

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? .....P1
- B. How do I open Port Mapping in order to allow users from Internet bypass the firewall and connect to internal hosts? .....P3
- 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? .....P4
- 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? .....P7

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

Network Environment:

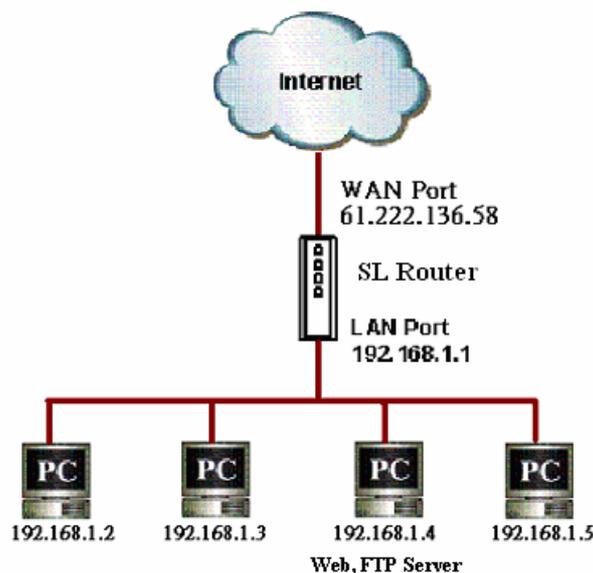
IP provided from ISP: 61.222.136.58 (fixed IP)

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.

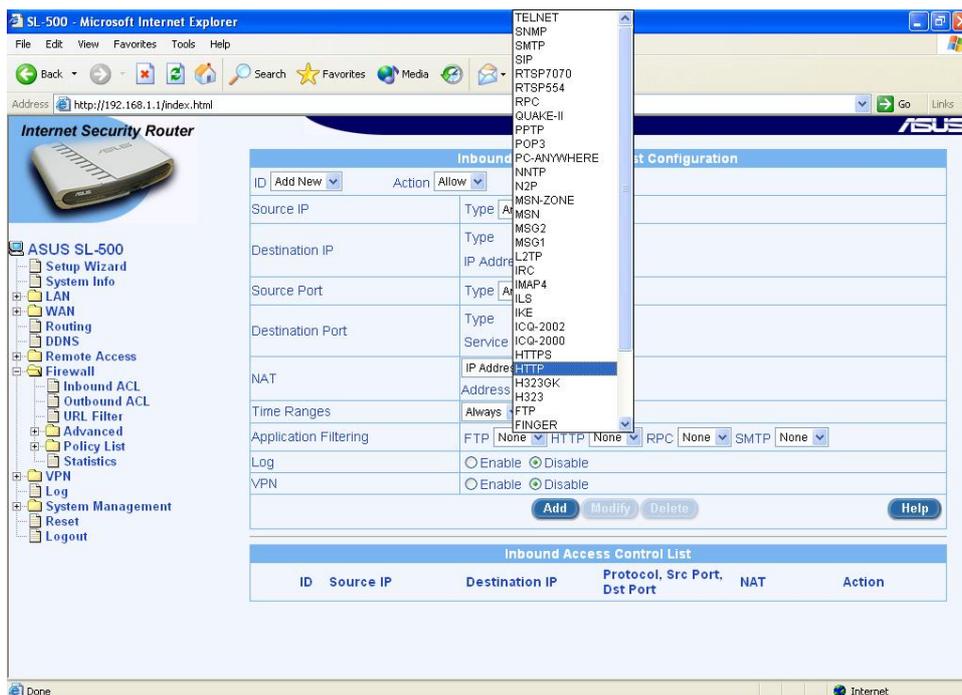
WAN Configuration	
Connection Mode	Static
IP Address	61.222.136.58
Subnet Mask	255.255.255.252
Gateway Address	61.222.136.57
Primary DNS	168.95.1.1
Secondary DNS	140.112.18.1 (Optional)
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Configuration Summary	
You have now completed the basic configuration. Following is a summary of your configuration.	
<b>LAN Settings</b>	
LAN IP Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP	Enable
<b>WAN Settings</b>	
WAN Connection Mode	Static IP
Default Gateway Address	61.222.136.57
Primary DNS	168.95.1.1
Secondary DNS	140.112.18.1
WAN Connection Status	Connected
WAN IP Address	61.222.136.58
WAN Subnet Mask	255.255.255.252

## 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.



ID	Source IP	Destination IP	Protocol, Src Port, Dst Port	NAT	Action

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:

