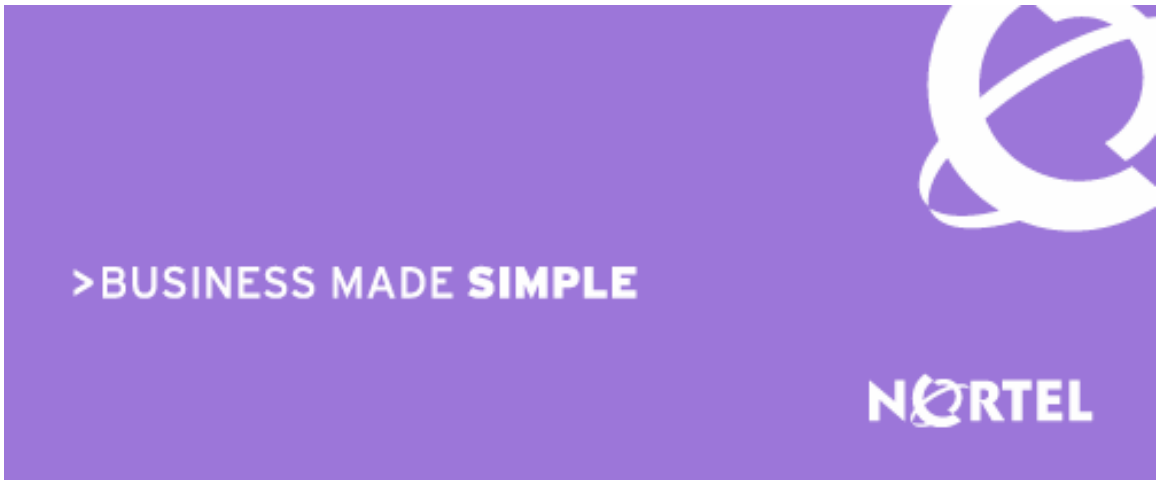

Ethernet Routing Switch 5510/5520/5530
Engineering

> Filters and QOS Configuration for Ethernet Routing Switch 5500 Technical Configuration Guide

Enterprise Solutions Engineering
Document Date: April 01, 2008
Document Number: NN48500-559
Document Version: 2.0

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband, Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at www.nortel.com.

Abstract

This technical configuration guide provides an overview on how to configure QoS and Filters on the Ethernet Routing Switch 5500 with software release 5.1. The configuration examples are all in reference to the Nortel Networks Command Line Interface (NNCLI).

Table of Contents

DOCUMENT UPDATES **5**

CONVENTIONS **5**

1. OVERVIEW: ETHERNET ROUTING SWITCH 5500 QOS AND FILTERING **6**

2. QOS FLOW CHART **9**

3. FILTER FUNCTIONALITY **10**

3.1 OVERALL CLASSIFICATION FUNCTIONALITY 10
3.2 CLASSIFIER BLOCK FUNCTIONALITY 10
3.3 PORT RANGE FUNCTIONALITY 11
3.4 POLICIES 12

