

Table 46 Network Setting > QoS > General (continued) (continued)

LABEL	DESCRIPTION
Upstream traffic priority Assigned by	<p>Select how the Zyxel Device assigns priorities to various upstream traffic flows.</p> <ul style="list-style-type: none"> • None: Disables auto priority mapping and has the Zyxel Device put packets into the queues according to your classification rules. Traffic which does not match any of the classification rules is mapped into the default queue with the lowest priority. • Ethernet Priority: Automatically assign priority based on the IEEE 802.1p priority level. • IP Precedence: Automatically assign priority based on the first three bits of the TOS field in the IP header. • Packet Length: Automatically assign priority based on the packet size. Smaller packets get higher priority since control, signaling, VoIP, Internet gaming, or other real-time packets are usually small while larger packets are usually best effort data packets like file transfers.
Cancel	Click Cancel to restore your previously saved settings.
Apply	Click Apply to save your changes.

10.4 Queue Setup

Click **Network Setting > QoS > Queue Setup** to open the screen as shown next.

Use this screen to configure QoS queue assignment to decide the priority on WAN/LAN interfaces. Traffic with higher priority gets through faster than those with lower priority. Low-priority traffic is dropped first when the network is congested.

Note: Configure the priority level for a QoS queue from 1 to 8. The smaller the number in the **Priority** column, the higher the priority.

Note: The corresponding classifier(s) will be removed automatically if a queue is deleted.

Note: Rate limit 0 means there is no rate limit on a queue.

Figure 87 Network Setting > QoS > Queue Setup

QoS

General **Queue Setup** Classification Setup Shaper Setup Policer Setup

Queue Setup decides the priority on WAN/LAN interfaces. Use this page to configure QoS queue assignment.

+ Add New Queue

#	Status	Name	Interface	Priority	Weight	Buffer Management	Rate Limit	Modify
1		default queue	WAN	8	1	DT		

Note

- (1) Maximum 7 configurable entries and 1 unconfigurable default queue for WAN port.
- (2) Priority level 1 is the highest priority for QoS.
- (3) Rate limit 0 is max bandwidth.
- (4) If queue is deleted, then related classifiers will be removed too.

The following table describes the labels in this screen.

Table 47 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Add New Queue	Click this button to create a new queue entry.
#	This is the index number of the entry.
Status	This field displays whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the Zyxel Device's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue. The lower the number, the higher the priority level.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used for this queue. Queue management algorithms determine how the Zyxel Device should handle packets when it receives too many (network congestion).
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue. Rate limit 0 means there's no rate limit on this queue.
Modify	Click the Edit icon to edit the queue. Click the Delete icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

10.4.1 Adding a QoS Queue

Click **Add New Queue** or the **Edit** icon in the **Queue Setup** screen to configure a queue.


Figure 88 Queue Setup: Add

The screenshot shows the 'Add New Queue' configuration window. It includes the following elements:

- Active:** A blue toggle switch is turned on.
- Name:** An empty text input field.
- Interface:** A dropdown menu with 'WAN' selected.
- Priority:** A dropdown menu with '1 (Highest)' selected.
- Weight:** A dropdown menu with '1' selected.
- Buffer Management:** A dropdown menu with 'Drop Tail(DT)' selected.
- Rate Limit:** An empty text input field with a '(kbps)' label to its right.
- Buttons:** 'Cancel' and 'OK' buttons are located at the bottom center.

The following table describes the labels in this screen.

Table 48 Queue Setup: Add

LABEL	DESCRIPTION
Active	Click this switch to enable or disable the queue. When the switch turns blue  , the function is enabled. Otherwise, it is not.
Name	Enter the descriptive name of this queue.
Interface	Select the interface to which this queue is applied. This field is read-only if you are editing the queue.
Priority	Select the priority level (from 1 to 7) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the Zyxel Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Buffer Management	This field displays Drop Tail (DT) . Drop Tail (DT) is a simple queue management algorithm that allows the Zyxel Device buffer to accept as many packets as it can until it is full. Once the buffer is full, new packets that arrive are dropped until there is space in the buffer again (packets are transmitted out of it).
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue. If you enter 0 here, this means there's no rate limit on this queue.
Cancel	Click Cancel to exit this screen without saving any changes.
OK	Click OK to save your changes.