Inbound Access Control List Configuration	
ID	1
Action	Allow
Move to	1
Source IP	Type Any
Destination IP	Type IP Address IP Address 61.222.136.58
Source Port	Type Any
Destination Port	Type Service Service HTTP
NAT	IP Address Address 192.168.1.4
Time Ranges	Always
Application Filtering	FTP None HTTP None RPC None SMTP None
Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
VPN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>	

Inbound Access Control List						
ID	Source IP	Destination IP	Protocol, Src Port, Dst Port	NAT	Action	
1	Internet	61.222.136.58	HTTP(TCP,80)	192.168.1.4	Allow	

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

Active Connections							
Source Network	Protocol	Source IP-Port	Destination IP-Port	NAT IP-Port	Life (Secs)	Bytes Out	Bytes In
LAN	UDP	192.168.1.4 - 3028	192.168.1.1 - 53	0.0.0.0 - 0	24	0	0
LAN	TCP	192.168.1.4 - 3169	192.168.1.1 - 80	0.0.0.0 - 0	600	0	0
LAN	TCP	192.168.1.4 - 3137	192.168.1.1 - 49200	0.0.0.0 - 0	336	0	0
LAN	UDP	192.168.1.4 - 3130	192.168.1.1 - 53	0.0.0.0 - 0	36	0	0
Internet	TCP	61.222.136.57 - 1224	61.222.136.58 - 80	192.168.1.4 - 80	540	4426	543
Local	UDP	61.222.136.58 - 2048	140.112.18.1 - 53	0.0.0.0 - 0	36	0	0
Local	TCP	192.168.1.1 - 2116	192.168.1.9 - 5000	0.0.0.0 - 0	336	0	0
Local	UDP	61.222.136.58 - 2048	168.95.1.1 - 53	0.0.0.0 - 0	36	0	0

Total Connections Count			
TCP	UDP	ICMP	Others
4	4	0	0

### 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:

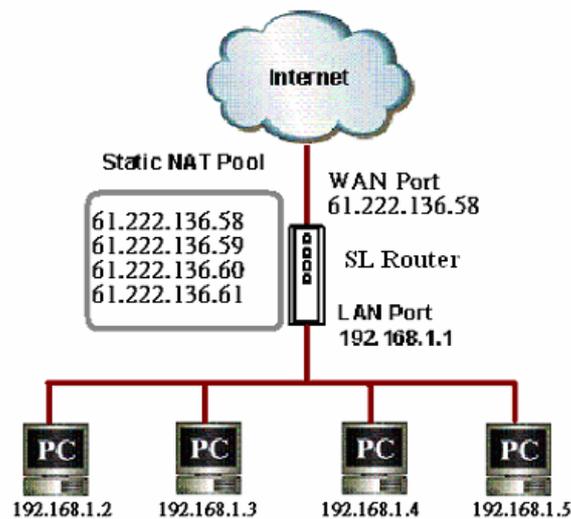
IP provided from ISP: 61.222.136.58~61

Subnet mask: 255.255.255.248

Default Gateway: 61.222.136.57

Router LAN IP: 192.168.1.1

Internal 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.

WAN Configuration	
Connection Mode	Static
IP Address	61.222.136.58
Subnet Mask	255.255.255.252
Gateway Address	61.222.136.57
Primary DNS	168.95.1.1
Secondary DNS	140.112.18.1 (Optional)
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Configuration Summary	
You have now completed the basic configuration. Following is a summary of your configuration.	
<b>LAN Settings</b>	
LAN IP Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP	Enable
<b>WAN Settings</b>	
WAN Connection Mode	Static IP
Default Gateway Address	61.222.136.57
Primary DNS	168.95.1.1
Secondary DNS	140.112.18.1
WAN Connection Status	Connected
WAN IP Address	61.222.136.58
WAN Subnet Mask	255.255.255.252

## 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

NAT Pool Configuration			
<input type="button" value="Add New Pool"/>			
Name	static_out		
Pool Type	Static		
Original IP	Start IP	192.168.1.2	
	End IP	192.168.1.5	
Mapped IP	Start NAT IP	61.222.136.58	
	End NAT IP	61.222.136.61	
<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>			

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.