4. QUEUE SETS **14**

5. TRAFFIC METER AND SHAPING **19**

5.1 ACTUAL BUCKET SIZE 20
5.2 POLICING TRAFFIC 20
5.3 INTERFACE SHAPER 22

6. DEFAULT NORTEL CLASS OF SERVICE **24**

7. QOS ACCESS LISTS (ACL) **25**

7.1 ACL CONFIGURATION 25

8. IP SECURITY FEATURES **30**

8.1 DHCP SNOOPING 30
8.2 DYNAMIC ARP INSPECTION 30
8.3 IP SOURCE GUARD 31

9. BPDU FILTERING **32**

9.1 BPDU FILTERING CONFIGURATION 32

10. QOS INTERFACE APPLICATIONS **33**

10.1 ARP SPOOFING 34
10.2 DHCP ATTACKS 35
10.3 DOS 36
10.4 BPDU BLOCKING 37

11. CONFIGURATION STEPS – POLICY CONFIGURATION **38**

11.1 ROLE COMBINATION 38
11.2 CLASSIFICATION 39
11.3 METERS 41
11.4 ADD A NEW POLICY 42

12. CONFIGURATION EXAMPLES **43**

12.1 PRE-DEFINED VALUES 43
12.2 CONFIGURATION EXAMPLE 1 – TRAFFIC METER USING POLICIES 44
12.3 CONFIGURATION EXAMPLE – IP ACL, DHCP SNOOPING, ARP INSPECTION, BPDU FILTERING, AND SOURCE GUARD 50
12.4 CONFIGURATION EXAMPLE 3: PORT RANGE USING ACL OR POLICY 59
12.5 CONFIGURATION EXAMPLE 4 – L2 CLASSIFICATION BASED ON MAC ADDRESS 62
12.6 CONFIGURATION EXAMPLE 5 – L2 AND L3 CLASSIFICATION 64

12.7 CONFIGURATION EXAMPLE 6 - QOS MARKING WITH PORT ROLE COMBINATION SET FOR UN-RESTRICTED USING ACL'S 66
12.8 CONFIGURATION EXAMPLE 7 – INTERFACE SHAPING 69
13. SOFTWARE BASELINE 70
14. REFERENCE DOCUMENTATION 70

List of Figures

Figure 1: QoS System Diagram 6
Figure 2: QoS Flow Chart 9
Figure 3: Arp Spoofing Example 34
Figure 4: IP ACL, DHCP Snooping, ARP Inspection, and Source Guard 50
Figure 5: L2 Classification Based on MAC Address Example 62
Figure 6: DSCP Mapping via Un-restricted Port Role 66

List of Tables

Table 1: Default QoS Action 7
Table 2: Example of Valid Port Ranges 11
Table 3: Default Policy Drop Action 12
Table 4: Ethernet Routing Switch 5500 Resource Sharing 14
Table 5: Ethernet Routing Switch 5500 Egress CoS Queuing 15
Table 6: Meter and Shaping Range and Granularity 19
Table 7: Actual Bucket Size in Bytes 20
Table 8: Meter Bucket Size and Duration 22
Table 9: Default Nortel CoS Markings 24
Table 10: QoS Applications – Number of Classifiers Used 33

Document Updates

Added ACL, DHCP Snooping, APP Inspection, BPDU Filtering and IP Source Guard.

Conventions

This section describes the text, image, and command conventions used in this document.

Symbols:

Tip – Highlights a configuration or technical tip.

Note – Highlights important information to the reader.

Warning – Highlights important information about an action that may result in equipment damage, configuration or data loss.

Text:

Bold text indicates emphasis.

Italic text in a Courier New font indicates text the user must enter or select in a menu item, button or command:

ERS5520-48T# ***show running-config***

Output examples from Nortel devices are displayed in a Lucinda Console font:

ERS5520-48T# ***show running-config***

```
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 5520-24T-PWR
! Software version = v5.0.0.011
enable
configure terminal
```

1. Overview: Ethernet Routing Switch 5500 QoS and Filtering

The Ethernet Routing Switch 5500 supports QoS and filter configuration via WEB, CLI, and Device Manager with no support for COPS at this time. As shown in the diagram below, the following functional components provide QoS support on the Ethernet Routing Switch 5500:

- Role Combination on the ingress port
- Classify traffic at either Layer 2 or at a Layer 3/4 level
- Take action by dropping, marking, redirecting, or metering (policing) traffic
- Send traffic to appropriate egress queue

