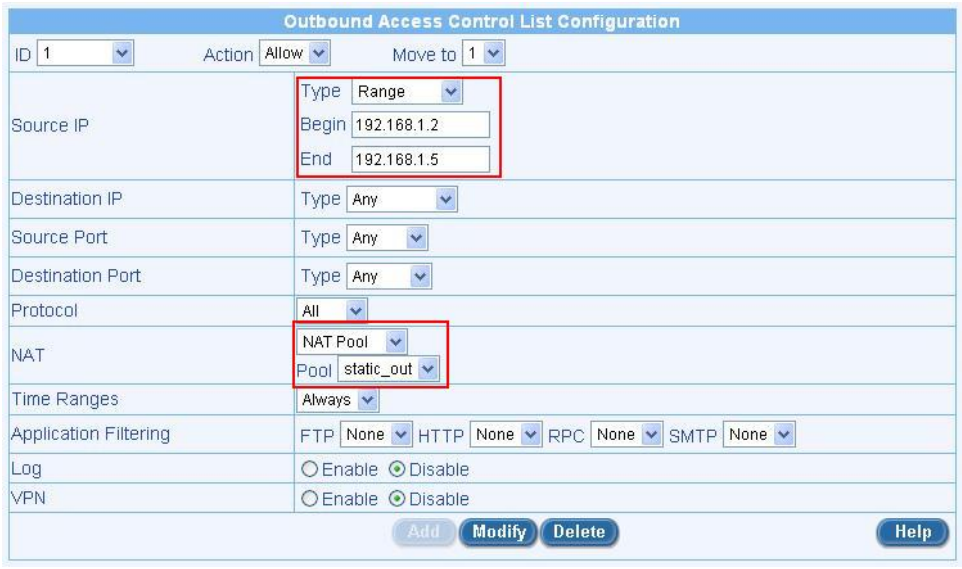
You may need to create a static NAT mapping from external network to internal network. Note that the action may not be necessary. Please refer to step 4 for more details.



The Static NAT mapping will be displayed.

3. Configure an outbound ACL rule

   Click **Firewall>Outbound ACL** and configure an outbound ACL rule. The following configuration means the router will translate and map source IP 192.168.1.2~192.168.1.5 to the real IP range defined in NAT pool. As the result, source IP in outgoing packets from the router represents the real IP, not the internal IP.



4. If you intend to allow external users bypass the firewall and access to internal hosts, you need to create an inbound ACL rule as below in **Firewall>Inbound ACL**.

Above configuration represents incoming packets destined for IP 61.222.136.58~61 will be redirected and mapped to internal hosts according to the predefined static NAT mapping.

61.222.136.58 →192.168.1.2
61.222.136.59 →192.168.1.3
61.222.136.60 →192.168.1.4
61.222.136.61 →192.168.1.5

Note: This example doesn't filter source IP, destination port and protocol in incoming packets. It means incoming packets destined for IP 61.222.136.58~61 will pass through firewall without any prohibition. Consider network security, you can block incoming packets by filtering certain types based on your requirement.

D. Destination IP of incoming packets is different from WAN IP but the two IPs are in the same subnet? How do I configure the router to conduct static IP mapping between the destination IP and corresponding internal IP?

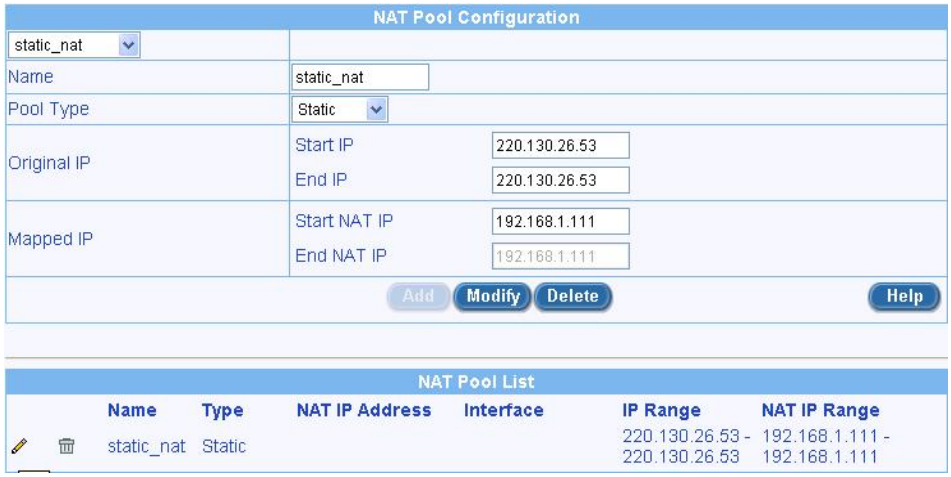
Consider remote desktop application in Windows XP as an example and network environment as follows.

IP provided from ISP: 220.130.26.50~54
Router WAN IP: 220.130.26.52
Subnet mask: 255.255.255.248
Default Gateway: 220.130.26.49
Router LAN IP: 192.168.1.1
Internal host for remote desktop access: 192.168.111 (default gateway is Router LAN IP: 192.168.1.1)
Destination IP targeted by remote desktop client: 220.130.26.53 (different from WAN IP, but they are in the same subnet.)

1. Configure WAN IP:

Configuration Summary	
You have now completed the basic configuration. Following is a summary of your configuration.	
LAN Settings	
LAN IP Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP	Enable
WAN Settings	
WAN Connection Mode	Static IP
Default Gateway Address	220.130.26.49
Primary DNS	168.95.1.1
Secondary DNS	168.95.192.1
WAN Connection Status	Connected
WAN IP Address	220.130.26.52
WAN Subnet Mask	255.255.255.248

2. Configure NAT Pool:



3. Configure an inbound ACL rule:

4. After remote desktop connection is established, you can check connection and NAT information in **Firewall>Statistics**.