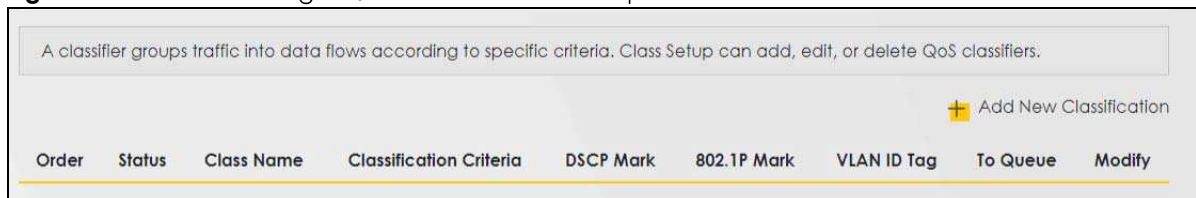
10.5 QoS Classification Setup

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the Zyxel Device forwards through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Network Setting > QoS > Classification Setup** to open the following screen.

Figure 89 Network Setting > QoS > Classification Setup



The following table describes the labels in this screen.

Table 49 Network Setting > QoS > Classification Setup

LABEL	DESCRIPTION
Add New Classification	Click this to create a new classifier.
Order	This is the index number of the entry. The classifiers are applied in order of their numbering.
Status	This field displays whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1P Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.
VLAN ID Tag	This is the VLAN ID number assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the Edit icon to edit the classifier. Click the Delete icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.

10.5.1 Add/Edit QoS Class

Click **Add New Classification** in the **Classification Setup** screen or the **Edit** icon next to a classifier to open the following screen.

Figure 90 Classification Setup: Add/Edit

Add New Classification

Please follow the guidance through step 1~5 to configure a QoS rule

Step1: Class Configuration

Active

Class Name

Classification Order Last

Step2: Criteria Configuration

Use the configurations below to specify the characteristics of a data flow needed to be managed by this QoS rule

Basic

From Interface LAN

Ether Type NA

Source

Address Subnet Mask Exclude

Port Range ~ Exclude

MAC MAC Mask Exclude

Destination

Address Subnet Mask Exclude

Port Range ~ Exclude

MAC MAC Mask Exclude

Others

Service RTSP Server Exclude

IP protocol TCP Exclude

DHCP Exclude

IP Packet Length ~ Exclude

DSCP (0~63) Exclude

802.1P 0 BE Exclude

VLAN ID (1~4094) Exclude

TCP ACK Exclude

Step3: Packet Modification

The content of the packet can be modified by applying the following settings

DSCP Mark Unchange (0~63)

VLAN ID Tag Unchange (1~4094)

802.1P Mark 0 BE

Step4: Class Routing

This module can route a packet to a certain interface according to the class setting

Forward To Interface Unchange

Step5: Outgoing Queue Selection

Outgoing queue decides the priority of the traffic and how traffic should be shaped in the WAN interface.

To Queue Index default queue

The following table describes the labels in this screen.

Table 50 Classification Setup: Add/Edit


LABEL	DESCRIPTION
Step1: Class Configuration	
Active	Click this switch to enable or disable the classifier. When the switch turns blue  , the function is enabled. Otherwise, it is not.
Class Name	Enter a descriptive name of up to 15 printable English keyboard characters, not including spaces.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking Apply . Select Last to put this rule in the back of the classifier list.
Step2: Criteria Configuration	
Basic	
From Interface	If you want to classify the traffic by an ingress interface, select an interface from the From Interface drop-down list box.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select IP , you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select 802.1Q , you can configure an 802.1p priority level.
Source	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Mask	Enter the source subnet mask.
Port Range	If you select TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Mask	Enter the source subnet mask.
Port Range	If you select TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	

