LANBIRD 1004 IOS Manual

Contents

How to Use IOS Commands

LANBIRD command mode overview

Lanbird IOS is divided into several command modes and the commands which can be used by mode are defined in each mode.

The command mode mainly consists of the following three layers.

User mode → Root mode → Configuration mode

When the connection to the system is done initially, the user mode is active. Only the commands, which enable only basic management of the system, can be used in this mode.

It is possible to enter the root mode from the user mode by using the **"root"** command. In the root mode, it is possible to convert to the configuration mode in which the system configuration can be changed and to use all the commands for the system management.

It is possible to enter the configuration mode from the root mode by using the **"config"** command. In the configuration mode, it is possible to change all the configuration values of the system.

Entering question mark (?) on the system prompt will display all the commands which can be used in the current mode. Also, there are on-line helps for all commands.

Whenever it is desired to know how to use commands, enter question mark in the middle of a command. Then, the types of the commands which can be entered in the current status and their descriptions will be displayed. The following example shows the on-line help functions.

```
LANBIRD> ?
  Exit          Exit from login state
  help          Describe interactive help system
  ping          Send ICMP echo messages
  root          Change to root mode
  show          Show current system information
  telnet        Connect to a remote host by TELNET
  tracert       Trace route to destination
LANBIRD> show ?
  arp           ARP table
  bridge        Bridge table
  config        Saved configuration
  dns           DNS table
  frame-relay   Frame relay information
  interface     Interface information
  log           Log file
  nat           NAT table
  rconfig       Running configuration
  route         Routing table
  system        System information
  snmp          SNMP information
  user          Information about currently connected users
LANBIRD> show r?
  rconfig  route
LANBIRD> show r
```

User mode

If a connection is made through console without any password or the connection to a router is made by entering the login password in the network, the default is the user mode. In this mode, only part of root mode commands are available. In general, the commands through which one can view the router status are provided. The prompt ends with **">"** as shown next.

LANBIRD>

The prompt of the initial product is LANBIRD and it is possible to change it by using the "**prompt"** command in the root mode. To exit from the user mode, use the **"exit"** command.

Root mode

Because the user can easily change the system configuration in the root mode, password should be used to access this mode. To enter the root mode, use the **"root"** command as shown below. The prompt ends with **"#"**.

```
LANBIRD> root
Password: *******
LANBIRD#
```

In this mode, the user can use all the commands and enter the configuration mode to change the system configuration. To exit the root mode, use the **"exit"** command as shown below.

```
LANBIRD# exit
LANBIRD>
```

Configuration mode

The user can enter this mode, in which the user can change the router's configuration, by using the **"config"** command. The prompt ends with **"(config)#"**.

```
LANBIRD# config
LANBIRD(config)#
```

To exit the configuration mode, use the "end" or "exit" command.

```
LANBIRD(config)# exit
LANBIRD#
```

Two types of password

* Login password

- Used to make a connection to a router through telnet.

- Password of the initial products: lanbird <-- small letters

- If the login is performed properly, the default after the connection to the router is the user mode.

* Root password

- Used to move to the root mode after the connection to the router through console and telnet.

- Root password for the initial products: lanbird <-- small letters

Interface Configuration Management

Interface number

Lanbird routers use interface numbers in each command. The interface numbers and corresponding interfaces are shown below.

Interface number	Description
0	Ethernet interface 0
1	Serial interface 1
2	Serial interface 2

Ethernet interface configuration

A separate configuration is unnecessary because Ethernet automatically searches 10 Mbps or 100 Mbps interface.

Serial interface configuration

Lanbird routers support various Wide Area Network (WAN) interface protocols. Especially, Point to Point Protocol (PPP) and Cisco High level Data Link Control (HDLC) automatic detection function are very convenient because they do not necessitate a separate configuration of the line protocol in the general router environment. The following shows how to configure the line protocol of the serial interface.

Command	Description
line-protocol *ifnum* {autodetect|ppp|hdlc|frame-relay}	Configure the line protocol.

As a default of a router, the autodetect in the above table is to automatically detect PPP or HDLC.

keepalive configuration

The configuration of the keepalive interval is necessary for all interfaces to verify if an interface is alive. The default is 10 seconds and the following shows how to change this value.

Command	Description
keepalive *ifnum interval*	Configure the keepalive interval with the unit of second.

Viewing the interface status

The following command is used to view the status of each interface.

Command	Description
show interface *ifnum*	Show the interface status.

Viewing the Ethernet interface status

The following example shows the Ethernet interface status.

```
LANBIRD# show interface 0
Ethernet0 is up, line protocol is up
  IP address 192.168.1.1 / 255.255.255.0
  MAC address is 00:d0:a6:03:00:00
  Mode is 10 Mbps, Half-duplex
  Input
    queue: 0/150
    1 minute rate: 1 packets/sec, 830 bits/sec
    20248 packets, 2469046 bytes, 0 no buffers
    0 giant, 0 runt, 0 frame, 0 CRC, 0 overrun
  Output
    queue: 0/50
    1 minute rate: 1 packets/sec, 653 bits/sec
    17685 packets, 4876529 bytes, 0 drops
    0 underrun, 0 collision, 0 late collision
```

Viewing the serial interface status

The following example shows the status of serial interface 1.

```
LANBIRD# show interface 1
```

```
Serial1 is up, line protocol is up
  IP address 211.32.1.1 / 255.255.255.252
  Line protocol HDLC, keepalive 10
  Input
    queue: 0/50
    1 minute rate: 0 packets/sec, 310 bits/sec
    19179 packets, 4944750 bytes, 0 no buffers
    0 giant, 0 runt, 0 frame, 0 abort, 0 CRC, 0 overrun
  Output
    queue: 0/1500
    1 minute rate: 0 packets/sec, 254 bits/sec
    17005 packets, 1417970 bytes, 0 drops
    0 underrun
  DTR=up, RTS=up, DCD=up, DSR=up, CTS=up
```

Management of IP Addresses and Routing Configuration

Configuring the primary IP address for the network interface

The IP address determines where to send an IP packet. Because some IP addresses are reserved for special purposes, they cannot be used as the addresses for a host, a subnet, and a network.

It is possible to configure only one primary IP address for one interface. The following shows how to configure the primary IP address and the mask for network interface. If another primary IP address is configured for the interface, the existing IP address is replaced by the new one.

Command	Description
ip-address **add** *ifnum ip-addr ip-mask*	Configure the primary IP address and the mast for the interface.

Configuring several IP addresses for the network interface

It is sometimes necessary to configure several IP addresses for one interface. At this time, the following method is used to add IP addresses.

Command	Description
ip-address **add** *ifnum ip-addr mask* secondary	Add IP addresses and masks to the interface.

Deleting the IP address from the network interface

The following shows how to delete the IP address configured for an interface.

Command	Description
ip-address **del** *ifnum ip-addr*	Delete the IP address from an interface.

Routing table configuration

The following shows how to configure or add a routing path to the routing table.

Command	Description
ip-route **add** *dip-addr dmask {ifnum|fip-addr}*	Add a routing path.

The following shows how to delete a routing path from the routing table.

Command	Description
ip-route delete *dip-addr*	Delete a routing path.

Domain Name System (DNS) server configuration

The following shows how to configure and add a DNS server.

Command	Description
dns-server **add** *ip-addr*	Add a DNS server.

The following shows how to delete a DNS server.

Command	Description
dns-server **del** *ip-addr*	Delete a DNS server.

Network Address Translation (NAT) configuration

Two problems which Internet is facing are the lack of IP addresses and the increasing size of the routing. NAT gives the illusion that the IP network internally used by an organization looked as a different IP network to those outside the organization. Consequently, NAT enables the organization not using public IP addresses to use IP addresses by converting the non-public IP addresses to public IP addresses.

NAT terminology

The inside network in NAT means the network owned by an arbitrary organization with the intention to change by using NAT. The hosts in the inside network posses the addresses located in the address space, but they look as if they had addresses located in a different address space to those outside the organization when NAT is configured. The first is called inside address space and the second is called global address space.

Similarly, the outside network means the opposite network connecting to the inside network and in general refers to the network which a common organization cannot manage.

- Inside private address – the non-public IP address out of the IP addresses assigned to the hosts in the inside network.
- Inside public address – the public IP address out of the IP addresses assigned to the hosts in the inside network. This address is not changed by NAT.
- Outside public address – As the address when the observer in the outside network views the inside network, it is the public IP address representing more than one inside area address.

Enabling/disabling NAT function

It is necessary to distinguish between the inside network and the outside network to start NAT. By executing the following commands, Lanbird router determines the direction to which NAT should be performed.

Command	Description
nat enable *ifnum*	Configure as the outside network the network connected to the interface whose number is *ifnum*.

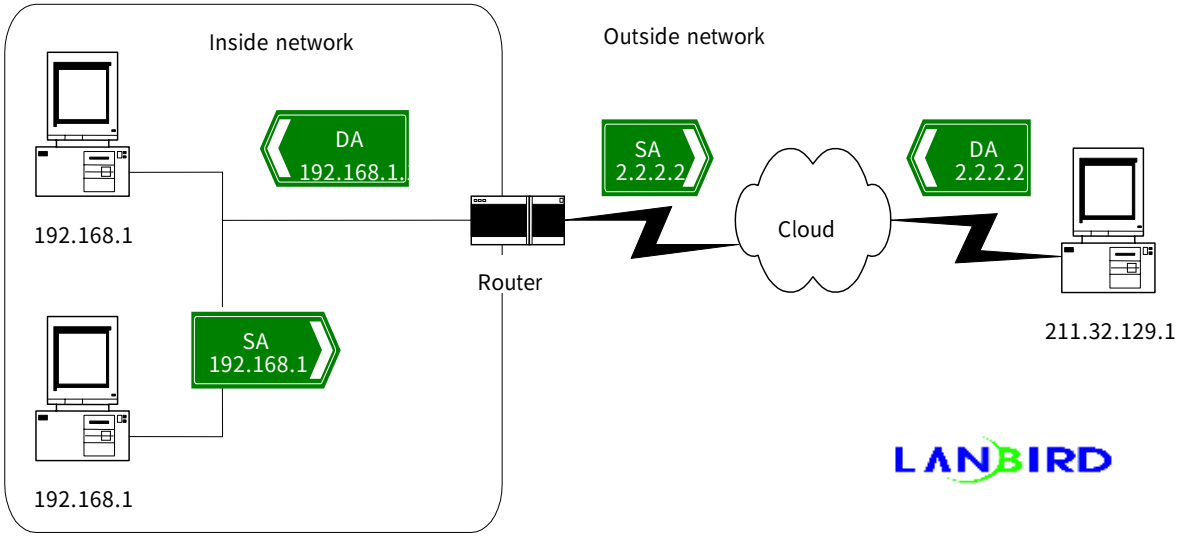
The following command is used not to use NAT function.

Command	Description
nat disable	Disable NAT function.

NAT configuration when more than one public IP address is possessed

For the host with an inside private address to communicate with the outside network, it is necessary to change the private IP address of the host into the public IP address. The address change can be configured in the following two ways: either dynamic or static.

The static translation is to allocate the inside area address and the inside public address to each other by one-to-one correspondence. This static translation is useful when the connection to the host located inside from outside by means of a fixed address is attempted. The dynamic translation is to allocate the inside area address and several public addresses dynamically.



The following procedure shows the example of using Internet through changing the source address of the host with the a inside private address by a router in the above figure.

1. The user in the host 192.168.1.1 is connected to the user in the host 211.32.129.104.
2. The router checks the NAT table for the first packet sent by the host 192.168.1.1. If the static translation is not configured, directly move to the third step. If the translation is not configured in the NAT table, the router creates the table which dynamically translates the source address (192.168.1.1) into one public address selected from the public address table.
3. The router translates the host's source address (192.168.1.1) into a public address according to the translation table and then send the packet to next hop.
4. The host 211.32.129.104 receives the transmitted packet and then answers to the host 192.168.1.1 by using the public (2.2.2.2).
5. When the router receives the packet with the public address of 2.2.2.2, it searches the translation table in the Nat table by using the public address, translates the public address into the inside area address (192.168.1.1), and then sends the packet to the host 192.168.1.1.

6. The host 192.168.1.1 receives the packet and continues to communicate. The router repeats the second and the fifth steps for all packets.

Configuring the static translation

The following configuration is done to always translate the host of a inside network to a specific public address.

Command	Description
nat out-static **add** *pub-ip pri-ip*	Connect a public IP address *pub-ip* and a private IP address *pri-ip* statically.

The following is how to cancel the static translation configuration.

Command	Description
nat out-static **del** *pub-ip pri-ip*	Cancel the static translation configuration.

Configuring the dynamic translation

The following configuration is done to dynamically translate the source address.

Command	Description
nat out-public **add** *pub-ip-network ip-mask*	Connect an inside private address and an outside public address *pub-ip-network* dynamically.

The following shows how to cancel the dynamic translation configuration.

Command	Description
nat out-public **del** *pub-ip-network*	Cancel the dynamic translation configuration.

Configuring the public address space in the inside network

Lanbird NAT regards all the addresses in the inside network as private IP addresses and translate them into outside public addresses. Consequently, when public IP network and private IP network are mixed inside, it is necessary to configure such that NAT is not performed for the public IP network located inside. The following

configuration is done to prevent NAT from being performed for the public IP network located inside.

Command	Description
nat in-public **add** *pub-ip-network ip-mask*	Not performing the NAT for the public IP network located in the inside network, *pub-ip-network*.

The following is done to cancel the public IP network configuration.

Command	Description
nat in-public **delete** *pub-ip-network*	Delete the public IP network configuration.

Using Internet by using only one public IP address (PAT)

Lanbird NAT supports the Port Address Translation (PAT) function which enables many hosts in the inside network to be connected to Internet at the same time only with one public IP address. Because this function can be used with the basic Nat described before, if there is no public IP address left due to the allocation of all public IP addresses used by NAT to a group of hosts, other hosts are automatically translated into the public addresses configured by PAT, which enables hosts to use Internet all the time. The following is how to configure PAT.

Command	Description
nat out-napt add *pub-ip-addr*	Configure a public IP address, *pub-ip-addr* as a PAT address.

Configuring a server inside by using only one public IP address

If there are many public IP addresses, it is possible to configure a specific host as a server through a static mapping. However, when PAT function is used because there is only one public IP, this function is unavailable. At this time, a server can be configured inside as shown below.

Command	Description
nat in-server add {tcp|udp} *port priv-ip-addr*	Configure the hosts with the inside private

	address, *priv-ip-addr* as the server connectable through the TCP or UDP port number of the IP address for which PAT is configured outside.

Opening A Specific Port

Under NAT environment, there is no restriction of connecting from the internal to the external, but the principle that the connection from the external to the internal will be blocked. When communicating from the internal to the external with the specific port, the packet can go through the specific port. Even though, the program doesn't match NAT environment, it requests the other specific port instead of the port which communicates from the internal to the external. In this case, open the specific port to get the service you wish to use.