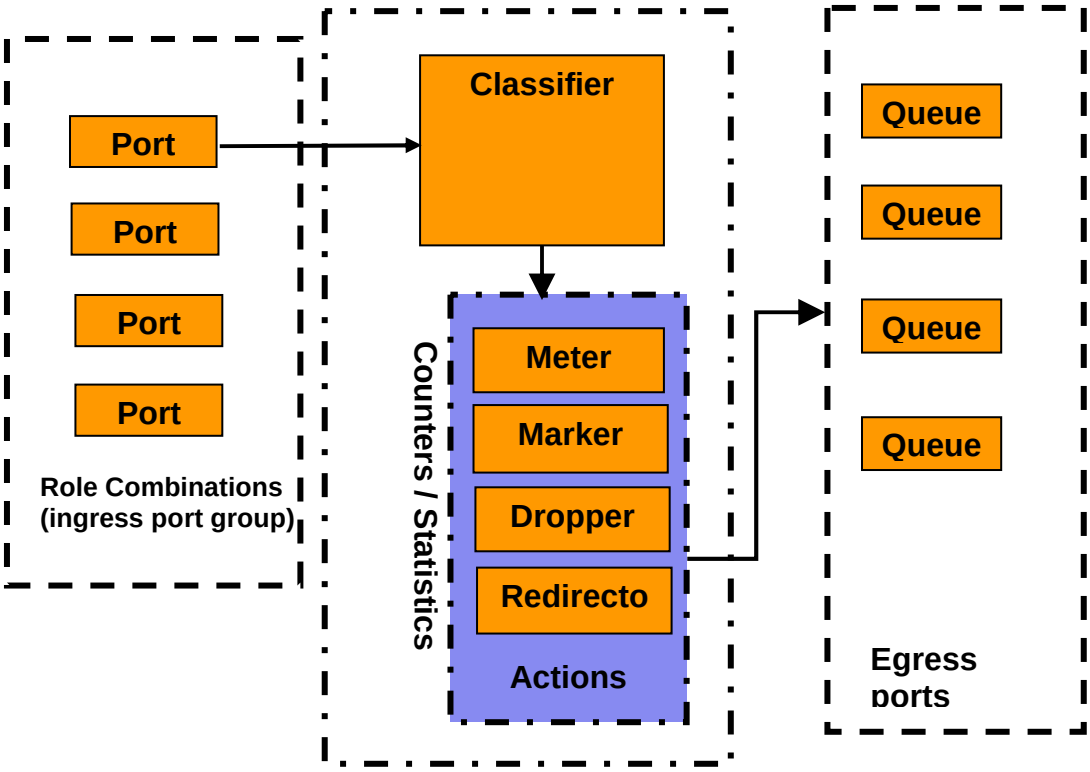

Figure 1: QoS System Diagram

Role Combination

A role combination is a grouping of one or more ports, capabilities, and interface classifications against which a policy is applied. The capabilities presently supported on the Ethernet Routing Switch 5500 include ingress IP and Layer 2 classification. The Ethernet Routing Switch 5500 supports the following interface classes that can be applied to zero, one, or many interfaces:

- **Trusted Ports**
  - Assumes that all traffic coming into the port is originating from a trusted source. Therefore, the DSCP field of any traffic that enters the Ethernet Routing Switch 5500 from a Trusted Port is not remarked by default. However, a policy can still be applied to a trusted port to remark if required. Note that only the 802.1p user priority value associated with 'well-known' DSCP values are remapped by the default trusted

polices. The 'well-know' DSCP values can be viewed by using the NNCLI command 'show qos eqressmap'.

- **Untrusted Ports**
  - Assumes that all traffic coming into the port is suspect. Therefore, the DSCP field of any traffic that enters the Ethernet Routing Switch 5500 from an Untrusted Port is re-marked. For untagged packets, the default classifier is used to change the DSCP. This results in a DSCP value determined by the CoS-to-DSCP mapping table using the default 802.1p priority of the interface where the packet is received. For tagged packets, the 802.1p value is determined by CoS-to-DSCP mapping table using the best effort DSCP, which is 0.

- **Unrestricted Ports**
  - Does not assume anything about the origin of the incoming traffic. You may assign an action to set the DSCP or not to set the DSCP; it's up to you. This allows you to manipulate the DSCP value based upon the filter criteria, and not upon the point of origin.

The following table displays a summary of the role combination capabilities.

Table 1: Default QoS Action

Type of Filter	Action	Trusted	Untrusted	Unrestricted
IPv4 filter criteria or Layer 2 filter criteria matching IPv4	DSCP	Does not change	• Tagged--Updates to 0 (Standard) • Untagged--Updates using mapping table and port's default value	Does not change
	IEEE 802.1p	Updates based on DSCP mapping table value	Updates based on DSCP mapping table value	Does not change

Classification

Classification identifies the traffic flow that requires QoS management. The traffic flow may be identified by the Layer 2 or IP content of the frame using any of the elements shown below.