NAT Pool Configuration			
<input type="button" value="Add New Pool"/>			
Name	static_in		
Pool Type	Static		
Original IP	Start IP	61.222.136.58	
	End IP	61.222.136.61	
Mapped IP	Start NAT IP	192.168.1.2	
	End NAT IP	192.168.1.5	
<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>			

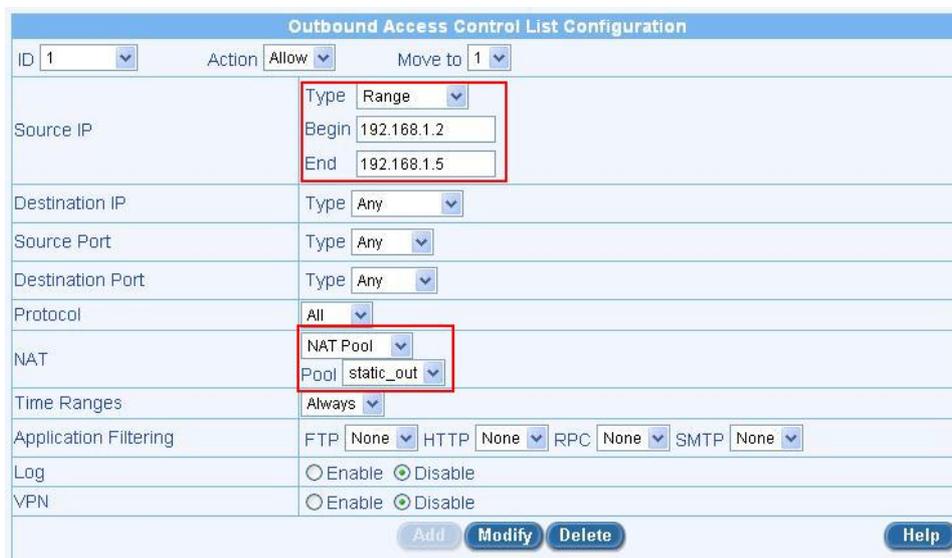
The Static NAT mapping will be displayed.

NAT Pool List						
	Name	Type	NAT IP Address	Interface	IP Range	NAT IP Range
		static_out	Static		192.168.1.2 - 192.168.1.5	61.222.136.58 - 61.222.136.61
		static_in	Static		61.222.136.58 - 61.222.136.61	192.168.1.2 - 192.168.1.5

### 3. Configure an outbound ACL rule

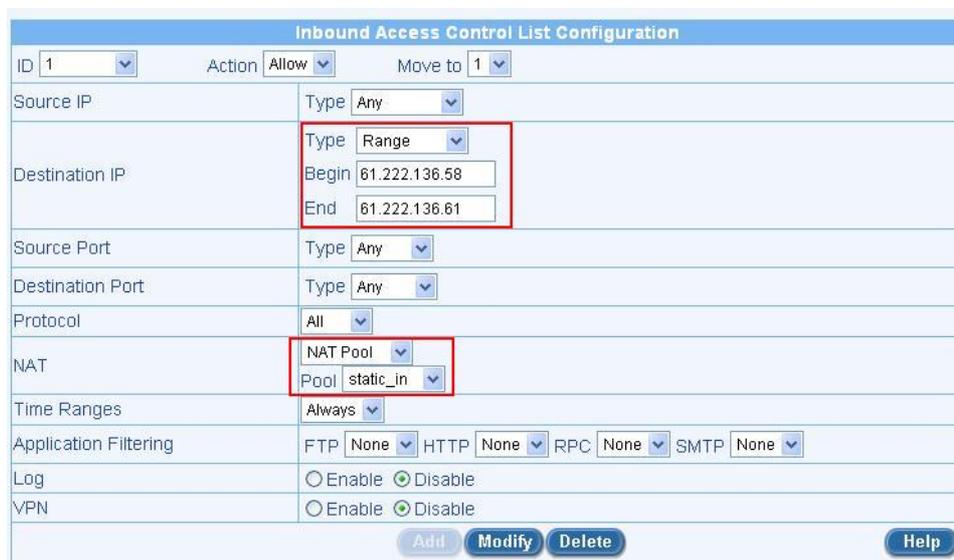
Click **Firewall>Outbound ACL** and configure an outbound ACL rule. The following configuration means the router will translate and map source IP

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.



The screenshot shows the 'Outbound Access Control List Configuration' window. The ID is 1, Action is Allow, and Move to is 1. The Source IP is configured with Type 'Range', Begin '192.168.1.2', and End '192.168.1.5'. The Destination IP is 'Any'. Source Port and Destination Port are 'Any'. Protocol is 'All'. The NAT Pool is 'static\_out'. Time Ranges are 'Always'. Application Filtering is set to 'None' for FTP, HTTP, RPC, and SMTP. Log and VPN are both 'Disable'. Buttons for Add, Modify, Delete, and Help are at the bottom.