The following shows the configuration when opening a specific port or when deleting the configured port

Command	Description
Nat in-port **add** {tcp|udp} port-nubmer	Open the specific port for the availability of connection
Nat in-port **delete** {tcp|udp} port-nubmer	delete the configured port.

Configuring the NAT timer

Lanbird router internally manages the NAT table for all mappings. Each mapping table, which has the timer to manage the current mapping, automatically disconnects the mapping when it is not disconnected properly. The followings show how to configure the timer according to the type of each of the connected traffic.

Command	Description
nat dns-timeout *timeval*	Configure the timeout of the DNS traffic.
nat fin-timeout *timeval*	Configure the FIN packet timeout of the TCP traffic.
nat icmp-timeout *timeval*	Configure the timeout of the ICMP traffic.
nat syn-timeout *timeval*	Configure the SYN packet timeout of the TCP traffic.
nat tcp-timeout *timeval*	Configure the timeout after the TCP connection.
nat udp-timeout *timeval*	Configure the timeout for the UDP traffic.

Configuration the NAT table size

The table size currently used by NAT is basically 1,000. However, when many users use Internet at the same time, it is necessary to increase the table size. At this time, the following is performed.

Command	Description
Nat max-entry *table-size*	Change the NAT table size into *table-size*. The table size ranges from 100 to 10000.

Frame-Relay Configuration Management

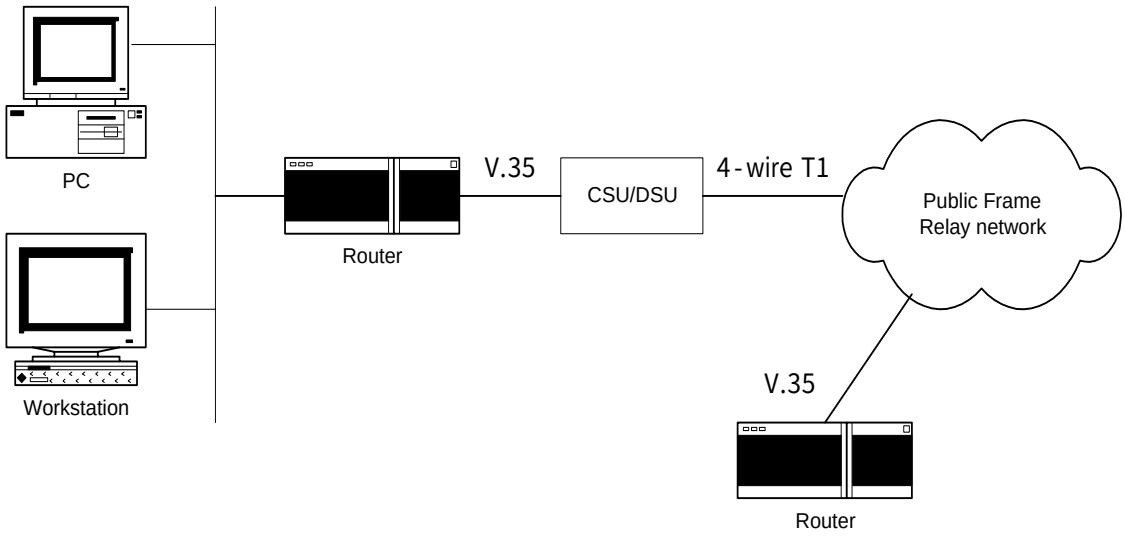
Configuring Permanent Virtual Circuit (PVC) frame-relay

Connecting frame-relay

There are two methods to connect the frame-relay as in the follows:

- Connect the router directly to the frame-relay switch.
- Connect the router to the remote frame-relay switch through CSU or DSU.

The figure below shows the different methods to connect router to the frame-relay network.



Setting the frame-relay protocol

To use the frame-relay service, it is necessary to change the line protocol of the interface, which will use the frame-relay, into the frame-relay first.

Command	Purpose
line-protocol *ifnum* **frame-relay**	To use the frame-relay for the *ifnum* interface.

Lanbird routers use RFC 1490 (IETF) with the frame-relay encapsulation method.

Setting the Data Link Connection Identifier (DLCI)

For the frame-relay to operate, the local IP address and the next hop IP address should be configured for each DLCI. Two methods are used to configure the DCLI: **local-map** and **static-map**.

In the **local-map**, DLCI and the IP address of the router are mapped and the frame-relay Inverse Address Resolution Protocol (IARP) is used to obtain the next hop IP address for a specific connection (DLCI). The router saves the destination IP address and DLCI in the internal table by using the answer to the IARP request. These two saved things are used to find the destination IP address or DLCI when the router sends out the packet. This method is available only when the destination router supports IARP. There are two methods to configure the **local-map**: the direct mapping of a specific IP address configured for the interface and the mapping of the primary address of the interface to be configured by omitting the IP address.

Method	Command	Purpose
1	**frame-relay local-map** *ifnum dlci* <cr>	To connect the given *dlci* and primary IP address to the *ifnum* interface.
2	**frame-relay local-map** *ifnum dlci local-ip*<cr>	To connect the given *dlci* and *local-ip* to the *ifnum* interface.

The **static-map** refers to the user's direct input of the next hop IP address of a specific connection (DLCI). IARP is not used to obtain the destination IP address. This method is used when the destination router does not support IARP. When the **static-map** method is used to input the destination IP address, the router automatically makes an internal connection to the IP in the same network out of the IP addresses configured for the interface. If the IP address in the same network is not configured for the interface, the input is cancelled.

Command	Purpose

frame-relay static-map *ifnum dlci remote-ip*<cr>	To connect the given *dlci* and *remote-IP* to the *ifnum* interface.

Configuring the Local Management Interface (LMI)

The router supports ANSI T1.617 Annex D LMI and ITU-T Q.933 Annex A LMI. Currently, the router has the function to find LMI automatically as a default. Consequently, it is unnecessary to configure LMI separate except for special cases. ANSI and Q.933 packets are sent out rapidly when the interface is updated and the automatic configuration is done to the LMI type with the answer to the sending. Once the LMI type is decided, the communication is done only through the decided LMI. The automatic configuration restarts only when the interface or the line protocol is downloaded.

Configuring the LMI type

Because only ANSI is supported by the lower version than IOS version 3.3, it is necessary to change the switch configuration if there is any problem with LMI. The method to configure the LMI type includes the followings.

Command	Purpose
frame-relay lmi-type *ifnum* {**ansi**|**q933a**}	To change the LMI type of the *ifnum* interface.

Configuring the keepalive interval

For the proper LMI operation, it is necessary to configure the keepalive interval. The current default is 10 seconds. This value must be smaller than the value configured to verify the keepalive status by the frame-relay switch. Because the switch is set to 15 seconds in general, it is unnecessary to change this interval except for special cases. The following is the method to change the keepalive interval.

Command	Purpose
keepalive *ifnum* {<cr>|<interval>}	To change the keepalive interval of the *ifnum* interface.

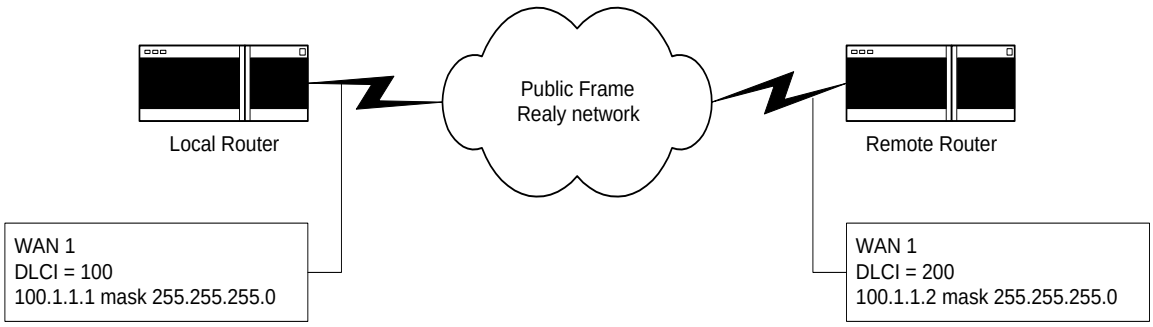
Configuring LMI variables

Unless the user is aware of the details of LMI, it is recommended not to leave LMI alone. Because an improper operation of LMI can cause a improper operation of the frame-relay, the user should not modify LMI except for special cases. The following commands are use to change LMI variables.

Command	Purpose
frame-relay lmi-mode *ifnum* {**user**|**network**|**bi-directional**}	To set the LMI mode of the *ifnum* interface.
frame-relay lmi-n391 *ifnum interval*	To change the full status polling interval of the *ifnum* interface.
frame-relay lmi-n392 *ifnum threshold*	To change the error threshold of the *ifnum* interface.
frame-relay lmi-n393 *ifnum enents*	To change the monitored event count of the *ifnum* interface.
frame-relay lmi-t391 *ifnum interval*	To change the keepalive interval of the *ifnum* interface.
frame-relay lmi-t392 *ifnum interval*	To change the polling verification timer of the *ifnum* interface.

Example of the configuration the PVC frame-relay

The following figure shows the frame-relay connected through the point-to-point method. Each router of both sides has one DLCI and one IP address and one DLCI and one IP address are respectively connected to the other DLCI and the other IP address.



Example of the configuration by means of the local-map

If the destination router supports IARP, the configuration by using the **local-map** is simple. The following is the configuration method by using the **local-map**.

```
LANBIRD> root
Password: *******
LANBIRD# config
LANBIRD(config)# ip-address add 1 100.1.1.1 255.255.255.0
LANBIRD(config)# line-protocol 1 frame-relay
LANBIRD(config)# frame-relay local-map 1 100
```

In the above configuration method, the IP address is omitted when configuring the **local-map**. Under this configuration, DLCI 100 is connected to the primary IP address of the serial interface 1 (100.1.1.1). The other configuration method by using the **local-map** is to input the IP address directly. In this case, the command on the last line shown above should be changed as shown below. This method is used when more than one DLCI are connected to different IP addresses.

```
LANBIRD(config)# frame-relay local-map 1 100 100.1.1.1
```

By doing this, DLCI 100 is connected to the IP address of 100.1.1.1. At this time, it should be ensured that the IP address to map must be one of the addresses configured for the serial interface.

To verify the proper configuration, the command, "**show rconfig"** can be used. The execution of this command to view the router configuration status should show the configuration of the serial interface 1 as shown below. It is noticed that the IP address not inputted by the user is automatically configured in the local-map.

```
Serial1 (Sync):
   ip address 100.1.1.1 255.255.255.0
   line-protocol frame-relay IETF
   frame-relay lmi-type ansi
   frame-relay local-map 100 100.1.1.1
```

Example of the configuration by means of the static-map

If the destination router does not support IARP, the **static-map** should be used for the configuration. The following shows the configuration method in which the **static-map** is used.

```
LANBIRD> root
password: *******
LANBIRD# config
LANBIRD(config)# ip-address add 1 100.1.1.1 255.255.255.0
LANBIRD(config)# line-protocol 1 frame-relay
        LANBIRD(config)# frame-relay static-map 1 100 100.1.1.2
```

The difference from the configuration by means of the **local-map** is that the destination IP address must be inputted. Also, it should be ensured that the destination IP address to map should be located on the same network as the IP address configured for the serial interface.

To verify the proper configuration, the command, "**show rconfig"** can be used. The execution of this command to view the router configuration status should show the configuration of the serial interface 1 as shown below.

```
Serial1 (Sync):
   ip address 100.1.1.1 255.255.255.0
   line-protocol frame-relay IETF
   frame-relay lmi-type ansi
            frame-relay static-map 1 100 100.1.1.2
```

Filtering

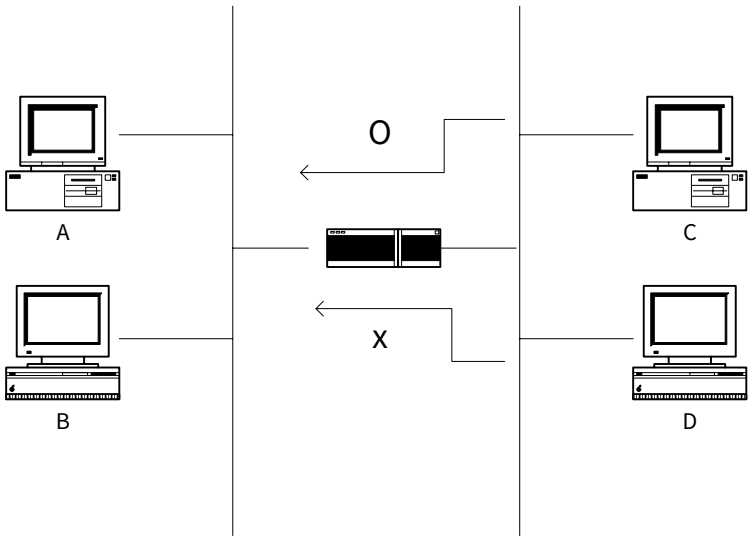
The purpose of Filtering

Filtering is the function that is to permit or deny the packet of which traffic come in and out on the Router. For the unwilling packets, the filtering function prevents the unwilling packets from the exterior to the interior by denying. This function provides the security of network.

In addition, unless you use ip-filter function, all packets through the router can approach your network easily.

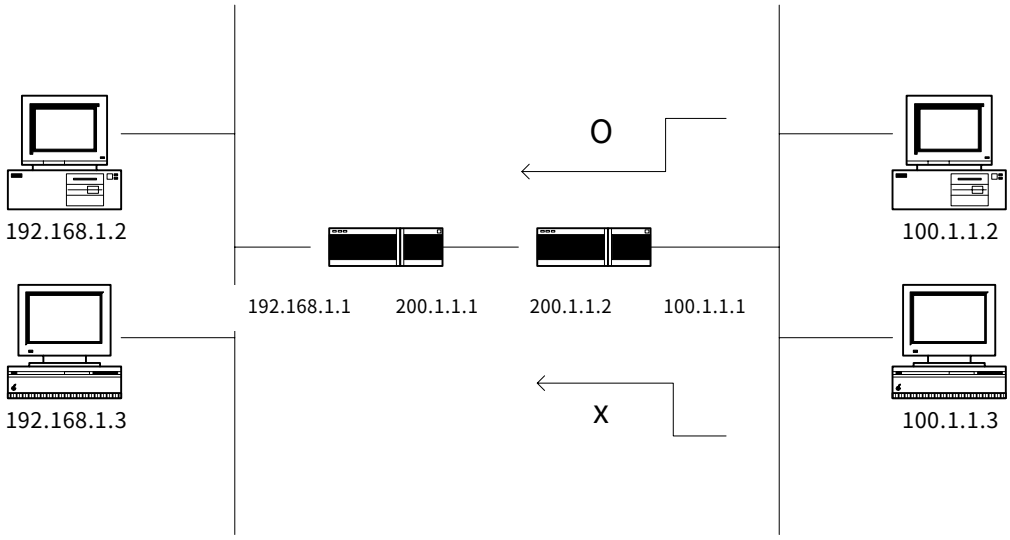
How to use Filtering

A host on the same network can permit or deny the approaching of different part of network. The following example represents the availability of accessing from C of branch 2 to branch 1(A, B) and the availability of blocking from D of branch 2 to branch 1(A, B).