- **Layer 2 Classifier Elements**
  - Source MAC with mask to filter on complete or partial MAC addresses
  - Destination MAC with mask to filter on complete or partial MAC addresses
  - VLAN ID – can be a range
  - Tagged or untagged packets
  - EtherType
  - 802.1p priority

- **IP Classifier Elements**
  - Source IPv4/v6 host or subnet

- Destination IPv4/v6 host or subnet
- IPv4/v6 DSCP value
- IPv4 Protocol type, IPv6 next-header
- IPv4/v6 Layer 4 (UDP/TCP) Source port – can be range of ports
- IPv4/v6 Layer 4 (UDP/TCP) Destination port – can be range of ports
- IPv6 flow identifier

A classifier can contain one Layer 2 element, one IP element, or one Layer 2 and one IP element. One or more classifiers can be combined to create a classifier block where up to 15 classifiers and/or classifier blocks can be assigned to a port. By using classifier blocks, the number of classifiers can be increased up to a total of 114 classifiers per port on the Ethernet Routing Switch 5500 for a total of over 40K in a stack. In addition, statistic counters can be used to match/in-profile and out-of-profile statistics with meter. Up to 32 match/in-profile counters and 63 out-of-profile counters (one per meter) are supported per interface.

Actions Supported

After matching a certain classification criteria, various actions can be initiated.

- In-profile actions (metered traffic within specific bandwidth limits)
  - Drop
  - Update DSCP
  - Update 802.1p
  - Drop precedence choice of low-drop, high-drop or use egress map
- Out-of-profile actions (metered traffic exceeding bandwidth limits)
  - Drop
  - Update DSCP
  - Set drop precedence
- Non-Match actions (non-metered traffic)
  - Drop
  - Update DSCP
  - Update 802.1p
  - Drop precedence choice of low-drop or high-drop

Metering data includes in-profile and out-of-profile actions with metered bandwidth allocated per port. Each meter has its own token bucket that controls the rate at which packets are accepted for processing at ingress. The committed information rate (CIR) and bucket sizes are as follows:

- Committed rate from 1 Mbps to 1 Gbps in 1 Mbps increments, 64K to 1 Gbps in 64K for ERS5530 only with 10/100/1000 Mbps interfaces – please see table 6 below for details
- Token bucket sizes in bytes: 16K, 20K, 32K, 44K, 76K, 140K, 268K, 512K where one byte is sent for each token
- Up to 63 counters are available per port

Statistics

The Ethernet Routing Switch 5500 supports tracking of statistics (packet counters) for the policies defined. The switch can be set-up for one counter for each classifier or a counter for all classifiers associated with a policy up to 63 counters are available per port. The statistics track match/in-profile and out-of-profile statistics associated with a meter.

2. QoS Flow Chart

The following flowchart displays the various steps required in setting up a QoS policy. You basically now need to create a Classifier with each Classifier made up of one IP Classifier Element, or one L2 Classifier Element or one IP and one L2 Classifier Element. You then add the Classifier to a separate Policy on a per port basis. Or you can group a number of Classifiers into a Classifier Block and then add the Classifier Block to a Policy on a per port basis. The Ethernet Routing Switch 5500 supports up to 114 Classifiers per port for a total of greater than 40K Classifiers in a fully configured stack.