Table 50 Classification Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Service	<p>This field is available only when you select IP in the Ether Type field.</p> <p>This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter fields.</p>
IP Protocol	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and select the protocol (service type) from TCP, UDP, ICMP or IGMP. If you select User defined, enter the protocol (service type) number.</p>
DHCP	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and select a DHCP option.</p> <p>If you select Vendor Class ID (DHCP Option 60), enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.</p> <p>If you select Client ID (DHCP Option 61), enter the Identity Association Identifier (IAD Option 61) of the matched traffic, such as the MAC address of the device.</p> <p>If you select User Class ID (DHCP Option 77), enter a string that identifies the user's category or application type in the matched DHCP packets.</p> <p>If you select Vendor Specific Info (DHCP Option 125), enter the vendor specific information of the matched traffic, such as the product class, model name, and serial number of the device.</p>
IP Packet Length	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and enter the minimum and maximum packet length (from 46 to 1500) in the fields provided.</p>
DSCP	<p>This field is available only when you select IP in the Ether Type field.</p> <p>Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.</p>
802.1P	<p>This field is available only when you select 802.1Q in the Ether Type field.</p> <p>Select this option and select a priority level (between 0 and 7) from the drop-down list box. "0" is the lowest priority level and "7" is the highest.</p>
VLAN ID	<p>This field is available only when you select 802.1Q in the Ether Type field.</p> <p>Select this option and specify a VLAN ID number.</p>
TCP ACK	<p>This field is available only when you select IP in the Ether Type field.</p> <p>If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.</p>
Exclude	<p>Select this option to exclude the packets that match the specified criteria from this classifier.</p>
Step3: Packet Modification	
DSCP Mark	<p>This field is available only when you select IP in the Ether Type field.</p> <p>If you select Remark, enter a DSCP value with which the Zyxel Device replaces the DSCP field in the packets.</p> <p>If you select Unchange, the Zyxel Device keep the DSCP field in the packets.</p>
VLAN ID	<p>If you select Remark, enter a VLAN ID number with which the Zyxel Device replaces the VLAN ID of the frames.</p> <p>If you select Remove, the Zyxel Device deletes the VLAN ID of the frames before forwarding them out.</p> <p>If you select Add, the Zyxel Device treat all matched traffic untagged and add a second VLAN ID.</p> <p>If you select Unchange, the Zyxel Device keep the VLAN ID in the packets.</p>

Table 50 Classification Setup: Add/Edit (continued)

LABEL	DESCRIPTION
802.1P Mark	Select a priority level with which the Zyxel Device replaces the IEEE 802.1p priority field in the packets. If you select Unchange , the Zyxel Device keep the 802.1p priority field in the packets.
Step4: Class Routing	
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select Unchange , the Zyxel Device forward traffic of this class according to the default routing table.
Step5: Outgoing Queue Selection	
To Queue Index	Select a queue that applies to this class. You should have configured a queue in the Queue Setup screen already.
Cancel	Click Cancel to exit this screen without saving any changes.
OK	Click OK to save your changes.

10.6 QoS Shaper Setup

This screen lets you use the token bucket algorithm to allow a certain amount of large bursts of traffic while keeping most outgoing traffic at the average rate. Click **Network Setting > QoS > Shaper Setup**. The screen appears as shown.

Figure 91 Network Setting > QoS > Shaper Setup

#	Status	Outgoing Interface	Rate Limit	Modify
+ Add New Shaper				

The following table describes the labels in this screen.

Table 51 Network Setting > QoS > Shaper Setup

LABEL	DESCRIPTION
Add New Shaper	Click this to create a new entry.
#	This is the index number of the entry.
Status	This field displays whether the shaper is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this shaper is not active.
Outgoing Interface	This shows the name of the Zyxel Device's interface through which traffic in this shaper applies.
Rate Limit	This shows the average rate limit of traffic bursts for this shaper.
Modify	Click the Edit icon to edit the shaper. Click the Delete icon to delete an existing shaper. Note that subsequent rules move up by one when you take this action.


10.6.1 Add/Edit a QoS Shaper

Click **Add New Shaper** in the **Shaper Setup** screen or the **Edit** icon next to a shaper to show the following screen.

Figure 92 Shaper Setup: Add/Edit

The following table describes the labels in this screen.

Table 52 Shaper Setup: Add/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable or disable the shaper. When the switch turns blue  , the function is enabled. Otherwise, it is not.
Interface	This field shows ETHWAN as the Zyxel Device's interface through which traffic in this shaper applies.
Rate Limit	Enter the average rate limit of traffic bursts for this shaper.
Cancel	Click Cancel to exit this screen without saving any changes.
OK	Click OK to save your changes.

10.7 QoS Policer Setup

Use this screen to view QoS policers that allow you to limit the transmission rate of incoming traffic and apply actions, such as drop, pass, or modify, to the DSCP value of matched traffic. Click **Network Setting > QoS > Policer Setup**. The screen appears as shown.

Figure 93 Network Setting > QoS > Policer Setup

The following table describes the labels in this screen.