### 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**.



The screenshot shows the 'Inbound Access Control List Configuration' window. The ID is 1, Action is Allow, and Move to is 1. The Destination IP is configured with Type 'Range', Begin '61.222.136.58', and End '61.222.136.61'. The Source IP is 'Any'. Source Port and Destination Port are 'Any'. Protocol is 'All'. The NAT Pool is 'static\_in'. Time Ranges are 'Always'. Application Filtering is set to 'None' for FTP, HTTP, RPC, and SMTP. Log and VPN are both 'Disable'. Buttons for Add, Modify, Delete, and Help are at the bottom.



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: 192.168.1.11 (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.	
<b>LAN Settings</b>	
LAN IP Address	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP	Enable
<b>WAN Settings</b>	
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:

**NAT Pool Configuration**

static\_nat

Name: static\_nat

Pool Type: Static

Original IP: Start IP: 220.130.26.53, End IP: 220.130.26.53

Mapped IP: Start NAT IP: 192.168.1.111, End NAT IP: 192.168.1.111

[Add] [Modify] [Delete] [Help]

---

**NAT Pool List**

Name	Type	NAT IP Address	Interface	IP Range	NAT IP Range
static_nat	Static			220.130.26.53 - 220.130.26.53	192.168.1.111 - 192.168.1.111

3. Configure an inbound ACL rule:

**Inbound Access Control List Configuration**

ID: 1, Action: Allow, Move to: 1

Source IP: Type: Any

Destination IP: Type: IP Address, IP Address: 220.130.26.53

Source Port: Type: Any

Destination Port: Type: Single, Port Number: 3389

Protocol: TCP

NAT: NAT Pool, Pool: static\_nat

Time Ranges: Always

Application Filtering: FTP: None, HTTP: None, RPC: None, SMTP: None

Log:  Enable,  Disable

VPN:  Enable,  Disable

[Add] [Modify] [Delete] [Help]

---

**Inbound Access Control List**

ID	Source IP	Destination IP	Protocol, Src Port, Dst Port	NAT	Action
1	Internet	220.130.26.53	TCP, All, 3389	static_nat	Allow

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

**Active Connections**

Source Network	Protocol	Source IP-Port	Destination IP-Port	NAT IP-Port	Life (Secs)	Bytes Out	Bytes In
LAN	TCP	192.168.1.111 - 3342	192.168.1.1 - 80	0.0.0.0 - 0	600	0	0
LAN	TCP	192.168.1.111 - 3340	192.168.1.1 - 80	0.0.0.0 - 0	8	0	0
LAN	TCP	192.168.1.111 - 3341	192.168.1.1 - 80	0.0.0.0 - 0	8	0	0
LAN	UDP	192.168.1.111 - 3091	192.168.1.1 - 53	0.0.0.0 - 0	60	0	0
LAN	UDP	192.168.1.111 - 3339	192.168.1.1 - 53	0.0.0.0 - 0	48	0	0
LAN	UDP	192.168.1.111 - 1025	192.168.1.1 - 53	0.0.0.0 - 0	60	0	0
LAN	UDP	192.168.1.111 - 3281	192.168.1.1 - 53	0.0.0.0 - 0	60	0	0
LAN	UDP	192.168.1.111 - 3274	192.168.1.1 - 53	0.0.0.0 - 0	60	0	0
LAN	UDP	192.168.1.111 - 3272	192.168.1.1 - 53	0.0.0.0 - 0	60	0	0
LAN	UDP	192.168.1.111 - 3273	192.168.1.1 - 53	0.0.0.0 - 0	60	0	0
LAN	UDP	192.168.1.111 - 3270	192.168.1.1 - 53	0.0.0.0 - 0	60	0	0
LAN	UDP	192.168.1.111 - 3268	192.168.1.1 - 53	0.0.0.0 - 0	60	0	0
LAN	UDP	192.168.1.111 - 3271	192.168.1.1 - 53	0.0.0.0 - 0	60	0	0
LAN	UDP	192.168.1.111 - 3269	192.168.1.1 - 53	0.0.0.0 - 0	60	0	0
Internet	TCP	220.130.26.50 - 1296	220.130.26.53 - 3389	192.168.1.111 - 3389	600	1166057	110245