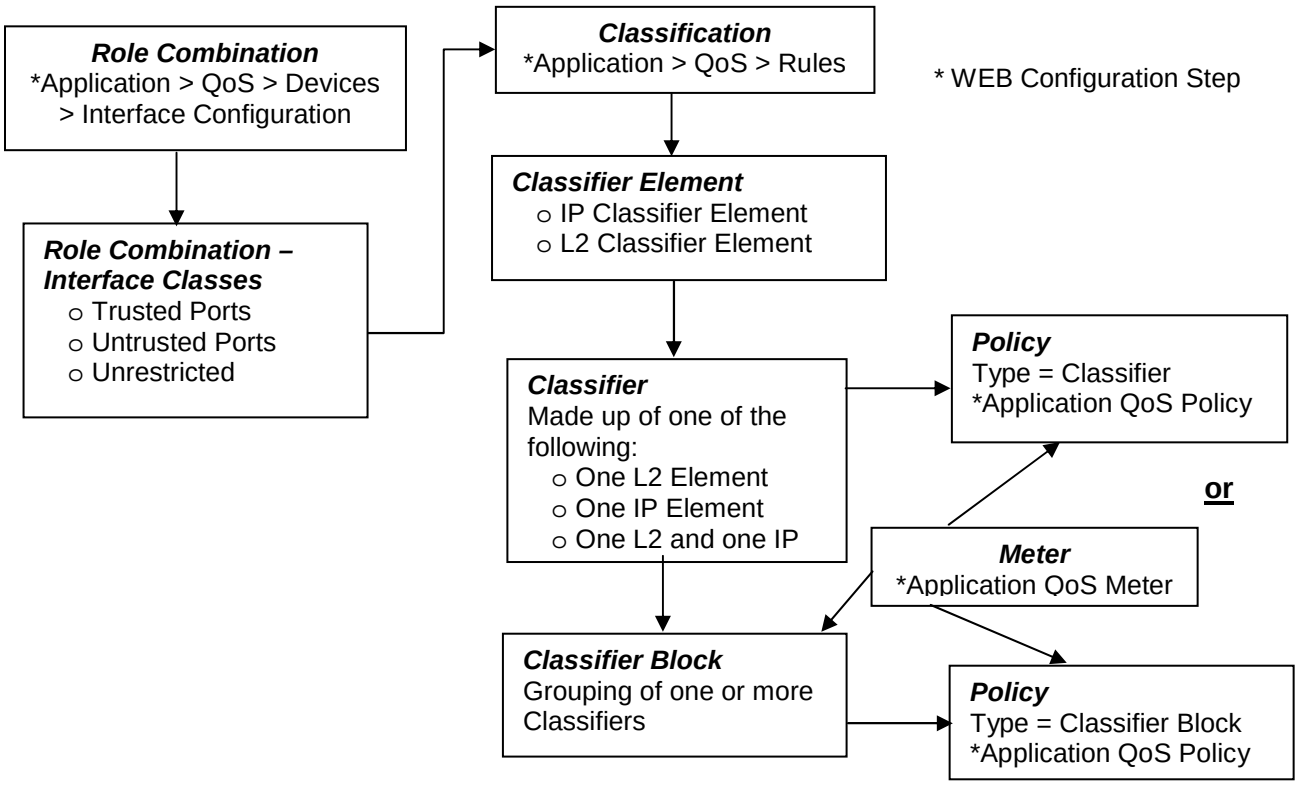

Figure 2: QoS Flow Chart

3. Filter Functionality

3.1 Overall Classification Functionality

Classification with the Ethernet Routing Switch 5500 has some fundamental classification limitations, imposed by hardware, that affect classification overall. The foremost limitation is related to the concept, introduced by the latest classification hardware and the supporting data model, of “classification masks”. A classification mask specifies the fields within a frame that will be used for matching purposes. The mask itself does not specify the data to be matched but rather indicates which fields, or portions thereof, in the various protocol headers (e.g., MAC, IPv4, IPv6 headers) will be examined during the classification process. Currently, a maximum of 15 classification masks and 114 classifiers are available per port for user-defined traffic classification. This effectively means that 15 or fewer unique combinations of classification criteria (i.e., Layer 2, 3 and 4 data) can be specified per port. However, multiple data sets can leverage the same classification mask. This means that, as long as the same protocol data fields are being matched (e.g., IPv4 source address, IPv6 flow label, Layer 2 802.1p User Priority and VLAN Id), a much larger number of classifiers, up to a maximum of 114 per port, can be defined containing unique data values for matching against the fields/offsets identified by the classification mask.

3.2 Classifier Block Functionality

A user should take care when grouping a large number of individual classifiers into a classifier block. Grouping is a quick way to inadvertently exhaust limited resources. For example, a limited number of counters are available per interface for tracking matching/in-profile packets. Associating a block of classifiers with a policy indicating that statistics are to be maintained could consume all counting resources for a single interface with one policy. To avoid exhausting the number of counters available per interface, one may select "aggregate classifier tracking" instead of "individual classifier tracking" when creating the policy. By specifying "aggregate classifier tracking", a single counter resource is used to track statistics for all the classifiers of that policy, rather than a single counter resource per classifier. The obvious downside to this is the inability to track the statistics down to the granularity of each of the classifiers associated with the policy. Individual attribute limitations include:

- Individual classifier identification – a classifier set must exist prior to being referenced by the Classifier-Block.
- Individual classifier data compatibility – a classifier is eventually broken down into a bitmask identifying fields in a packet header that are of interest and values to be matched against those fields. Classifiers within a block must match the same protocol header fields, or portions thereof. For example, all classifiers in a block must match against an IPv4 source host address, an IPv4 source subnet with the same number of significant bits or the Layer 2 EtherType field in a tagged packet. A classifier matching against an IPv4 source host address and another matching against an IPv4 destination host address may not be members of the same block as these classifiers do not share a common classification mask. The values to be matched against may differ but the fields being matched may not.