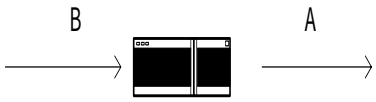


Branch 1 Branch 2

In addition, you can also do filtering packets which come from the external network as well.



The Position of LANBIRD Filter with Inbound and outbound



Router

LANBIRD's products have 2 filters in each interface. In each interface, you can do filtering to inbound packet or outbound packet. Additionally, LANBIRD 1004 offers filtering adaptively.

As the figure above, you can either filter the packet on B(inbound) or A(outbound).

Types of Protocols Which Can Be Filtered

Types of Protocols

LANBIRD 1004 offers all types of protocols such as udp, tcp, ip, icmp and numbers between 0-255.

ICMP

icmp message type can be configured with the value of 0-255 as well as echo-request, echo-reply, time-exceed and destination unreachable.

TCP

Input the port number between 0-65535 for filtering tcp packet as well as ftp, pop3, rlogin, smtp, telnet, www. Additionally, syn packet(packet which uses the connection establish for the exterior) can be filtered as well.

UDP

Input the port number between 0-65535 for filtering udp packet as well as dns, snmp.

※ allocate a range for the ease of filtering when configuring the port number.

Filtering Policy

Set up a policy first before doing Filtering.

when packet comes in, set up a policy for denying or permitting.

set up a policy for the packet which isn’t configured.

Process of Accomplishing Filtering

1. search the condition which configured as the sequence of filter.

2. execute the filter when the condition satisfies the filter which has configured.

3. manage the packet by depending default if the condition doesn't satisfy the filter.

The following example is to assume that the filter has been configured on Serial 1,

Serial 1
Ip-filter List1
Ip-filter List2
Ip-filter List3
Ip-set deny

1. does it satisfy the condition of List1 ➔ execute when satisfying

2. if the condition doesn't satisfy List 1, then does it satisfy List 2➔ execute when satisfying

3. if the condition doesn't satisfy List 2, then does it satisfy List 3➔ execute when satisfying

4. if there is no satisfied condition, then deny corresponding packet

※ when the packet comes in, if it doesn't satisfy, them mange it as default.

The Configuration and Enforcement of LANBIRD Filter

Add Data on Filter

When you add the new filter to the filter which already exits, the new filter will automatically be adding to the end of the filter list. It means that the inputting

sequence of ip-filter table will influence the execution of filtering. In addition, you can't change the sequence when adding the data to the table.

Delete Data on Filter

You can delete the filter without any sequence violation.

Default filter

If you don't execute the command ip-filter on LANBIRD Router, the filtering function will not work at all.

When you use the command "ip-filter", it automatically denies all traffic between input filter & output filter as the default. Due to there is no configuration, it executes as deny.

How to Use

Filter Command

Command	Description
IP-filter {add|delete} <ifnum> input permit <source> <destination> <IP-protocol>	permit the filter which Adds/Deletes the packet from the source to the destination that comes through the interface
IP-filter {add|delete} <ifnum> input deny <source> <destination> <IP-protocol>	Deny the filter which Adds/Deletes the packet from the source to the destination that comes through the interface
IP-filter {add|delete} <ifnum> output permit <source> <destination> <IP-protocol>	permit the filter which Adds/Deletes the packet from the source to the destination that goes out through the interface
IP-filter {add|delete} <ifnum> output deny <source> <destination> <IP-protocol>	deny the filter which Adds/Deletes the packet from the source to the destination that goes out through the interface

Explanation of Filter Command

Grammar	Description
<ifnum> ::= 0 | 1 |2	Assign the interface number which will be filtered
<source>::= <source-IP-address > <subnetmask>	Assign the source address of packet which will be filtered ※refer to the network address assigning method
<destination>::= <destnation-IP-address > <subnetmask>	Assign the destination address of packet which will be filtered ※refer to the network address assigning method
<IP-protocol>::=[<1-255>| icmp |IP| tcp <tcp-port>|udp <udp-port>]	When defining ip-protocol which will be filtered, define protocol as a number between <1-255>. icmp, ip,tcp,udp can be defined as a name instead of numbers.
<tcp-port>::=[<1-65535> | ftp (21)| pop3(110) | snmp(25) | telnet(23) | www(80)]	When defining tcp-port which will be filtered, define port as a number between <1-65535>. ftp, pop3, snmp, telnet, www can be defined as a name instead of numbers.
< udp-port >::=[<1-65535>| dns(53)|snmp(161)]	When defining udp-port which will be filtered, define port as a number between <1-65535>. dns, snmp can be defined as a name instead of numbers..

Assigning Method of Network Address

Network address::= <IP-address> <subnetmak>
- Network address can be configured with IP address and subnetmask.

<IP-address>::={xxx.xxx.xxx.xxx | all}
<subnetmask>::={xxx.xxx.xxx.xxx | host | all}

※ it is available for inputting simple name instead of IP address and subnetmask.
all = 0.0.0.0
host = 255.255.255.255

Set command configuration

Command	Description
IP-filter set <ifnum> input permit	Permitting all inputting packet which is not configured on Filter
IP-filter set <ifnum> input deny	Denying all inputting packet which is not configured on Filter
IP-filter set <ifnum> output permit	Permitting all outputting packet which is not configured on Filter
IP-filter set <ifnum> output deny	Denying all outputting packet which is not configured on Filter

※ The command set is to save ip-filter default value. Namely, it will be searching for ip-filter table if the current value doesn't exist, it does filtering depending on the default value which is configured by the command set.

Example of Filtering

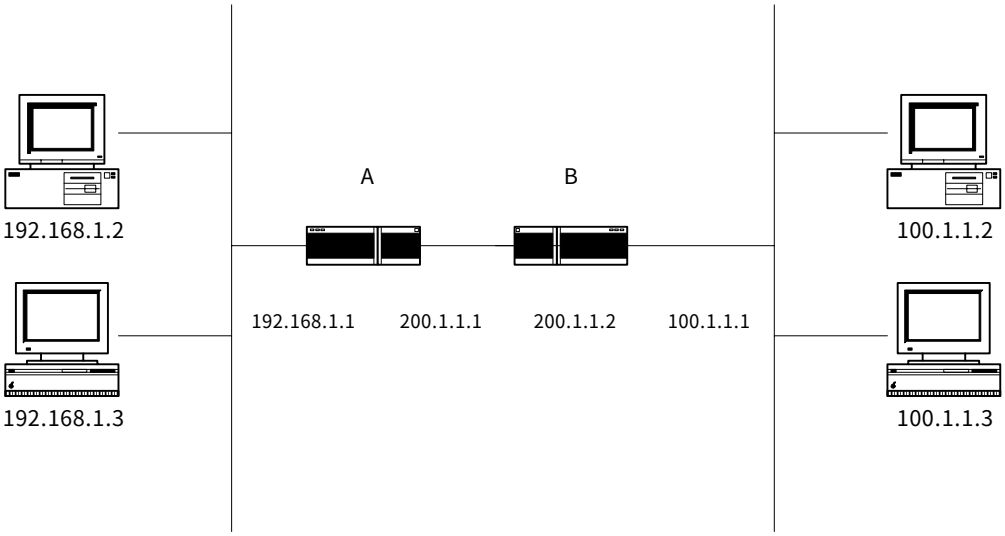
Example of set command

```
LANBIRD(config)# IP-filter set 0 input permit
LANBIRD(config)# sh rconfig
Current running configuration:
|
Ethernet0:
   IP-address 192.168.1.1 255.255.255.0
   IP-filter input permit default
Serial1:
   IP-address 200.1.1.1 255.255.255.0
   line-protocol autodetect (ppp/hdlc)
Serial2:
   no IP-address
   line-protocol autodetect (ppp/hdlc)
|
IP-route 100.1.1.0 255.255.255.0 interface 1
|
```

※ When input filter is activating on Ethernet, permit all input.

Example of filter on network

The example below is the configuring method which uses the command “set” to permit the packet as default. However, if you don’t know how to use the command “set”, then refer to the example which is representing above.



1. The diagram above represents how to deny ping from 192.168.1.2 to 100.1.1.2

On Router A

Deny icmp input packet from 192.168.1.2 to 100.1.1.2 on Ethernet

```
LANBIRD(config)# IP-filter add 0 input deny 192.168.1.2 host 100.1.1.2 host icmp
LANBIRD(config)# sh rconfig
Current running configuration:
|
Ethernet0:
   IP-address 192.168.1.1 255.255.255.0
   IP-filter input deny 192.168.1.2 host 100.1.1.2 host icmp
   IP-filter input permit default    //permit input by using default of set command
Serial1:
   IP-address 200.1.1.1 255.255.255.0
   line-protocol autodetect (ppp/hdlc)
Serial2:
   no IP-address
   line-protocol autodetect (ppp/hdlc)
|
IP-route 100.1.1.0 255.255.255.0 interface 1
|
```

2. the diagram above represents how to only permit ping 100.1.1.3 from the network 100.1.1.0

to the network 192.168.1.9

Permit icmp input packet from 100.1.1.3 to network 192.168.1.0 on Ethernet

```
LANBIRD(config)# IP-filter add 0 input permit 100.1.1.3 host 192.168.1.0 all icmp
LANBIRD(config)# sh rconfig
Current running configuration:
|
Ethernet0:
   IP-address 200.1.1.2 255.255.255.0
   IP-filter input permit 100.1.1.3 host all all icmp
                              //IP-filter input deny default has been configured temporarily
Serial1:
   no IP-address
   line-protocol autodetect (ppp/hdlc)
Serial2:
   no IP-address
   line-protocol autodetect (ppp/hdlc)
|
IP-route 0.0.0.0 0.0.0.0 interface 1
|
```

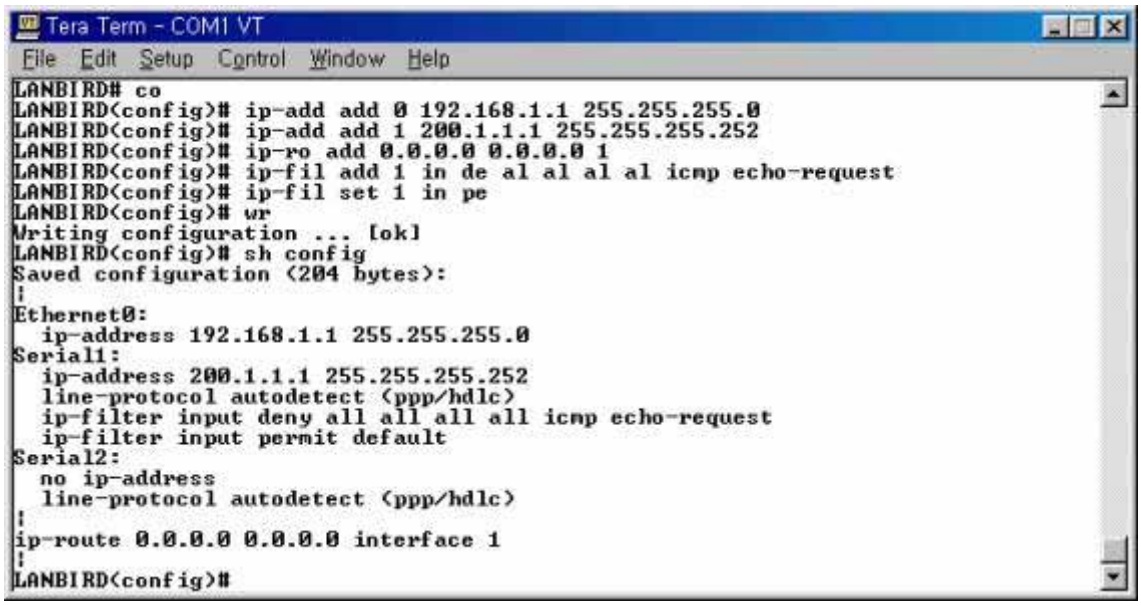
3. the diagram above represents how to deny telnet connection of router A from the outside of network

Router A only needs to deny inputting tcp telnet from Ethernet and tcp telnet from serial

```
LANBIRD(config)# IP-filter add 0 input deny all all all all tcp telnet
LANBIRD(config)# IP-filter add 1 input deny all all all all tcp telnet
LANBIRD(config)# sh rcon
Current running configuration:
|
Ethernet0:
   IP-address 192.168.1.1 255.255.255.0
   IP-filter input deny all all all all tcp telnet          //deny all inputting tcp telnet packet
   IP-filter input permit default    //permit input by using default of set command
Serial1:
   IP-address 200.1.1.1 255.255.255.0
   line-protocol autodetect (ppp/hdlc)
   IP-filter input deny all all all all tcp telnet             //deny all inputting tcp telnet packet
   IP-filter input permit default    // per input by suing default of set command
Serial2:
   no IP-address
   line-protocol autodetect (ppp/hdlc)
|
IP-route 100.1.1.0 255.255.255.0 interface 1|
```

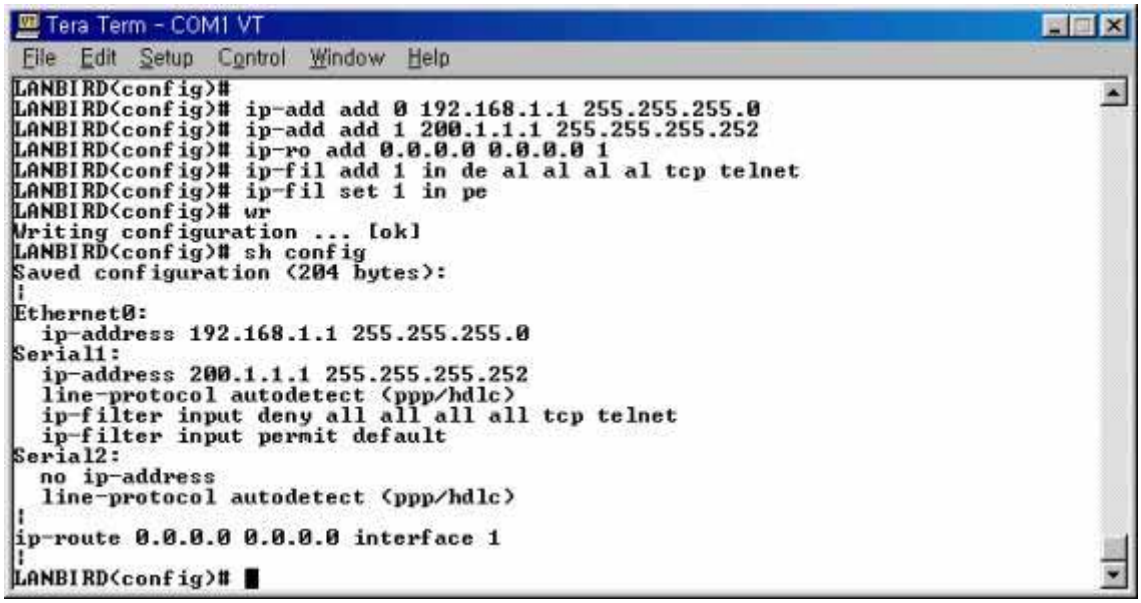
The Example of Filtering after Version 0.4.4

When the ping test is available from the network 192.168.1.0 to the network 100.1.1.0 and the ping test doesn't wish to be available from the network 100.1.1.0 to the network 192.168.1.0, you only need to deny echo-request from the network 100.1.1.0. For other packets(default), you need to permit it.