Table 53 Network Setting > QoS > Policer Setup

LABEL	DESCRIPTION
Add new Policer	Click this to create a new entry.
#	This is the index number of the entry.
Status	This field displays whether the policer is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this policer is not active.
Name	This field displays the descriptive name of this policer.
Regulated Classes	This field displays the name of a QoS classifier
Meter Type	This field displays the type of QoS metering algorithm used in this policer.
Rule	These are the rates and burst sizes against which the policer checks the traffic of the member QoS classes.
Action	This shows how the policer has the Zyxel Device treat different types of traffic belonging to the policer's member QoS classes.
Modify	Click the Edit icon to edit the policer. Click the Delete icon to delete an existing policer. Note that subsequent rules move up by one when you take this action.

10.7.1 Add/Edit a QoS Policer

Click **Add New Policer** in the **Policer Setup** screen or the **Edit** icon next to a policer to show the following screen.

Figure 94 Policer Setup: Add/Edit

The following table describes the labels in this screen.

Table 54 Policer Setup: Add/Edit


LABEL	DESCRIPTION
Active	Click this switch to enable or disable the policer. When the switch turns blue  , the function is enabled. Otherwise, it is not.
Name	Enter the descriptive name of this policer.
Meter Type	This shows the traffic metering algorithm used in this policer. The Simple Token Bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. Each token represents one byte. The algorithm allows bursts of up to b bytes which is also the bucket size. The Single Rate Three Color Marker (srTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR), the Committed Burst Size (CBS) and the Excess Burst Size (EBS). The Two Rate Three Color Marker (trTCM) is based on the token bucket filter and identifies packets by comparing them to the Committed Information Rate (CIR) and the Peak Information Rate (PIR).
Committed Rate	Specify the committed rate. When the incoming traffic rate of the member QoS classes is less than the committed rate, the device applies the conforming action to the traffic.

Table 54 Policer Setup: Add/Edit

LABEL	DESCRIPTION
Committed Burst Size	Specify the committed burst size for packet bursts. This must be equal to or less than the peak burst size (two rate three color) or excess burst size (single rate three color) if it is also configured. This is the maximum size of the (first) token bucket in a traffic metering algorithm.
Excess Burst Size	Specify the additional amount of bytes that are admitted at the committed rate besides the committed burst size. This is the maximum size of the second token bucket in the srTCM. This field is only available when you select Single Rate Three Color in the Meter Type field.
Peak Rate	Specify the maximum rate at which packets are admitted to the network. The peak rate should be greater than or equal to the committed rate. This is to specify how many bytes of tokens are added to the second bucket every second in the trTCM. This field is only available when you select Two Rate Three Color in the Meter Type field.
Peak Burst Size	Specify the maximum amount of bytes that are admitted at the committed rate. This is the maximum size of the second token bucket in the trTCM. This field is only available when you select Two Rate Three Color in the Meter Type field.
Conforming Action	Specify what the Zyxel Device does for packets within the committed rate and burst size (green-marked packets). <ul style="list-style-type: none"> • Pass: Send the packets without modification. • DSCP Mark: Change the DSCP mark value of the packets. Enter the DSCP mark value to use.
Partial Conforming Action	Specify the action that the Zyxel Device takes on yellow-marked packets. Select Pass to forward the packets. Select Drop to discard the packets. Select DSCP Mark to assign a specified DSCP number (between 0 and 63) to the packets and forward them. The packets are dropped if there is congestion on the network. This field is only available when you select Single/Two Rate Three Color in the Meter Type field.
Non-Conforming Action	Specify what the Zyxel Device does for packets that exceed the excess burst size or peak rate and burst size (red-marked packets). <ul style="list-style-type: none"> • Drop: Discard the packets. • DSCP Mark: Change the DSCP mark value of the packets. Enter the DSCP mark value to use. The packets may be dropped if there is congestion on the network.
Available Class	Select a QoS classifier to apply this QoS policer to traffic that matches the QoS classifier.
Selected Class	Highlight a QoS classifier in the Available Class box and use the > button to move it to the Selected Class box. To remove a QoS classifier from the Selected Class box, select it and use the < button.
Cancel	Click Cancel to exit this screen without saving any changes.
OK	Click OK to save your changes.

10.8 QoS Monitor

To view the Zyxel Device's QoS packet statistics, click **Network Setting > QoS > Monitor**. The screen appears as shown.