Referenced component consistency – all the elements that comprise a block (i.e., all classifier blocks with the same block number) must either reference an action or a meter component or none of the elements are permitted to reference an action or a meter. In other words, all block members must specify the same type of information, be it action criteria, metering criteria or neither. The referenced action or metering elements may differ across block members but all members must reference individual actions or meters (but not actions and meters) if any do.

Filter example:

a) IP Classifier #1: src IP = 10.1.1.0/24

b) IP Classifier #2: src IP = 10.20.0.0/16

c) IP Classifier #3: src IP = 172.1.1.0/24

d) IP Classifier #4: src IP = 10.22.0.0/16

e) IP Classifier #5: src IP = 10.1.2.0/24, dst IP = 192.1.1.0/24

f) IP Classifier #6: src = 10.1.10.0/24

Classifiers a, c and f can be combined to create a classifier block if you wish to filter on these addresses on a port(s). Classifiers b and d can be combined to create a second classifier block if you wish to filter on these addresses on a port(s).

3.3 Port Range Functionality

The Ethernet Routing Switch 5500 has the ability to specify a range of values supported by the QoS data model for several classification components (e.g., Layer 4 source and destination port numbers, VLAN Id values). Range support is limited to a certain extent, however, because ranges are represented as a bitmask within the overall classification mask, and not with explicit minimum and maximum values. A range must thus be specified by indicating which bits in the given field (e.g., Layer 4 source port) are 'ignored' (i.e., set to 0). Taking into account this limitation, the following rules are used to determine valid range values:

I. Minimum value: n

   Maximum value: n

   >> Example: min: 20 max: 20 (min = max equates to a range of 1)

II. Minimum value: 0

   Maximum value: (2^n) – 1

   >> Example: min: 0 max: 63 (n = 6)

III. Minimum value: even number

   Maximum value: minimum port number in binary with rightmost consecutive 0's replaced with 1's using the formula: Port Maximum = ((Port minimum + 2^n) -1)) where n equal number of consecutive trailing zero's.

   >> Example: min: 128 max: 255 ((128 + 2^7) – 1 = 255; 128 in binary has 7 consecutive trailing zero's)

   Specified ranges that do not adhere to one of these three rules cannot be supported and will be flagged as erroneous.

The following table shows some examples of valid port ranges supported on the Ethernet Routing Switch 5500.

Table 2: Example of Valid Port Ranges

Minimum Value (must be even number)	Maximum Value	Binary Value
0	1, 3, 7, 15, 31, 63, 127, 255, 511, 1025, 2047, 4095, 8191, 16355, 32762, or 65535	
2	3	Min = 10

		Max = 11
4	7	Min = 100 Max = 111
8	15	Min = 1000 Max = 1111
80	95	Min = 10100000 Max = 10111111

3.4 Policies

- Packets received on an interface are matched against all policies associated with that interface. Hence, all policies are applied to the packet.
- Policy precedence – the precedence attribute is used to specify the evaluation order of policies that apply to the same interfaces. Policies with higher precedence (i.e., a larger value) are applied before those with lower precedence (i.e., a smaller value). Precedence values must be unique for all policies being applied to the same interface role.
- If one policy associated with the specific interface only specifies a value updating the DSCP value while another policy associated with that same interface only specifies a value for updating the 802.1p user priority value, both of these actions occur.
- If two policies on the specified interface request that the DSCP be updated but specify different values - the value from the policy with the higher precedence will be used.
- Referenced component conflicts - action or meter criteria can be specified through individual classifier blocks. When a policy references a classifier block and members of the referenced block identify their own action or meter criteria, action and meter data must not be specified by the policy.
- The actions applied to packets include those actions defined from user-defined policies and those actions defined from system default policies. The user-defined actions always carry a higher precedence than the system default actions. This means that, if user-defined policies do not specify actions that overlap with the actions associated with system default policies (for example, the DSCP and 802.1p update actions installed on untrusted interfaces), the lowest precedence, default policy actions will be included in the set of actions to be applied to the identified traffic.
- The following table displays the ERS 5500 default policy action with corresponding drop actions. The drop action specifies whether a packet should be dropped, not dropped, or deferred. A drop action of deferred-Pass specifies that a traffic flow decision will be deferred to other installed policies.