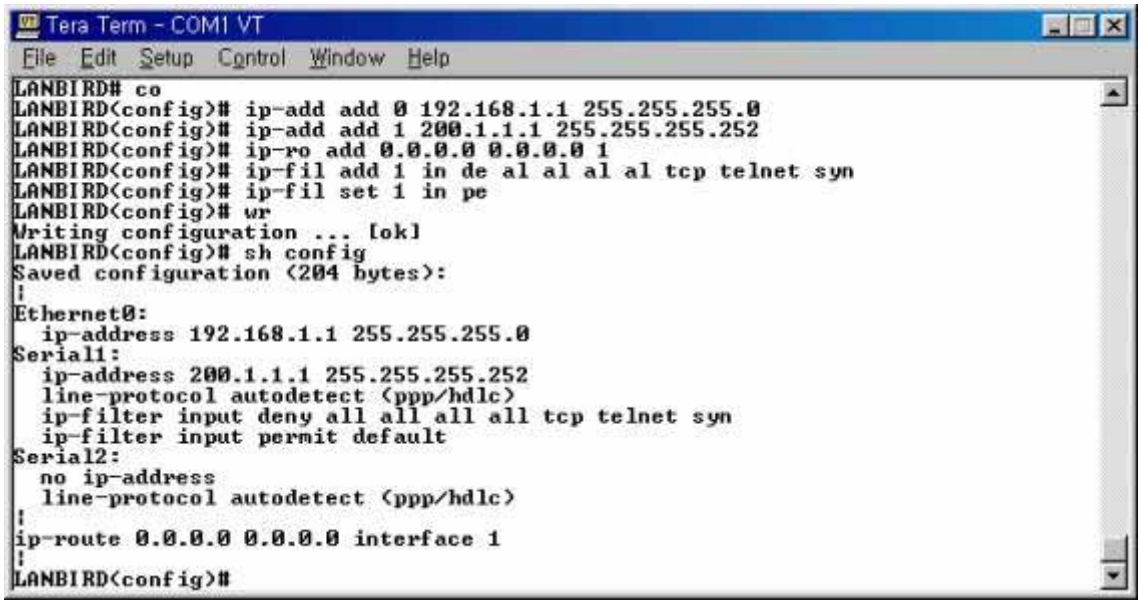


To block telnet connection from the network 100.1.1.0 to the network 192.168.1.0, you need to block the telnet port which comes from the network 100.1.1.0 or block syn packet which is willing to do telnet connection. After that, permit other packets.

1. Block telnet port on router A

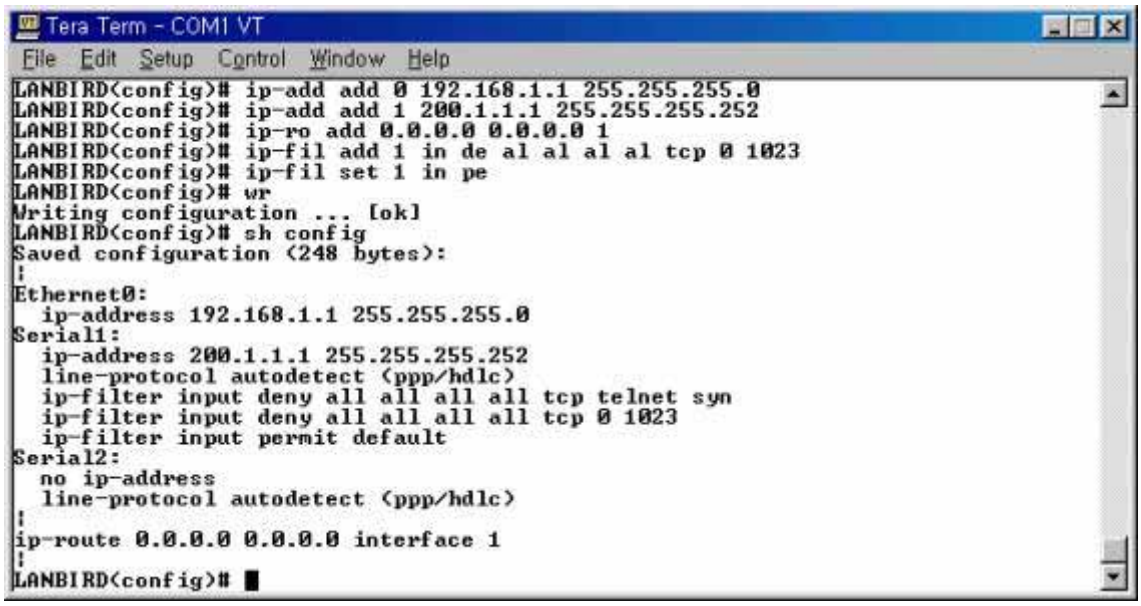


2. **Block telnet syn packet which wishes to come in for telnet connection on router A.**

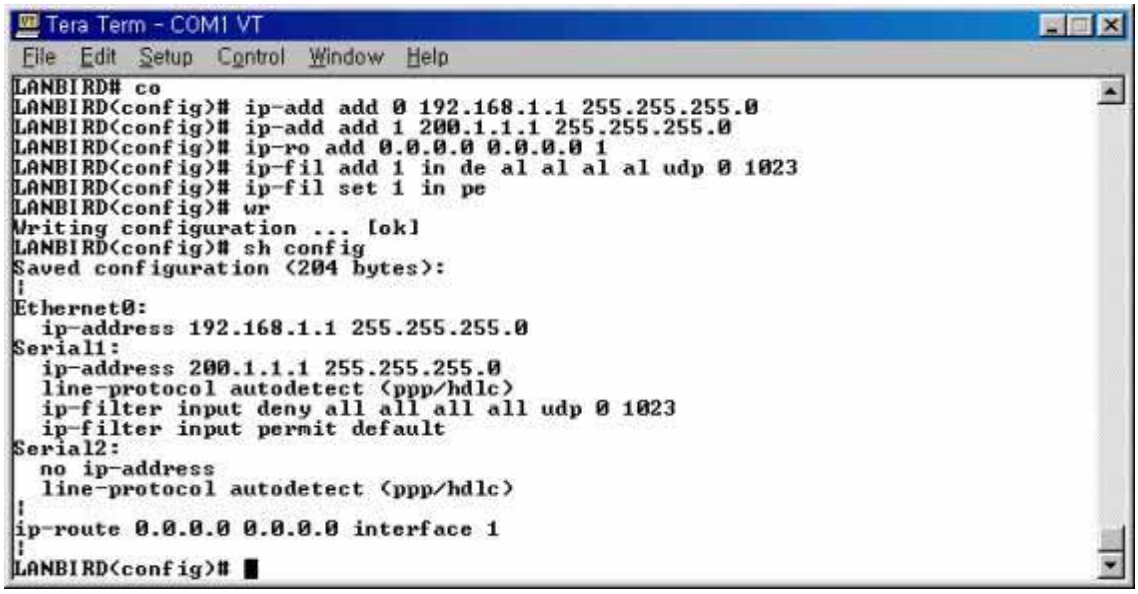


※The difference between blocking tcp telnet and tcp telnet syn is tcp telnet blocks all telnet ports for not being able to do the telnet connection. On the other hand, tcp telnet syn is not to materialize the connection when telnet connection is accomplishing. User who is already on the connection before configuring tcp telnet syn, the user can be on the telnet connection continuously.

the packet which comes from the network 100.1.1.0 to the network 192.168.1.0 denies 10231 from tcp 0 and permit other packets.



the packet which comes from the network 100.1.1.0 to the network 192.168.1.0 denies 1023 from udp 0 and permit other packets.

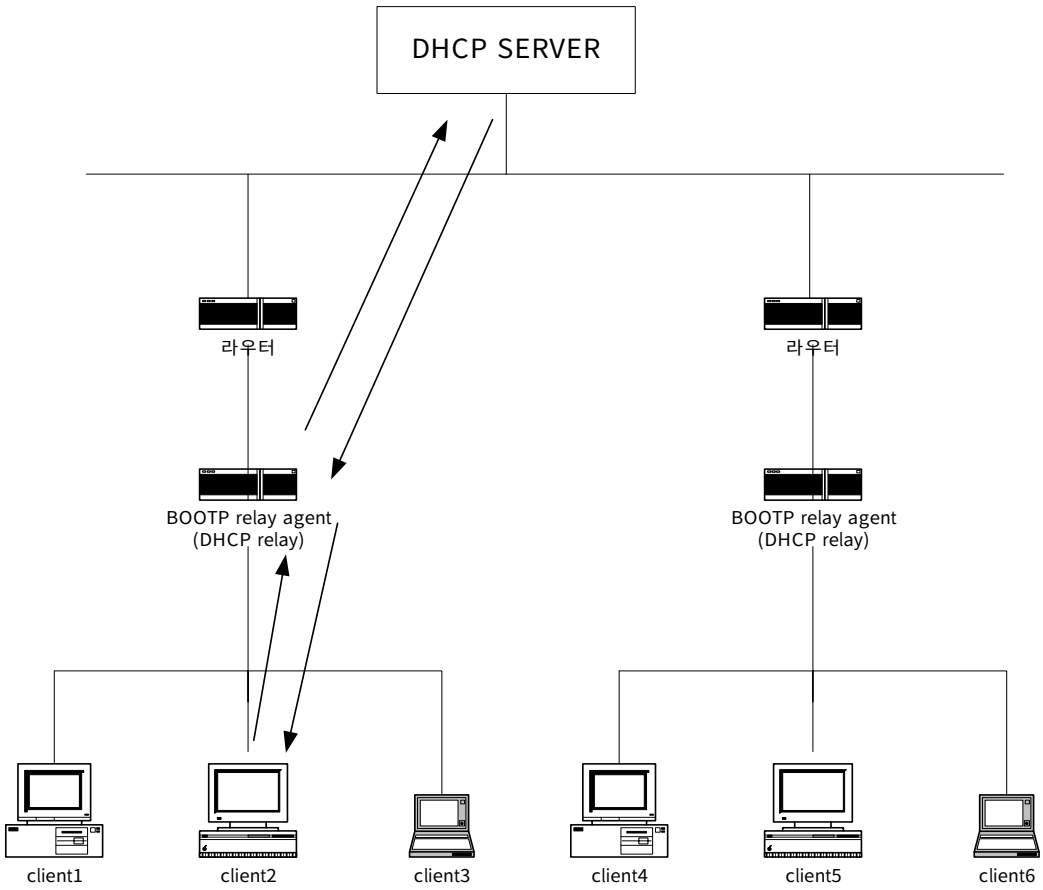


BOOTP-relay

BOOTP relay is the function that each client can connect to the remote server which exist on the different network.

Example of BOOTP-relay

When an organization divided into several networks, the manger can mange whole network through central DHCP-server by using BOOTP-relay agent.



Working Principle

Each client, willing to get the information from DHCP server, broadcasts to the local network. At this time, the router which is been doing BOOTP relay agent function relays the request packet, which has been received from client, to assigned DHCP server.

As the same meaning, the router which is been doing BOOTP relay agent function transits the response packet from DHCP server to local client.

As the same way, each client through BOOTP relay agent will be offered the service from DHCP server of which is in remote area.

Explanation of Command

The following example is to add / delete bootp-relay.

Command	Description
bootp-relay add <bootp-IP-addr>	Add IP-address of Bootp-relay
bootp-relay del <bootp-IP-addr>	Delete IP-address of Bootp-relay

Using Tips

Next is the example which uses BOOTP-relay to get the service from the server 100.1.1.1

```
LANBIRD(config)# bootp-relay add 100.1.1.1
LANBIRD(config)# show rconfig
Current running configuration:
|
bootp-relay 100.1.1.1
|
Ethernet0:
   IP-address 192.168.1.1 255.255.255.0
Serial1:
   IP-address 200.1.1.1 255.255.255.0
   line-protocol autodetect (ppp/hdlc)
Serial2:
   no IP-address
   line-protoco
   l autodetect (ppp/hdlc)
```

```
|
IP-route 0.0.0.0 0.0.0.0 interface 1
|
```

DHCP(Dynamic Host Configuration Protocol) server

DHCP is the function that earns the configuration of its network. In addition, it reduces the work of managing.

Client earns the configuration such as ip address, subnet mask, gateway, dns-server address from the server. When requesting the configuration from client, server will allocate the address dynamically.

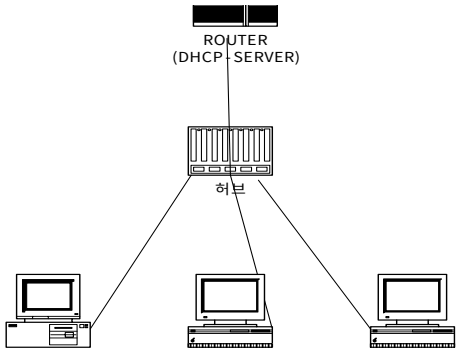
When using DHCP sever, client will be allocated ip address dynamically. It means that DHCP sever offers much adaptable than using static for managing IP.

Whatever the users know Internet or not, they can access Internet easily by using DHCP to manage IP address.

When IP network environment has changed, you only need to change the configuration of DHCP server for those whom to use the network without any configuration.

Example of DHCP server

DHCP delivers the information of network configuration to each client



Allocated IP automatically

Working Principle

When a host is booting, it requests IP. In this case, DHCP server router responses the usable IP address to each client. After that, the client requests its configuration option. Finally, server delivers the information of IP address, gateway, subnet mask, dns-server IP, etc, to clients.

Necessary Information for Server

The information of the host IP-address which will be managed, subnet mask, gateway, dns-server will be needed.