Figure 95 Network Setting > QoS > Monitor

Monitor shows the statistics of QoS on WAN/LAN interface and the status of Queue setup.

Refresh Interval:

Interface Monitor

#	Name	Pass Rate(bps)	Drop Rate (bps)
1	WAN	0	0
2	LAN	0	0

Queue Monitor

#	Name	Pass Rate(bps)	Drop Rate (bps)
---	------	----------------	-----------------

The following table describes the labels in this screen.

Table 55 Network Setting > QoS > Monitor

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the Zyxel Device to update this screen. Select None to stop refreshing statistics.
Interface Monitor	
#	This is the index number of the entry.
Name	This shows the name of the interface on the Zyxel Device.
Pass Rate (bps)	This shows how many packets forwarded to this interface are transmitted successfully.
Drop Rate (bps)	This shows how many packets forwarded to this interface are dropped.
Queue Monitor	
#	This is the index number of the entry.
Name	This shows the name of the queue.
Pass Rate (bps)	This shows how many packets assigned to this queue are transmitted successfully.
Drop Rate (bps)	This shows how many packets assigned to this queue are dropped.

10.9 Technical Reference

The following section contains additional technical information about the Zyxel Device features described in this chapter.

IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 56 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

DiffServ

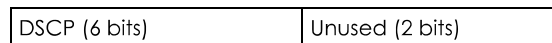
QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new Differentiated Services (DS) field to replace the Type of Service (ToS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.



The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There

are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

Automatic Priority Queue Assignment

If you enable QoS on the Zyxel Device, the Zyxel Device can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the Zyxel Device. On the Zyxel Device, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 57 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000	
		7	111000	

Token Bucket

The token bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. The bucket stores tokens, each of which represents one byte. The algorithm allows bursts of up to b bytes which is also the bucket size, so the bucket can hold up to b tokens. Tokens are generated and added into the bucket at a constant rate. The following shows how tokens work with packets:

- A packet can be transmitted if the number of tokens in the bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the bucket.
- If there are no tokens in the bucket, the Zyxel Device stops transmitting until enough tokens are generated.
- If not enough tokens are available, the Zyxel Device treats the packet in either one of the following ways:

In traffic shaping:

- Holds it in the queue until enough tokens are available in the bucket.

In traffic policing:

- Drops it.
- Transmits it but adds a DSCP mark. The Zyxel Device may drop these marked packets if the network is overloaded.

Configure the bucket size to be equal to or less than the amount of the bandwidth that the interface can support. It does not help if you set it to a bucket size over the interface's capability. The smaller the bucket size, the lower the data transmission rate and that may cause outgoing packets to be dropped. A larger transmission rate requires a big bucket size. For example, use a bucket size of 10 kbytes to get the transmission rate up to 10 Mbps.

Single Rate Three Color Marker

The Single Rate Three Color Marker (srTCM, defined in RFC 2697) is a type of traffic policing that identifies packets by comparing them to one user-defined rate, the Committed Information Rate (CIR), and two burst sizes: the Committed Burst Size (CBS) and Excess Burst Size (EBS).

The srTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The srTCM is based on the token bucket filter and has two token buckets (CBS and EBS). Tokens are generated and added into the bucket at a constant rate, called Committed Information Rate (CIR). When the first bucket (CBS) is full, new tokens overflow into the second bucket (EBS).

All packets are evaluated against the CBS. If a packet does not exceed the CBS it is marked green. Otherwise it is evaluated against the EBS. If it is below the EBS then it is marked yellow. If it exceeds the EBS then it is marked red.

The following shows how tokens work with incoming packets in srTCM:

- A packet arrives. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes).

- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the CBS bucket.
- If there are not enough tokens in the CBS bucket, the Zyxel Device checks the EBS bucket. The packet is marked yellow if there are sufficient tokens in the EBS bucket. Otherwise, the packet is marked red. No tokens are removed if the packet is dropped.

Two Rate Three Color Marker

The Two Rate Three Color Marker (trTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

The trTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The trTCM is based on the token bucket filter and has two token buckets (Committed Burst Size (CBS) and Peak Burst Size (PBS)). Tokens are generated and added into the two buckets at the CIR and PIR respectively.

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

The following shows how tokens work with incoming packets in trTCM:

- A packet arrives. If the number of tokens in the PBS bucket is less than the size of the packet (in bytes), the packet is marked red and may be dropped regardless of the CBS bucket. No tokens are removed if the packet is dropped.
- If the PBS bucket has enough tokens, the Zyxel Device checks the CBS bucket. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes). Otherwise, the packet is marked yellow.