IP-address : IP-address which will be managed by DHCP server

Subnet mask : the subnet mask of network where host is belonging

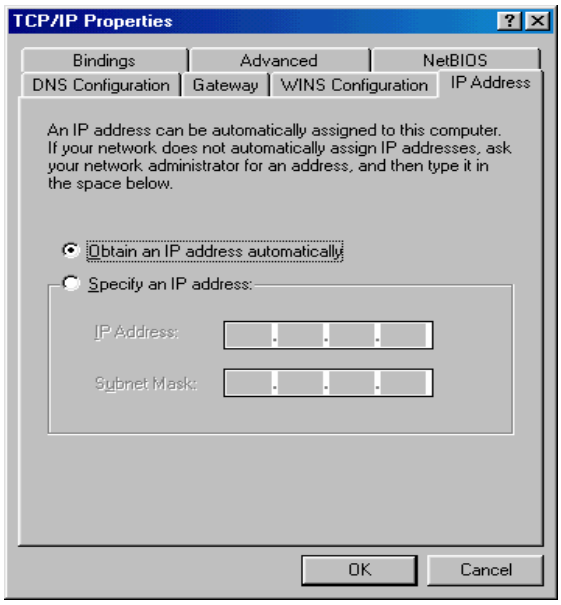
Gateway : the router(gateway) of ip address where the host is belonging to

Lease time : DHCP server sets how long IP will be leased to the client

DNS-server : DNS-server IP address which will be configured to the host

Configuration of Host

On the properties of TCP/IP in network neighborhood configures the IP address as auto (available for Window 95/98, Window NT).



Explanation of Command

Enabling DHCP-server

Next is the command which is for enabling DHCP-server or disabling DHCP-server.

Command	Description
dhcp-server enable	Enable DHCP-server
dhcp-server disable	Disable DHCP-server

Adding DHCP-server

Next is the necessities to manage such as a range of address, subnet mask of host, gateway of host.

You can configure the range of address through defining the beginning address and the ending address.

Command	Description
dhcp-server IP-address add < start-IP-addr> <end-IP-addr> < IP-subnet mask> <gateway-IP-addr>	Adding a range of ip-address, subnet mask and gateway address which will be managed by DHCP-server.

<start-IP-addr> starting IP-address

<end-IP-addr> ending IP-address

< IP-subnet-mask> subnet mask which host belongs to the network

<gateway-IP-addr> gateway IP address which host belongs to the network

※ After version 0.4.1, when DHCP automatically allocates private + public ip, it depends on user's request to give public ip as the first priority. If no public ip is available, it will allocate private ip automatically.

Command of version 0.4.1

dhcp-server IP-address add < start-IP-addr> <end-IP-addr> < IP-subnet mask> <gateway-IP-addr> <priority>

Deleting DHCP-server

when deleting the contents fo configuration

Command	Description
dhcp-server IP-address del < start-IP- addr>	Delete a range of ip-address which will be managed by DHCP-server

<start-IP-addr> starting ip-address which dhcp-server will be managed

Add/Delete DNS-server

DHCP-server has to contain the information which dns-server is used by the host

Command	Description
dhcp-server dns-server add <dns-IP-addr>	Adding IP-address of dns-server
dhcp-server dns-server del <dsn-IP-addr>	Deleting IP-address of dns-server

Lease time configuration

How long the information which elucidates to DHCP-server lease-time will lease to the host. When hosts are communicating continuously, request an allocation before end of

the leasing time. In addition, router will recover the information which has allocated to the host if there is no request for the allocation from host

Command	Explanation
dhcp dns-server lease-time <seconds>	Configure lease time

<seconds> configuring the range between 1-2147483647seconds

default : 3600

※ We recommend you that configure the lease-time to 1,000seconds. The lease-time will be an hour if you configure the lease-time to 3,600seconds, even the host doesn't communicate.

Additional grammar check after version 0.4.1

the command form dhcp-server ip address has changed after version 0.4.1

※priority has added. when public ip is lacked, you can use public and private together. As a result, this function increases the efficiency of using public ip.

advantages when allocating the sequence of priority

1. when ip is not enough, you can use public and private ip for increasing the efficiency of usage.
2. when public ip is not enough, it can be the data of how many public ip should be allocated.

Example of Configuration

Giving condition

IP address which will be managed by DHCP-server: 192.168.1.2 ~ 192.168.1.254
※ 192.168.1.1 is allocated as the address of router
Subnet mask : 255.255.255.0
gateway of host : 192.168.1.130
DNS sever of host : 164.124.101.2

Configuration

```
LANBIRD(config)# dhcp-server enable
LANBIRD(config)# dhcp-server IP-address add 192.168.1.2 192.168.1.254 255.255.255.0 192.168.1.1
LANBIRD(config)# dhcp-server dns-server add 164.124.101.2
LANBIRD(config)# show rconfig
Current running configuration:
|
dhcp-server enabled
   IP-address 192.168.1.2 192.168.1.254 255.255.255.0 192.168.1.1
   dns-server 164.124.101.2
|
Ethernet0:
   IP-address 192.168.1.1 255.255.255.0
Serial1:
   IP-address 200.1.1.1 255.255.255.0
   line-protocol autodetect (ppp/hdlc)
Serial2:
   no IP-address
   line-protocol autodetect (ppp/hdlc)
|
IP-route 0.0.0.0 0.0.0.0 interface 1
||
```

Conforming the Configuration

Conforming the configuration of Host

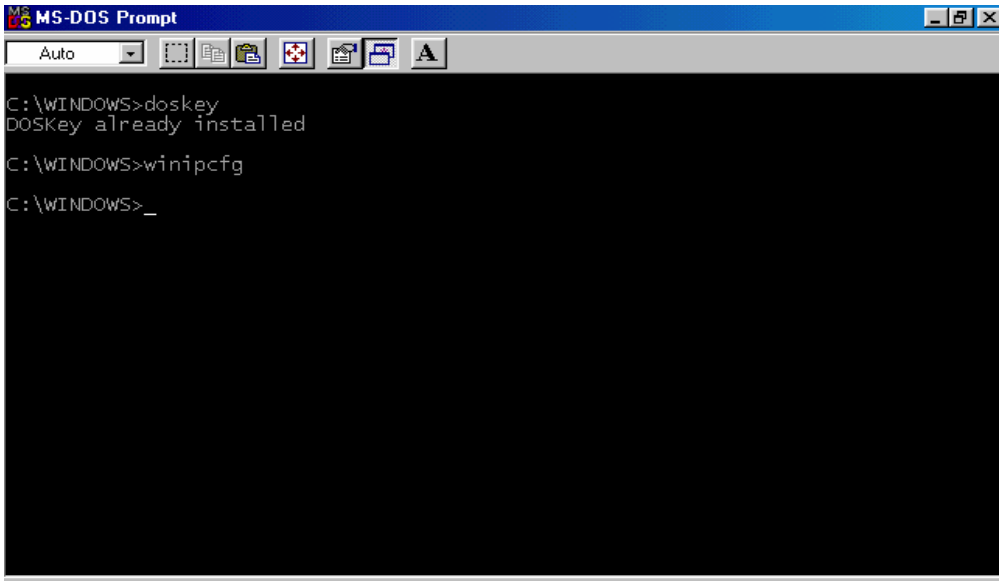
```
LANBIRD# sh dhcp
lease-time = 3600 seconds
dns-server = 0.0.0.0
Start IP          End IP            Subnet Mask       Gateway
--------------- --------------- --------------- ---------------
192.168.1.2       192.168.1.254     255.255.255.0     192.168.1.1
IP address        Ethernet Address          IP address        Ethernet Address
--------------- ----------------- ----   ------- ----------------- ----
192.168.1.2       00:90:27:d5:aa:b0         YES
192.168.1.3       00:90:27:d5:aa:b1         YES
192.168.1.4       00:90:27:d5:aa:b2         NO
192.168.1.5       00:90:27:d5:aa:b3         YES
```

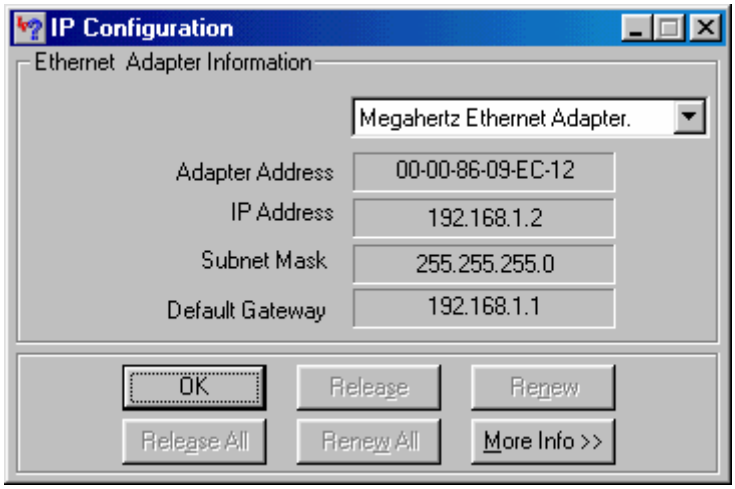
Conforming the configuration of Host

Inputting WINIPCFG on DOS prompt

You can see such as ip address, subnet mask, gateway which have allocated to the host.

If you wish to check the information of dns-server which hosts use and the information of information that is used by hosts, please check "IP Configuration" and click "more info>>"


MS-DOS Prompt
Auto
C:\WINDOWS>doskey
DOSKey already installed
C:\WINDOWS>winipcfg
C:\WINDOWS>_

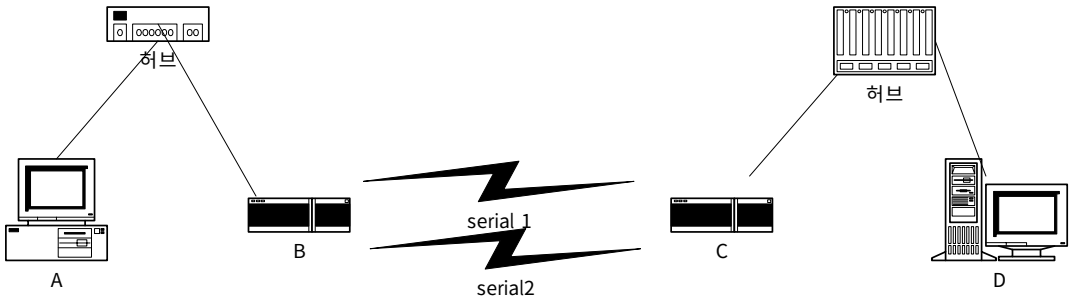

IP Configuration
Ethernet Adapter Information
Megahertz Ethernet Adapter.
Adapter Address
00-00-86-09-EC-12
IP Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
OK
Release
Renew
Release All
Renew All
More Info >>

Dynamic Backup

Purpose

Dynamic Backup is the function that gives the redundancy to the line to recover the communicational obstacle with the alternative path.

Example



In case that the host A connected with the server D and the serial 1between B&C is down, consequently, the host will be served by server D continuously via serial2.

Method of Configuration

You can configure it through the command ip-route.

(Please refer to the command of load balancing)

If the communication is available with more than 2 paths for the same destination,

1. Allocate the same metric value for executing dynamic backup when a line is abnormal.

2. Only execute dynamic back up when the metric value is different. The connection will be accomplished to the interface which is the high priority(low metric value). If the line is abnormal the connection will be available for the interface which is the low priority(high metric value).

Consideration

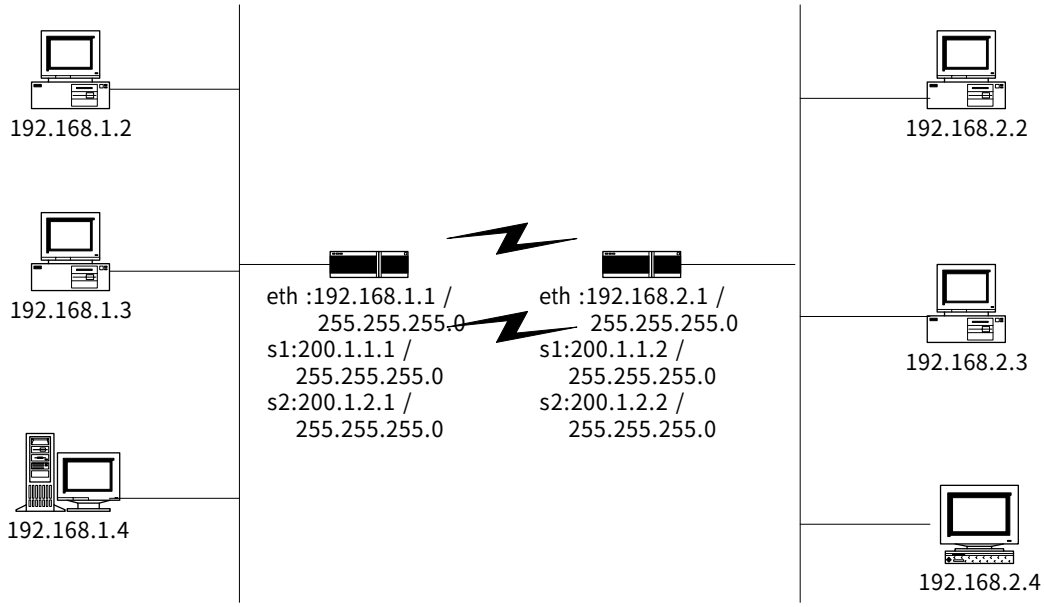
You can use the command "show route" to check the information oc communicative destination. You can't use the command "show route" to check the uncommunicative path.

※Through the command "show config" to check the content of configuring when you wish to check the routing table which has configured.

Example

Next is the example that executing load balancing on 2 lines when a line is down. As a result, the connection will go through the communicative interface as configuration.

※Dynamic back up can be configured with load balancing.



When A & B are communicating, you can activate the serial line redundancy to deal with the communicational obstacle.

```
A: serial1 IP address : 200.1.1.1 subnetmask : 255.255.255.0
Serial2 IP address : 200.1.2.1 subnetmask : 255.255.255.0
Static route
destination : 0.0.0.0 0.0.0.0     interface : 1
destination : 0.0.0.0 0.0.0.0     interface : 2
```

Configuring on Router A

```
LANBIRD(config)# IP-address add 1 200.1.1.1 255.255.255.0
LANBIRD(config)# IP-address add 2 200.1.2.1 255.255.255.0
LANBIRD(config)# IP-route add 0.0.0.0 0.0.0.0 1
LANBIRD(config)# IP-route add 0.0.0.0 0.0.0.0 2
```

Conforming Configuration

The method of conforming configuration is as follow.

Using show rconfig to conform the status of Router A

```
LANBIRD(config)# show rconfig
Current running configuration:
|
Ethernet0:
no IP-address
Serial1:
   IP-address 200.1.1.1 255.255.255.0
   line-protocol autodetect (ppp/hdlc)
Serial2:
   IP-address 200.1.2.1 255.255.255.0
   line-protocol autodetect (ppp/hdlc)
|
IP-route 0.0.0.0 0.0.0.0 interface 1
IP-route 0.0.0.0 0.0.0.0 interface 2
|
```

Using command show router to conform the status Router A

```
LANBIRD(config)# show route
IP Routing table: L (local), S (static)
   Destination       Subnet Mask       Metric and Gateway
- --------------- --------------- ----------------------------
L 200.1.1.0         255.255.255.0     [0] connected to interface 1
L 200.1.2.0         255.255.255.0     [0] connected to interface 2
S 0.0.0.0             0.0.0.0           [1] via interface 1
S 0.0.0.0             0.0.0.0           [1] via interface 2
```

When serial1 is down, using command show route to conform the status of Router A

```
LANBIRD(config)# show route
IP Routing table: L (local), S (static)
   Destination       Subnet Mask       Metric and Gateway
- --------------- --------------- ----------------------------
L 200.1.1.0         255.255.255.0     [0] connected to interface 1
L 200.1.2.0         255.255.255.0     [0] connected to interface 2
S 0.0.0.0             0.0.0.0           [1] via interface 2    //serial 1 down
```

When serial2 is down, using command show route to conform the status of Router A

```
LANBIRD(config)# show route
IP Routing table: L (local), S (static)
   Destination        Subnet Mask        Metric and Gateway
- --------------- --------------- ----------------------------
L 200.1.1.0         255.255.255.0      [0] connected to interface 1
L 200.1.2.0         255.255.255.0      [0] connected to interface 2
S 0.0.0.0             0.0.0.0            [1] via interface 1    //serial 2 down
```

When serial1 and serial2 are down, using the command show route to conform the status of Router A

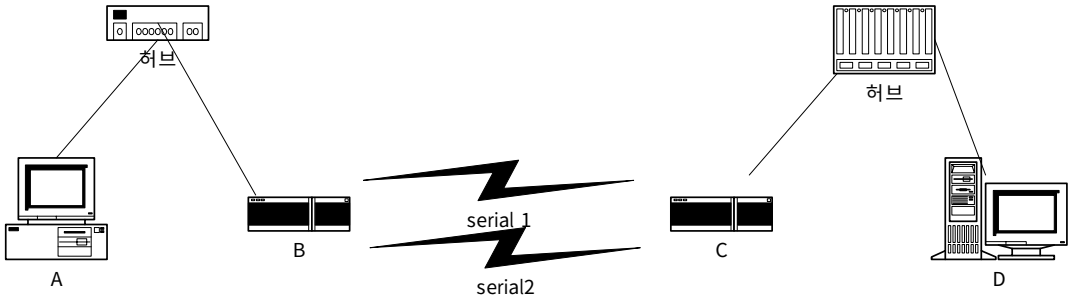
```
LANBIRD(config)# show route
IP Routing table: L (local), S (static)
   Destination        Subnet Mask        Metric and Gateway
- --------------- --------------- ----------------------------
L 200.1.1.0         255.255.255.0      [0] connected to interface 1
L 200.1.2.0         255.255.255.0      [0] connected to interface 2
                                                    //serial1 and serial2 are down
```

Load balaning

Purpose

Load balancing, which depends on the destination, is the function that gives the efficiency to operate the whole network and balances the traffic at the time.

Example of Load Balancing



When host A is connecting with the remote server D, you can activate the load balancing through serial1 and serial2 between B and C. Host can be served by server through load balancing.

Consideration of Load Balancing

To use the load balancing function, please check the router which contains the perfect management of packet.

LANBIRD's product has the tremendous packet managing ability which handles E1*2(4.096M) on WAN.

LANBIRD's product contain the remarkable 8M performance on WAN, namely, it offers the perfect managing ability of 4M*2.

What is Metric?

Metric is the measure that determines for forwarding the packet through what interface and gateway when adding the static route table.

When user inputs more than 2 static route table to the same destination, it will communicate through the high priority (lower metric value).

To the same priority(same metric value), it will communicate with the destination through load balancing.

※ using metric value on LANBIRD router, you can organize the environment you wish to have through the load balancing function. Namely, if you give the same metric value, the load balancing function will be executed. Moreover, the dynamic back up will be executed if you give the different metric value. When the load balancing function is executing, even an interface is down, the communication will be continuous to the interface which is up.

LANBIRD Load balancing Configuring Tips

1. draw a whole network structure
2. predict the data flow and calculate the metric value to each destination
3. input destination, gateway and metric value to the route table
4. conform route table through the command show route table

※when configuring route table to the same destination on LANBIRD Router, it will communicate with the destination by the data which has the higher priority.

Method of Configuration

This function is available for configuring command ip-address and ip-route.

Through the command “ip-route”, input interface(or Ethernet local ip address), which depends on the destination and metric value.

When communicating with the destination through balancing, you must configure the equal metric value to the destination.

When using product of LANBIRD, you can conform the inputting value by ip-address and ip-route. Through the command “show route”, you can also check the route table that depends on the metric value of destination by high priority(lower metric value). In addition, more than 2 data must be configured to the same destination if you want to activate the load balancing.

※caution : check the inputting data and route table constantly.

Command

The command ip-route has changed after version 0.3.9 as follows.

Using the command ip-route, you can configure the load balancing function for setting the same metric value for the same destination.

Command	Description
IP-route add *dest-IP-addr dest-IP-mask {fw-IP-addr|ifnum } [metric]*	Add Static route
IP-route delete *dest-IP-addr* **IP-route delete *dest-IP-addr dest-IP-mask*** **IP-route delete dest-IP-addr dest-IP-mask {fw-IP-addr|ifnum} [metric]**	Delete Static route

add adding routing path.

delete deleting routing path.

dest-IP-addr destination IP address

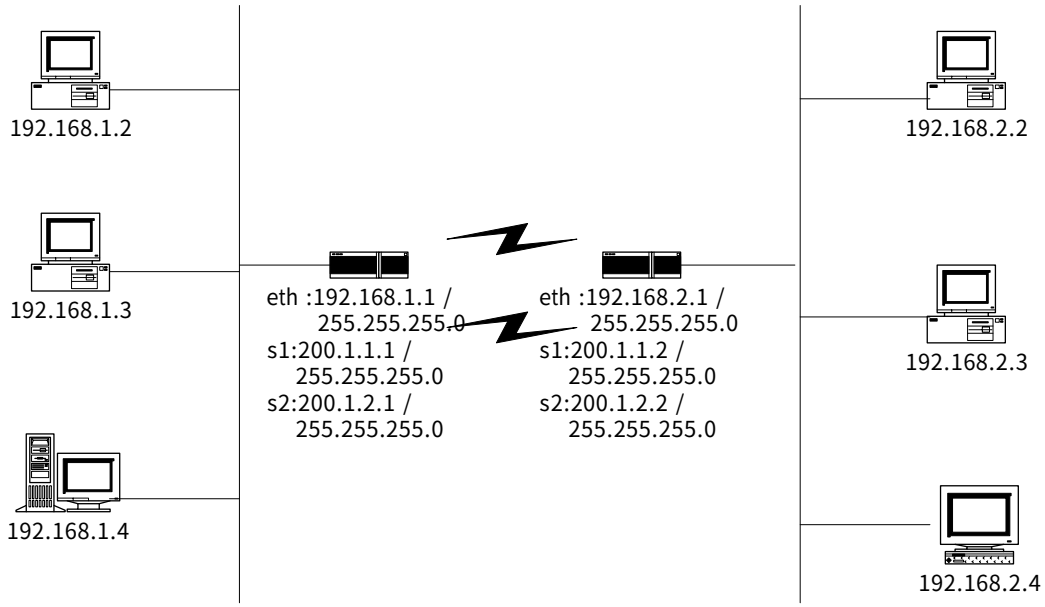
dest-IP destination IP mask

fw-IP-addr	IP address of a forwarding router
ifnum	interface number of a forwarding router
metric	< 1-255>

※If you don't input the metric value, it configures as default 1.

Example

Next is the example that is the configuration which is for executing the load balancing.



When A and B are communicating, you can use serial1 and serial2 to break up the traffic.

Giving Condition

```
A: serial1 IP address : 200.1.1.1 subnetmask : 255.255.255.0
Serial2 IP address : 200.1.2.1 subnetmask : 255.255.255.0
Static route
destination : 0.0.0.0 0.0.0.0     interface : 1
destination : 0.0.0.0 0.0.0.0     interface : 2
```

when configuring on Router A

```
LANBIRD(config)# IP-address add 1 200.1.1.1 255.255.255.0
LANBIRD(config)# IP-address add 2 200.1.2.1 255.255.255.0
LANBIRD(config)# IP-route add 0.0.0.0 0.0.0.0 1 2
LANBIRD(config)# IP-route add 0.0.0.0 0.0.0.0 2 2
```

Conforming Configuration

Conforming the configuration as above is as follow.

Using command show rconfig to conform the status of Router A.

```
LANBIRD(config)# show rconfig
Current running configuration:
|
Ethernet0:
no IP-address
Serial1:
   IP-address 200.1.1.1 255.255.255.0
   line-protocol autodetect (ppp/hdlc)
Serial2:
   IP-address 200.1.2.1 255.255.255.0
   line-protocol autodetect (ppp/hdlc)
|
IP-route 0.0.0.0 0.0.0.0 interface 1
IP-route 0.0.0.0 0.0.0.0 interface 2
|
```

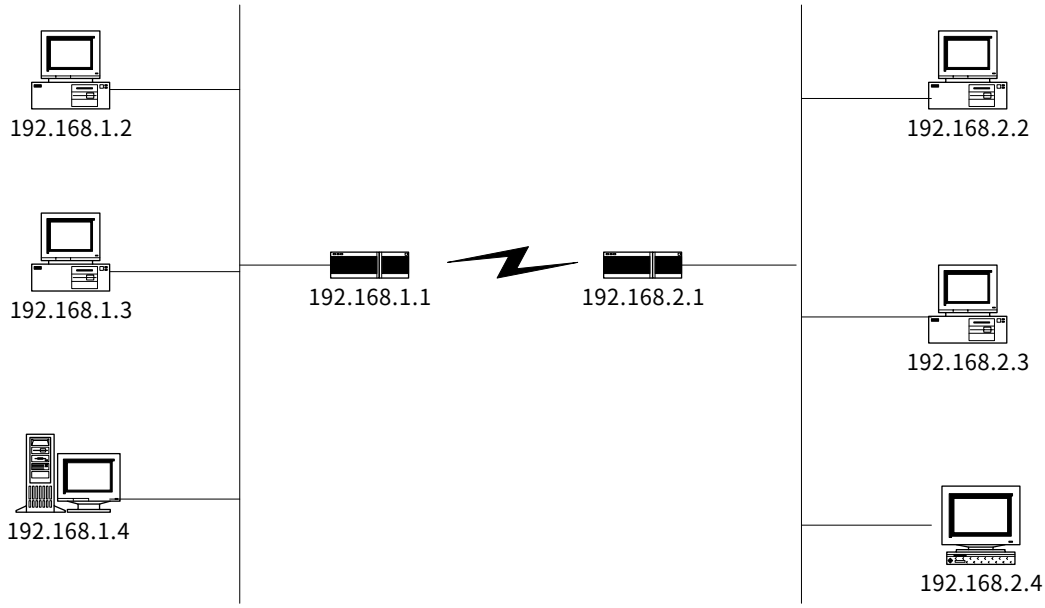
Using command show route to conform the status of Router A

```
LANBIRD(config)# show route
IP Routing table: L (local), S (static)
   Destination       Subnet Mask       Metric and Gateway
- --------------- --------------- ----------------------------
L 200.1.1.0         255.255.255.0     [0] connected to interface 1
L 200.1.2.0         255.255.255.0     [0] connected to interface 2
S 0.0.0.0             0.0.0.0           [2] via interface 1
S 0.0.0.0             0.0.0.0           [2] via interface 2
// Through interface 1and interface 2 to do load balancing for the same destination
```

UDP forward

UDP forward is the function that is for the uses of file sharing. All hosts must exist on the same network. However, it is not capable for the uses of file sharing when hosts are existed on the remote. For doing file sharing with the remote, you only need to forward UDP packet for the availability of sharing file.

Example



The Network 192.168.1.0 The Network 192.168.2.0

As the diagram above, different network 192.168.1.0 and network 192.168.2.0 can share file as well.

Advantages of UDP Forwarding

The form of udp forwarding forwards the udp packet to the willing destination you wish to reach. Additionally, udp forwarding reduces the unnecessary data to whom it forwards. It is different from IPX of which it gains the bandwidth.

Required Information of Forwarding udp Packet

For doing udp packet forwarding, following information such as interface, ip address and port will be required.

Interface : determine to what interface the data should be forwarded

IP-address : represents destination ip address

Port: determine to what kinds of port should be forwarded

Using Tips

Add/Delete Helper

Add/Delete the helper for forwarding UDP packet to the destination.

when configuring helper, you can use the information which contains the interface number and destination to add/delete through the commands which represent below.

Grammar	Description
udp-forward helper add <ifnum> <dest-IP-address>	Add Helper
udp-forward helper del <ifnum> <dest-IP-address>	Delete Helper

<if_num> interface number

<dest-ip-address> destination ip address

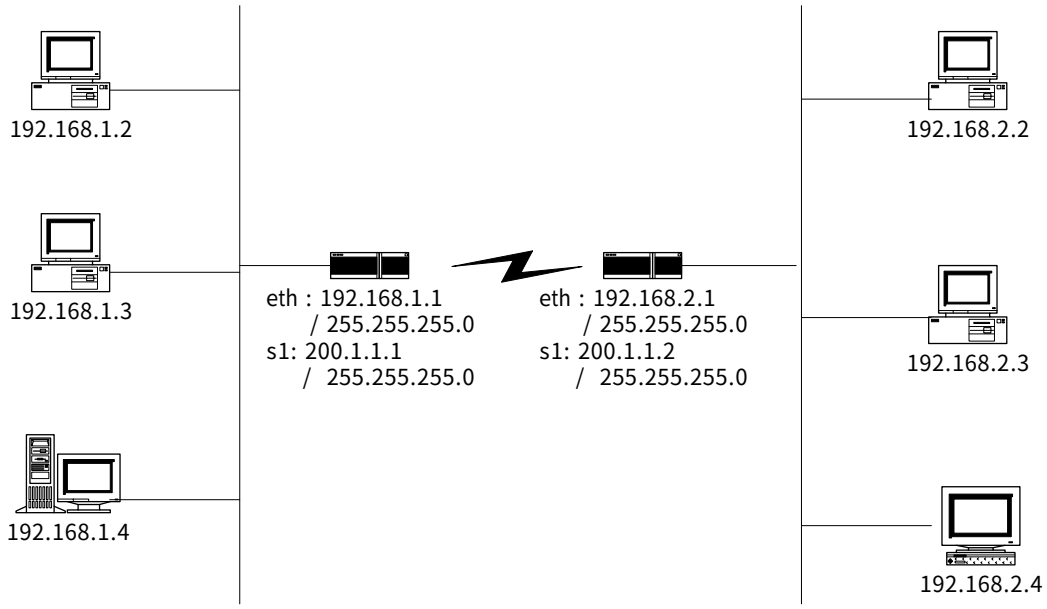
Add/Delete Port

Add/Delete the udp packet that you are willing forwarding by through the commands which represent below.