CHAPTER 11

Network Address Translation (NAT)

11.1 NAT Overview

This chapter discusses how to configure NAT on the Zyxel Device. NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet; for example, the source address of an outgoing packet, used within one network, to a different IP address known within another network.

11.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network ([Section 11.2 on page 169](#)).
- Use the **Port Triggering** screen to add and configure the Zyxel Device's trigger port settings ([Section 11.3 on page 173](#)).
- Use the **DMZ** screen to configure a default server ([Section 11.4 on page 176](#)).
- Use the **ALG** screen to enable and disable the ALGs in the Zyxel Device ([Section 11.5 on page 177](#)).
- Use the **Address Mapping** screen to configure the Zyxel Device's address mapping settings ([Section 11.6 on page 178](#)).
- Use the **Sessions** screen to configure the Zyxel Device's maximum number of NAT sessions ([Section 11.6 on page 178](#)).

11.1.2 What You Need To Know

Inside/Outside

Inside/outside denotes where a host is located relative to the Zyxel Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/Local

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN

side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

Finding Out More

See [Section 11.8 on page 181](#) for advanced technical information on NAT.

11.2 Port Forwarding

Use **Port Forwarding** to forward incoming service requests from the Internet to the server(s) on your local network. Port forwarding is commonly used when you want to host online gaming, P2P file sharing, or other servers on your network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

The most often used port numbers and services are shown in [Appendix C on page 298](#). Please refer to RFC 1700 for further information about port numbers.

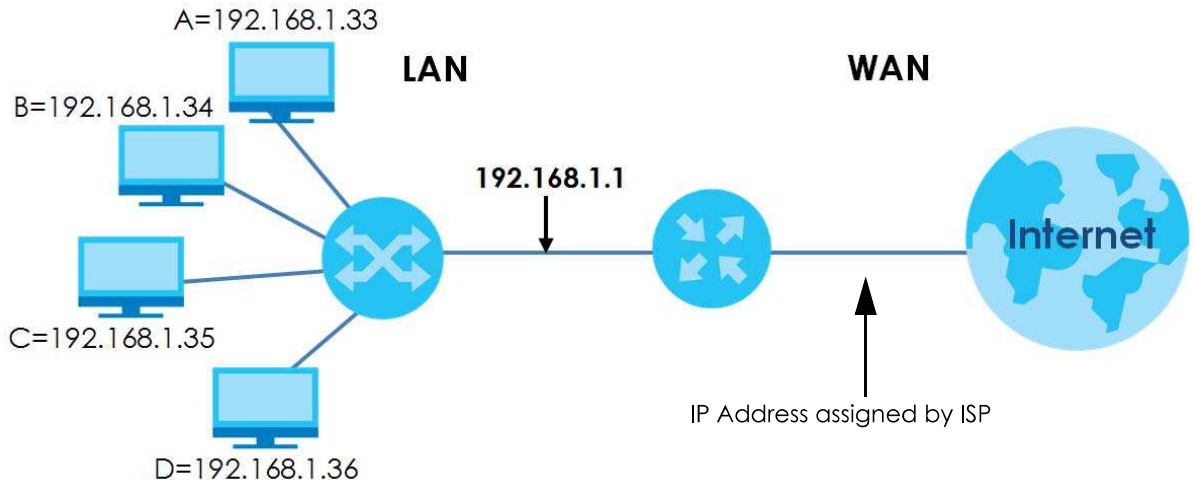
Note: TCP port 7547 is reserved for system use.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 96 Multiple Servers Behind NAT Example



Click **Network Setting > NAT > Port Forwarding** to open the following screen.

Figure 97 Network Setting > NAT > Port Forwarding

Port Forwarding is commonly used when you want to use Internet activities such as, online gaming, P2P file sharing or even hosting servers on your network. It creates a bridge to allow another party from the internet, to contact a specific LAN client on your network correctly.

+ Add New Rule

#	Status	Service Name	Originating IP	WAN Interface	Server IP Address	Start Port	End Port	Translation Start Port	Translation End Port	Protocol	Modify
Note											
The TCP port 7547 is reserved for system usage.											

The following table describes the fields in this screen.