Grammar	Description
udp-forward port add <1-65535>	Add udp port for forwarding
udp-forward port del <1-65535>	Delete udp port for forwarding

Example

Next is the example that shares the files between the network of main office 192.168.1.0 and the network of branch office 192.168.2.0.



The method of doing file sharing between network 10.1.1.0 and network 10.1.2.0 under Window environment

The method of configuration on gateway 10.1.1.1

```
1. LANBIRD(config)# udp-forward helper add 0 192.168.2.255
2. LANBIRD(config)# udp-forward port add 137
3. LANBIRD(config)# udp-forward port add 138
```

1. using command udp-forward helper to configure the availability of forwarding udp packet to 10.1.2.255
2. configuring udp port 137 for forwarding
3. configuring udp port 138 for forwarding

configuring step 2 and 3 for the availability of Window file sharing between two networks

The method of configuration on gateway 10.1.2.1

```
1. LANBIRD(config)# udp-forward helper add 0 192.168.1.255
2. LANBIRD(config)# udp-forward port add 137
      3. LANBIRD(config)# udp-forward port add 138
```

All methods are same, besides configuring helper destination to 10.1.1.255.

Queueing

Queueing is the function that offers the services to whom and how when packet comes into the router.

Types of Queueing

FIFO (Fast In Fast Out) : : Offers the service to the packet which comes into the router first.

WFQ (Weighted fair queueing) : unlike FIFO, it offers the equal service to each user.

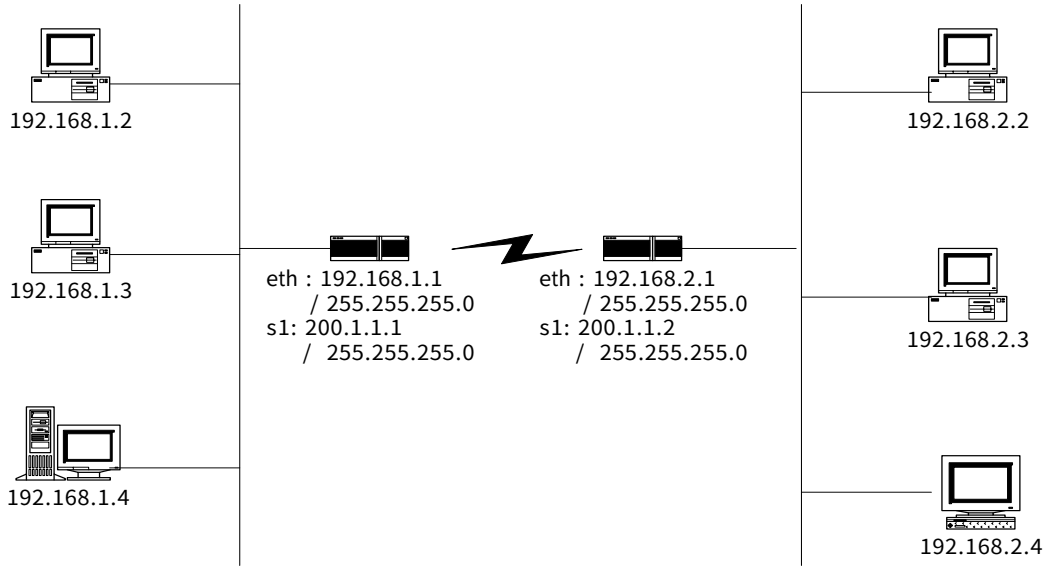
Advantages of WFQ

When a user monopolizes the bandwidth, the service for the rest of users will be slow down. The Weighted Fair Queueing(WFQ) is the necessary function that shares the equal bandwidth and gets the faster Service to users.

※ LANBIRD offers WFQ perfectly. Moreover, the performance of WFQ which LANBIRD offers is tremendously superior than Cisco offers.

※ LANBIRD's product offers the better QoS through WFQ.

Example



If the host 192.168.1.2 monopolizes the bandwidth such as video chatting, video conferencing, etc., the service for other users will be slow down. At this time, you can use WFQ(weighted Fair Queuing) to restrict the bandwidth which 192.168.1.2 is using, as a result, other users will be offered the faster service.

Using Tips

the types of queueings which LANBIRD has are FIFO and WFQ. The commands which offer the configuration are as below.

Command	Explanation
queueing <ifnum> fifo	**Execute fifo queueing**
queueing <ifnum> wfq <64-1000>	**Execute weighted fari queueing**

<ifnum> interface Number

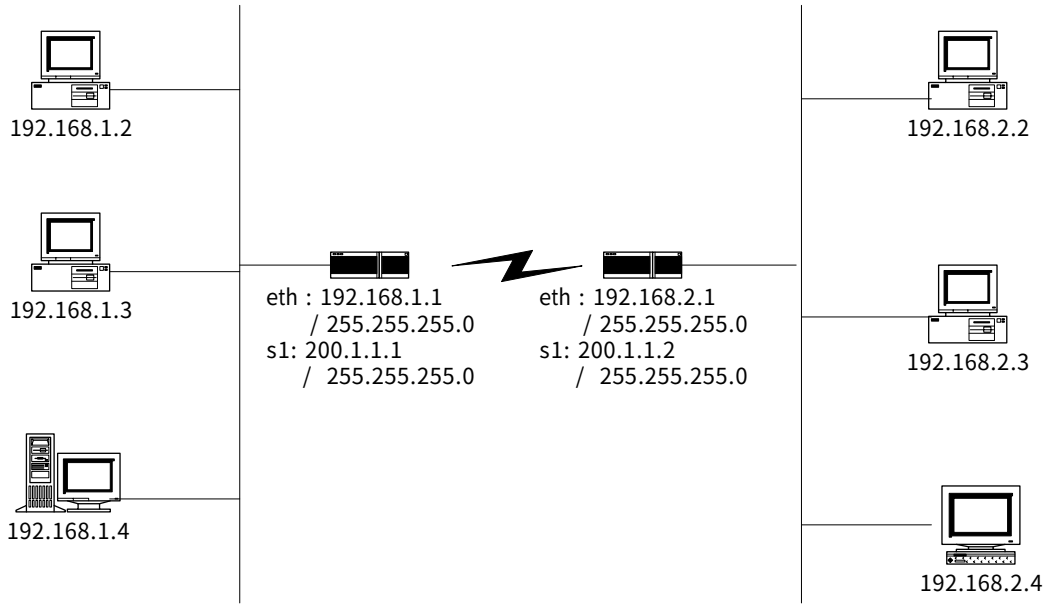
wfq : weighted fair queueing

fifo : FIFO queueing

<64-1000> : threshold(default : 1000)

※WFQ has been configured as the default value.

Example



The configuring method of Weighted Fair Queueing to 10.1.1.0 users.

```
LANBIRD(config)# queueing 1 wfq
```

TIP

Without any configuration, LANBIRD 1004 is using Weighted Fair Queueing as default. In addition, LANBIRD 1004 always offers the equal service to every user.

User

The command “user” is the function that verifies the user who has the authority to be connected with the router.

Using Tips

You can use the command "user" to configure it if you wish to allocate an authority to user for approaching the router. Next is the forms of commands which is related to the configuration.

Command	Description
User add <ip-addr> *[<subnet_mask>]*	**Add user**
User del <ip-addr> *[<subnet_mask>]*	**Delete user**

Add : add user

Del : delete user

<Ip-addr> : network ip or host ip

<Subnet_mask> : subnet mask

※ You can input 5 values as the maximum

※ User del <ip>255.255.255.255 and user del <ip> are the same command

※ When adding or deleting by the network unit, you have touse subnet mask option

Consideration

1. when doing telnet connection, user, with an unauthorized approach, will be accomplished by tcp connection.

※ the message represents the connection is lost when using the command "user".(After the connection, it cuts off)

※ the message represent when blocking telnet port by using filtering.(can't be connected at all)

※ tcp connection is available, but the connection with host has cut. As the result, you have to check whether the command "user" has set or not through the message which represents on the screen.

2. Before configuring the command "user", user who is on telnet connection can connect with it continuously. After configuring the command "user", user who is unauthorized can't connect with telnet connection. Namely, after configuring the command "user", an authorized user and user who had connected before it configured can do telnet connection to the router.

3. Using "show user" to check the current status of user who is on the connection.

Before configuring the command "user", user who is unauthorized and on the connection through telnet can be remove through the command "disconnect <shell_ID>.

Example

When adding the configuration

Permit telnet connection to the user who is on the network 211.32.101.16 / 255.255.255.240

```
LANBIRD(config)# user add 211.32.101.16 255.255.255.240
```

Permit telnet connection to the host 211.32.101.18

```
LANBIRD(config)# user add 211.32.101.18
```

or

```
LANBIRD(config)# user add 211.32.101.18 255.255.255.255
```

When deleting the configuration

Delete the content of configuration to 211.32.101.16 / 255.255.255.240

```
LANBIRD(config)# user del 211.32.101.16 255.255.255.240
```

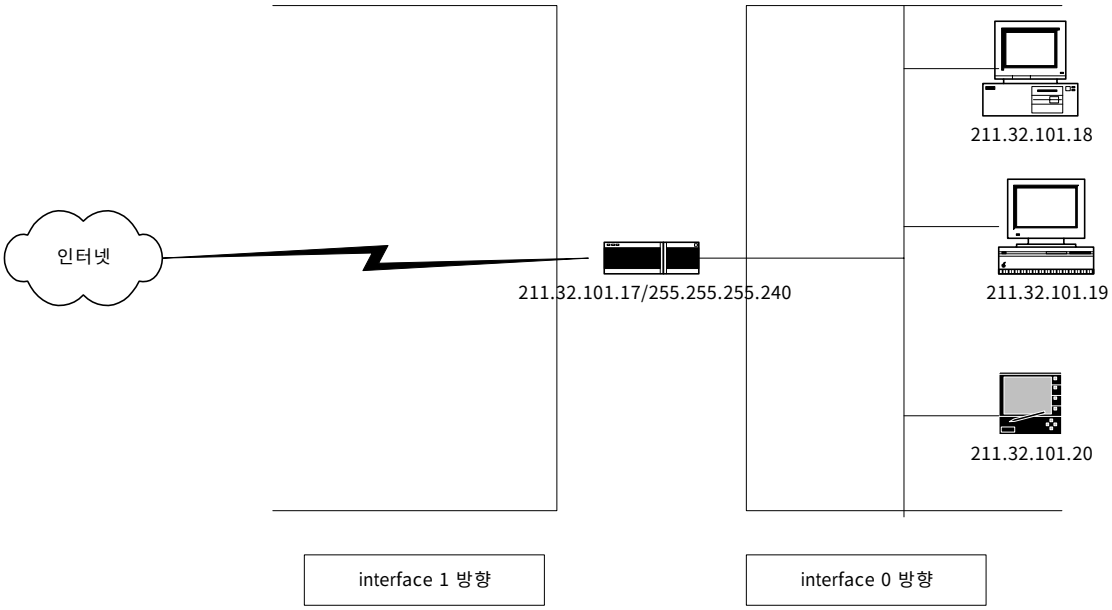
```
LANBIRD(config)# user del 211.32.101.16 255.255.255.240
```

```
LANBIRD(config)# user del 211.32.101.18
or
LANBIRD(config)# user del 211.32.101.18 255.255.255.255
```

IP-account

Working Principle

IP-account is the function that is to understand the amount of traffics on each interface



※ It represents the information of traffic which is for the interior ip when enable ip-account to the interface which linked with the interior.

※ It represents the information of traffic which is for Internet direction when enable ip-account to the interface which linked with Internet direction.

Related Command

Command	Description
Ip-account <*if_num*> enable	Enable ip account
Ip-account <*if_num*> disable	Disable ip account
show ip-account <*if_num*>	Indicate the table which is related to ip-account
clear ip-account <*if_num*>	Clear the table which is related to ip-account

※ ***<if_num>*** : interface number

Example

```
LANBIRD(config)# ip-account enable 0
```

※ enable ip-account to the interface 0

Conforming ip-account table

show ip-account <if_num>

It indicates the traffic information of ip on which the communication has happened

within 10 minutes

```
LANBIRD> sh ip 0
Accounting period: 2d 23:48:22
                          Input                    Output
IP Address              packets      bytes       packets      bytes
--------------- ---------- --------- -------- ---------
211.32.101.18              204      25977             0          0
211.32.101.19              769     110980             0          0
211.32.101.20             5689     579347           937      57380
211.32.101.21              226      38750             0          0
211.32.101.22              544      96004             0          0
211.32.101.23              569      98472             0          0
```

※ Command mode : user mode, root mode

※ Router(211.32.101.17) recived 56,89(573,947bytes) packets from 211.32.101.20. On the contrary, router(211.32.101.17) delivered 937 packets(57,380bytes) to 211.32.101.20. Namely, if you think it on the position of PC, the explanation is as below.

PC delivered 5689 packets(57,394bytes). On the contrary, It recivied 937 packet (57,380bytes).

※ Account period is the function that represents the time elapse of activating ip-account. In addition, using the command "clear ip-account" to delete the ip-account table, it represents the time elapse.

※ It represents the table that ip has been communicated for recent 10 minutes.

clear ip-account <if_num>

```
LANBIRD# clear ip-account 0
LANBIRD # sh ip-account 0
Accounting period: 0d 00:00:00
                          Input                    Output
IP Address                packets        bytes     packets        bytes
--------------- ---------- ---------- ---------- ----------
LANBIRD #
```

※ command mode : root mode

※ Accounting period will be 0d 00:00:00 and the value of table will be indicated when you use the command "clear ip-account".

NULL Interface

Working Principle

Null interface is the function that has been made as a virtual interface. Null interface is always up, but it doesn't converge or receive traffic. On the other hand, null interface provides various ways for filtering the traffic.

Example

As the figure above, from the router 192.168.1.1 to the network 10.1.100.0, routing goes through the serial interface. If the default path is 192.168.1.143, the loop remains within TTL(Time To Alive) when the serial interface is down.

Hence, you have to give the higher metric value for the path 10.1.100.0 and assign as a null interface. In addition, this function reduces the phenomenon that the packet goes around the network when serial interface occurs problem.

How to use

You can use the command “ip-route” to add on configuration.