Table 58 Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
Add New Rule	Click this to add a new rule.
#	This is the index number of the entry.
Status	This field displays whether the NAT rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This shows the service's name.
Originating IP	This field displays the source IP address from the WAN interface.
WAN Interface	This shows the WAN interface through which the service is forwarded.
Server IP Address	This is the server's IP address.
Start Port	This is the first external port number that identifies a service.
End Port	This is the last external port number that identifies a service.
Translation Start Port	This is the first internal port number that identifies a service.

Table 58 Network Setting > NAT > Port Forwarding (continued)

LABEL	DESCRIPTION
Translation End Port	This is the last internal port number that identifies a service.
Protocol	This shows the IP protocol supported by this virtual server, whether it is TCP , UDP , or TCP/UDP .
Modify	Click the Edit icon to edit this rule. Click the Delete icon to delete an existing rule.

11.2.1 Add/Edit Port Forwarding

Click **Add New Rule** in the **Port Forwarding** screen or click the **Edit** icon next to an existing rule to open the following screen. Specify either a port or a range of ports, a server IP address, and a protocol to configure a port forwarding rule.

Note: To configure port forwarding, you need to have the same configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.

Note: To configure port translation, you need to have different configurations in the **Start Port**, **End Port**, **Translation Start Port**, and **Translation End Port** fields.

Note: TCP port 7547 is reserved for system use.

Figure 98 Port Forwarding: Add/Edit

Add New Rule

Active:

Service Name:

Obtain WAN IP Automatically: Enable (Auto Detect Default WAN IP/Interface)

WAN IP:

WAN Interface:

Start Port:

End Port:

Translation Start Port:

Translation End Port:

Server IP Address:

Configure Originating IP: Enable

Originating IP:

Protocol:

Note

- If Start Port and Translation Start Port, End Port and Translation End Port is configured the same, then Port Forwarding is configured.
If Start Port and Translation Start Port, End Port and Translation End Port are configured differently, then Port Translation is configured (one to one mapping).
For example: Start Port: 100 End Port: 120; Translation Start Port: 200 Translation End Port: 220
- Originating IP is optional. User must enable Configure Originating IP to add a source IP address which from the WAN Interface.
- The TCP port 7547 is reserved for system usage.

Cancel **OK**

The following table describes the labels in this screen.

Table 59 Port Forwarding: Add/Edit

LABEL	DESCRIPTION
Active	Click this switch to enable or disable the rule. When the switch goes to the right <input checked="" type="checkbox"/> , the function is enabled. Otherwise, it is not.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
Obtain WAN IP Automatically	Select the Enable check box to have the Zyxel Device automatically detect and use an available WAN interface for port forwarding.
WAN IP	Enter your WAN IP address in this field if you did not select Obtain WAN IP Automatically .

Table 59 Port Forwarding: Add/Edit (continued)

LABEL	DESCRIPTION
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled. Note: This field is not available if you select Obtain WAN IP Automatically .
Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the End Port field. To forward a series of ports, enter the start port number here and the end port number in the End Port field.
End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the Start Port field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the Start Port field above.
Translation Start Port	This shows the port number to which you want the Zyxel Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Configure Originating IP	Select Enable to enter the source IP address of WAN interface.
Originating IP	Enter the source IP address of WAN interface.
Protocol	Select the protocol supported by this virtual server. Choices are TCP , UDP , or TCP/UDP .
Cancel	Click Cancel to exit this screen without saving any changes.
OK	Click OK to save your changes.

11.3 Port Triggering

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding, you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding addresses this problem. Trigger port forwarding allows computers on the LAN to dynamically take turns using the service. The Zyxel Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the Zyxel Device's WAN port receives a response with a specific port number and protocol ("open" port), the Zyxel Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

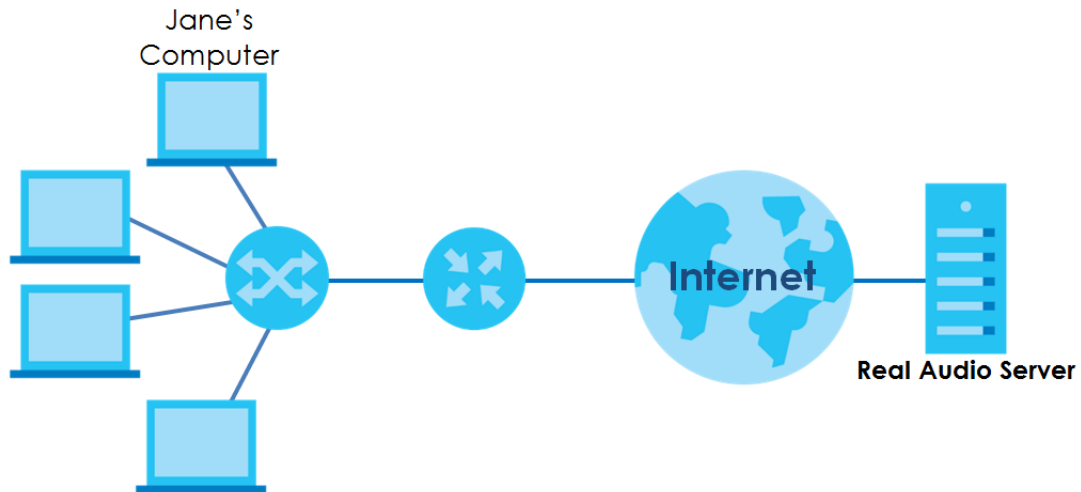
Note: TCP port 7547 is reserved for system use.

Note: The maximum number of trigger ports for a single rule or all rules is 999.

Note: The maximum number of open ports for a single rule or all rules is 999.

For example:

Figure 99 Trigger Port Forwarding Process: Example





- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the Zyxel Device to record Jane's computer IP address. The Zyxel Device associates Jane's computer IP address with the "open" port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.
- 4 The Zyxel Device forwards the traffic to Jane's computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The Zyxel Device times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **Network Setting > NAT > Port Triggering** to open the following screen. Use this screen to view your Zyxel Device's trigger port settings.

Figure 100 Network Setting > NAT > Port Triggering

Port Triggering is a way to automate port forwarding with a little better security. It dynamically forwards connection or data to whatever LAN client made a certain outgoing connection. Example: You define port 25 as Trigger Port and port 113 as Open Port. If any of the LAN devices on your network creates an outgoing connection via port 25, all incoming connections via port 113 will temporarily go to that client.

 Add New Rule

#	Status	Service Name	WAN Interface	Trigger Start Port	Trigger End Port	Trigger Proto.	Open Start Port	Open End Port	Open Protocol	Modify
<p> Note</p> <p>(1) The sum of trigger ports in all rules must be less than 1000 and every open port range must be less than 1000. When the protocol is TCP/UDP, the ports are counted twice.</p> <p>(2) The TCP port 7547 is reserved for system usage.</p>										

The following table describes the labels in this screen.

Table 60 Network Setting > NAT > Port Triggering

LABEL	DESCRIPTION
Add New Rule	Click this to create a new rule.
#	This is the index number of the entry.
Status	This field displays whether the port triggering rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This field displays the name of the service used by this rule.
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the Zyxel Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. This is the first port number that identifies a service.
Trigger End Port	This is the last port number that identifies a service.
Trigger Proto.	This is the trigger transport layer protocol.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Zyxel Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. This is the first port number that identifies a service.
Open End Port	This is the last port number that identifies a service.
Open Proto.	This is the open transport layer protocol.
Modify	Click the Edit icon to edit this rule. Click the Delete icon to delete an existing rule.

11.3.1 Add/Edit Port Triggering Rule

This screen lets you create new port triggering rules. Click **Add new rule** in the **Port Triggering** screen or click a rule's **Edit** icon to open the following screen. Use this screen to configure a port or range of ports and protocols for sending out requests and for receiving responses.

Figure 101 Port Triggering: Add/Edit

The following table describes the labels in this screen.

Table 61 Port Triggering: Configuration Add/Edit

LABEL	DESCRIPTION
Active	Select Enable or Disable to activate or deactivate the rule.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the Zyxel Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers.
Trigger End Port	Type a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the transport layer protocol from TCP , UDP , or TCP/UDP .
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Zyxel Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Type a port number or the starting port number in a range of port numbers.
Open End Port	Type a port number or the ending port number in a range of port numbers.
Open Protocol	Select the transport layer protocol from TCP , UDP , or TCP/UDP .
Cancel	Click Cancel to exit this screen without saving any changes.
OK	Click OK to save your changes.

11.4 DMZ Settings

A client in the Demilitarized Zone (DMZ) is no longer behind the Zyxel Device and therefore can run any Internet applications such as video conferencing and Internet gaming without restrictions. This, however, may pose a security threat to the Zyxel Device.