Command	Explanation
Ip-route add ip-addr ip-mask null <metric>	Set network path as null interface 로
Ip-route del ip-addr	Delete configured path which has been set as Null interface

Null interface Example

```
LANBIRD(config)# ip-filter set 0 input permit
LANBIRD(config)# sh rconfig
Current running configuration:
|
Ethernet0:
   ip-address 192.168.1.1 255.255.255.0
   ip-filter input permit default
Serial1:
   ip-address 200.1.1.1 255.255.255.0
   line-protocol autodetect (ppp/hdlc)
Serial2:
   no ip-address
   line-protocol autodetect (ppp/hdlc)
|
ip-route 0.0.0.0 0.0.0.0 192.168.1.143
ip-route 10.1.100.0 255.255.255.0 interface 1
ip-route 10.1.100.0 255.255.255.0 null 10
```

The network 10.1.100.0 registered the interface1 and null interface on the routing table. In this case, the function prevents the loop that packet returning to default table when interface1 is down.

In this case, you can use “sh ro” to check the routing table. When interface1 is connected normally, you can refer to the box below.

```
LANBIRD> sh ro
IP Routing table: L (local), S (static)
   Destination        Subnet Mask        Metric and Gateway
- --------------- --------------- ----------------------------
L 10.1.100.0         255.255.255.0     [0] connected to interface 1
S 0.0.0.0            0.0.0.0           [1] via 192.168.1.143
```

When Interface 1 is dowm

```
LANBIRD> sh ro
IP Routing table: L (local), S (static)
   Destination        Subnet Mask        Metric and Gateway
- --------------- --------------- ----------------------------
L 10.1.100.0        255.255.255.0     [10] connected to null
S 0.0.0.0           0.0.0.0           [1] via 192.168.1.143
```

In this case, the packet, which goes through 10.1.100.0 will be gone through null interface

Appendix 1. Subnet mask and available IP addresses

The following table shows how to use IP addresses of the A.B.C.x network according to various types of subnet mask.

Subnet mask 255.255.255.128

Network IP	First IP	Last IP	Broadcast IP
A.B.C.0	A.B.C.1	A.B.C.126	A.B.C.127
A.B.C.128	A.B.C.129	A.B.C.254	A.B.C.255

Subnet mask 255.255.255.192

Network IP	First IP	Last IP	Broadcast IP
A.B.C.0	A.B.C.1	A.B.C.62	A.B.C.63
A.B.C.64	A.B.C.65	A.B.C.126	A.B.C.127
A.B.C.128	A.B.C.129	A.B.C.190	A.B.C.191
A.B.C.192	A.B.C.193	A.B.C.254	A.B.C.255

Subnet mask 255.255.255.224

Network IP	First IP	Last IP	Broadcast IP
A.B.C.0	A.B.C.1	A.B.C.30	A.B.C.31
A.B.C.32	A.B.C.33	A.B.C.62	A.B.C.63
A.B.C.64	A.B.C.65	A.B.C.94	A.B.C.95
A.B.C.96	A.B.C.97	A.B.C.126	A.B.C.127
A.B.C.128	A.B.C.129	A.B.C.158	A.B.C.159
A.B.C.160	A.B.C.161	A.B.C.190	A.B.C.191
A.B.C.192	A.B.C.193	A.B.C.222	A.B.C.223
A.B.C.224	A.B.C.225	A.B.C.254	A.B.C.255

Subnet mask 255.255.255.240

Network IP	First IP	Last IP	Broadcast IP
A.B.C.0	A.B.C.1	A.B.C.14	A.B.C.15
A.B.C.16	A.B.C.17	A.B.C.30	A.B.C.31
A.B.C.32	A.B.C.33	A.B.C.46	A.B.C.47
A.B.C.48	A.B.C.49	A.B.C.62	A.B.C.63
A.B.C.64	A.B.C.65	A.B.C.78	A.B.C.79
A.B.C.80	A.B.C.81	A.B.C.94	A.B.C.95
A.B.C.96	A.B.C.97	A.B.C.110	A.B.C.111
A.B.C.112	A.B.C.113	A.B.C.126	A.B.C.127
A.B.C.128	A.B.C.129	A.B.C.142	A.B.C.143
A.B.C.144	A.B.C.145	A.B.C.158	A.B.C.159
A.B.C.160	A.B.C.161	A.B.C.174	A.B.C.175
A.B.C.176	A.B.C.177	A.B.C.190	A.B.C.191
A.B.C.192	A.B.C.193	A.B.C.206	A.B.C.207
A.B.C.208	A.B.C.209	A.B.C.222	A.B.C.223
A.B.C.224	A.B.C.225	A.B.C.238	A.B.C.239
A.B.C.240	A.B.C.241	A.B.C.254	A.B.C.255

Subnet mask 255.255.255.248

Network IP	First IP	Last IP	Broadcast IP
A.B.C.0	A.B.C.1	A.B.C.6	A.B.C.7
A.B.C.8	A.B.C.9	A.B.C.14	A.B.C.15
A.B.C.16	A.B.C.17	A.B.C.22	A.B.C.23
A.B.C.24	A.B.C.25	A.B.C.30	A.B.C.31
A.B.C.32	A.B.C.33	A.B.C.38	A.B.C.39
A.B.C.40	A.B.C.41	A.B.C.46	A.B.C.47
A.B.C.48	A.B.C.49	A.B.C.54	A.B.C.55
A.B.C.56	A.B.C.57	A.B.C.62	A.B.C.63
A.B.C.64	A.B.C.65	A.B.C.70	A.B.C.71
A.B.C.72	A.B.C.73	A.B.C.78	A.B.C.79
A.B.C.80	A.B.C.81	A.B.C.86	A.B.C.87
A.B.C.88	A.B.C.89	A.B.C.94	A.B.C.95
A.B.C.96	A.B.C.97	A.B.C.102	A.B.C.103
A.B.C.104	A.B.C.105	A.B.C.110	A.B.C.111
A.B.C.112	A.B.C.113	A.B.C.118	A.B.C.119
A.B.C.120	A.B.C.121	A.B.C.126	A.B.C.127
A.B.C.128	A.B.C.129	A.B.C.134	A.B.C.135
A.B.C.136	A.B.C.137	A.B.C.142	A.B.C.143
A.B.C.144	A.B.C.145	A.B.C.150	A.B.C.151
A.B.C.152	A.B.C.153	A.B.C.158	A.B.C.159
A.B.C.160	A.B.C.161	A.B.C.166	A.B.C.167
A.B.C.168	A.B.C.169	A.B.C.174	A.B.C.175
A.B.C.176	A.B.C.177	A.B.C.182	A.B.C.183
A.B.C.184	A.B.C.185	A.B.C.190	A.B.C.191
A.B.C.192	A.B.C.193	A.B.C.198	A.B.C.199
A.B.C.200	A.B.C.201	A.B.C.206	A.B.C.207
A.B.C.208	A.B.C.209	A.B.C.214	A.B.C.215
A.B.C.216	A.B.C.217	A.B.C.222	A.B.C.223
A.B.C.224	A.B.C.225	A.B.C.230	A.B.C.231
A.B.C.232	A.B.C.233	A.B.C.238	A.B.C.239
A.B.C.240	A.B.C.241	A.B.C.246	A.B.C.247
A.B.C.248	A.B.C.249	A.B.C.254	A.B.C.255

Subnet mask 255.255.255.252

Network IP	First IP	Last IP	Broadcast IP
A.B.C.0	A.B.C.1	A.B.C.2	A.B.C.3
A.B.C.4	A.B.C.5	A.B.C.6	A.B.C.7
A.B.C.8	A.B.C.9	A.B.C.10	A.B.C.11
A.B.C.12	A.B.C.13	A.B.C.14	A.B.C.15
A.B.C.16	A.B.C.17	A.B.C.18	A.B.C.19
A.B.C.20	A.B.C.21	A.B.C.22	A.B.C.23
A.B.C.24	A.B.C.25	A.B.C.26	A.B.C.27
A.B.C.28	A.B.C.29	A.B.C.30	A.B.C.31
A.B.C.32	A.B.C.33	A.B.C.34	A.B.C.35
A.B.C.36	A.B.C.37	A.B.C.38	A.B.C.39
A.B.C.40	A.B.C.41	A.B.C.42	A.B.C.43
A.B.C.44	A.B.C.45	A.B.C.46	A.B.C.47
A.B.C.48	A.B.C.49	A.B.C.50	A.B.C.51
A.B.C.52	A.B.C.53	A.B.C.54	A.B.C.55
A.B.C.56	A.B.C.57	A.B.C.58	A.B.C.59
A.B.C.60	A.B.C.61	A.B.C.62	A.B.C.63
A.B.C.64	A.B.C.65	A.B.C.66	A.B.C.67
A.B.C.68	A.B.C.69	A.B.C.70	A.B.C.71
A.B.C.72	A.B.C.73	A.B.C.74	A.B.C.75
A.B.C.76	A.B.C.77	A.B.C.78	A.B.C.79
A.B.C.80	A.B.C.81	A.B.C.82	A.B.C.83
A.B.C.84	A.B.C.85	A.B.C.86	A.B.C.87
A.B.C.88	A.B.C.89	A.B.C.90	A.B.C.91
A.B.C.92	A.B.C.93	A.B.C.94	A.B.C.95
A.B.C.96	A.B.C.97	A.B.C.98	A.B.C.99
A.B.C.100	A.B.C.101	A.B.C.102	A.B.C.103
A.B.C.104	A.B.C.105	A.B.C.106	A.B.C.107
A.B.C.108	A.B.C.109	A.B.C.110	A.B.C.111
A.B.C.112	A.B.C.113	A.B.C.114	A.B.C.115
A.B.C.116	A.B.C.117	A.B.C.118	A.B.C.119
A.B.C.120	A.B.C.121	A.B.C.122	A.B.C.123
A.B.C.124	A.B.C.125	A.B.C.126	A.B.C.127
A.B.C.128	A.B.C.129	A.B.C.130	A.B.C.131
A.B.C.132	A.B.C.133	A.B.C.134	A.B.C.135
A.B.C.136	A.B.C.137	A.B.C.138	A.B.C.139
A.B.C.140	A.B.C.141	A.B.C.142	A.B.C.143
A.B.C.144	A.B.C.145	A.B.C.146	A.B.C.147
A.B.C.148	A.B.C.149	A.B.C.150	A.B.C.151
A.B.C.152	A.B.C.153	A.B.C.154	A.B.C.155
A.B.C.156	A.B.C.157	A.B.C.158	A.B.C.159
A.B.C.160	A.B.C.161	A.B.C.162	A.B.C.163
A.B.C.164	A.B.C.165	A.B.C.166	A.B.C.167
A.B.C.168	A.B.C.169	A.B.C.170	A.B.C.171
A.B.C.172	A.B.C.173	A.B.C.174	A.B.C.175
A.B.C.176	A.B.C.177	A.B.C.178	A.B.C.179
A.B.C.180	A.B.C.181	A.B.C.182	A.B.C.183
A.B.C.184	A.B.C.185	A.B.C.186	A.B.C.187
A.B.C.188	A.B.C.189	A.B.C.190	A.B.C.191
A.B.C.192	A.B.C.193	A.B.C.194	A.B.C.195
A.B.C.196	A.B.C.197	A.B.C.198	A.B.C.199
A.B.C.200	A.B.C.201	A.B.C.202	A.B.C.203
A.B.C.204	A.B.C.205	A.B.C.206	A.B.C.207
A.B.C.208	A.B.C.209	A.B.C.210	A.B.C.211
A.B.C.212	A.B.C.213	A.B.C.214	A.B.C.215
A.B.C.216	A.B.C.217	A.B.C.218	A.B.C.219
A.B.C.220	A.B.C.221	A.B.C.222	A.B.C.223
A.B.C.224	A.B.C.225	A.B.C.226	A.B.C.227
A.B.C.228	A.B.C.229	A.B.C.230	A.B.C.231
A.B.C.232	A.B.C.233	A.B.C.234	A.B.C.235
A.B.C.236	A.B.C.237	A.B.C.238	A.B.C.239
A.B.C.240	A.B.C.241	A.B.C.242	A.B.C.243
A.B.C.244	A.B.C.245	A.B.C.246	A.B.C.247

A.B.C.248	A.B.C.249	A.B.C.250	A.B.C.251
A.B.C.252	A.B.C.253	A.B.C.254	A.B.C.255

Appendix 2. Examples of Lanbird 1004 Router NAT Configuration (version 0.3.5 and later)

It is assumed that the IP addresses assigned to subscribers are as follows:

Interface	IP address	Subnet mask
Ethernet IP	211.32.101.16 ~ 31	255.255.255.240
Serial IP	192.168.150.194	255.255.255.252

Examples of router configuration

1. LANBIRD(config)# ip-address add 0 192.168.1.1 255.255.255.0
2. LANBIRD(config)# ip-address add 1 **192.168.150.194 255.255.255.252**
3. LANBIRD(config)# ip-route add 0.0.0.0 0.0.0.0 1
4. LANBIRD(config)# nat enable 1
5. LANBIRD(config)# nat out-public add **211.32.101.16 255.255.255.240**
6. LANBIRD(config)# nat out-napt add **211.32.101.17**
7. LANBIRD(config)# nat in-server add udp 6112 255.255.255.255
8. LANBIRD(config)# nat in-server add udp 51200 255.255.255.255
9. LANBIRD(config)# ip-address add 0 **211.32.101.17** 255.255.255.255 secondary
10. LANBIRD(config)# write

In the above examples, the values in the boxes should be replaced by the IP addresses initially given. The following describes the configuration method.

1. Configure the Ethernet IP of the router (private IP is set for the Ethernet IP.).
2. Configure the serial IP of the router.
3. Configure the default route of the router.
4. Enable NAT of the router.
5. Configure the pub-IP-network to be used by NAT.
6. Designate the NAPT (PAT) IP address to be used by NAT.
7. Configure such that battlenet can be used by NAT.
8. Configure such that dialpad can be used by NAT.
9. **Configuring the IP set for PAT to the secondary IP of the Ethernet** to enable the telnet connection to the router from the outside network
10. Save the set values in the flash memory

If the set values are verified by means of **"show config"** command, the followings should be displayed.

```
LANBIRD# show config
Saved configuration
|
Ethernet:
ip address 192.168.1.1 255.255.255.0
ip address 211.32.101.17 255.255.255.255 secondary
Serial1 (sync):
ip address 192.168.150.194 255.255.255.252
line-protocol autodetect (ppp/hdlc)
Serial2 (sync):
no ip address
line-protocol autodetect (ppp/hdlc)
|
ip route 0.0.0.0 0.0.0.0 interface 1
|
nat enabled interface 1
in-server UDP 6112 255.255.255.255
in-server UDP 51200 255.255.255.255
out-napt 211.32.101.17
out-public 211.32.101.16 255.255.255.240
|
LANBIRD#
```

Example of subscriber PC configuration:

```
IP address          : Allocate one of 192.168.1.2 to 254
Subnet mask         : 255.255.255.0
Gateway             : 192.168.1.1
```