Table 3: Default Policy Drop Action

ID	Name	Drop	Update DSCP	User Priority	Drop Precedence
1	Drop_Traffic	drop	Ignore	Ignore	highDropPrec
2	Standard_Service	Don't Drop	0x00	Priority 0	highDropPrec
3	Bronze_Service	Don't Drop	0x0a	Priority 2	lowDropPrec
4	Silver_Service	Don't Drop	0x12	Priority 3	lowDropPrec
5	Gold_Service	Don't Drop	0x1a	Priority 4	lowDropPrec
6	Platinum_Service	Don't Drop	0x22	Priority 5	lowDropPrec
7	Premium_Service	Don't Drop	0x2e	Priority 6	lowDropPrec
8	Network_Service	Don't Drop	0x30	Priority 7	lowDropPrec
9	Null_Service	Don't Drop	ignore	ignore	lowDropPrec

When setting up multiple policies using any of the default policy actions ID's 2 to 9 (i.e. Standard_Service, Bronze_Service, etc) a lower precedence policy with a drop action, (i.e. Drop_Traffic), the Drop_Traffic action will effect the higher precedence policies. The end result is all the higher precedence policies will also be dropped. The reason for this is each of the default actions, with the exception of Drop_Traffic, uses a drop action of *deferred-Pass*. A drop action of *deferred-Pass* specifies that a traffic flow decision will be deferred to other installed policies.

To make a policy behave somewhat similar to stop-on-match, you will have to create a new action with a drop action of *dontDrop* (JDM) or *disable* (CLI).

- Statistics accumulation support – a limited number of counters are available for tracking statistics. Specifically, 32 counters are available per port for tracking matching (no metering specified) /in-profile (metering specified) traffic statistics. A total of 63 counters are available (per port) to track out-of-profile statistics, with the caveat that these counters are associated with the metering component and flows sharing the same meter on the same port use the same counter for statistics.

The valid precedence range for QoS policies is from 1 to 15. However, depending on the application enabled, the valid precedence range can change as QoS shares resources with other switch applications including DHCP Relay, MAC Security, IP Fix, IGMP, EAPOL, EAP multihost (5530-24TFD only), OSPF, IP Source Guard, and ADAC. Please use the command '*show qos diag'* to view the mask utilization per port.

In release 4.1, FCS November 2004, the system default actions (e.g. bronze, silver, gold, etc.) will be changed from *deferred-Pass* to *dontDrop*.

4. Queue Sets

Prior to software release 4.0, the Ethernet Routing Switch 5500 supported a single queue set with eight queues, one absolute queue and seven WRR queues.

With the introduction of software release 4.0, eight different queue sets where made available. Each queue set has different characteristics in regards to number of queues and service weights allowing the user to select a queue set based on the user's particular needs. With eight queue settings and three resource sharing options, the Ethernet Routing Switch 5500 supports a total of 24 different queues and buffer setting combinations. Prior to making any changes to the egress queue, the buffer resource sharing feature must be enabled.

Resource Sharing

The three (3) possible resource sharing settings in version 4.0 or greater software release are regular, large, and maximum. These settings allow the user to change the amount of buffer which can be allocated or shared to any port. Note that the switch must be rebooted if any changes are made.

Table 4: Ethernet Routing Switch 5500 Resource Sharing

Setting	Description
Regular	1 port may use up to 16% of the buffers for a group of 12 ports.
Large	1 port may use up to 33% of the buffers for a group of 12 ports.
Maximum	1 port may use 100% of the buffers for a group of 12 ports.

Resource Sharing Commands

- 5520-24T-PWR(config)# ***qos agent buffer <large | maximum | regular>***

  The qos agent buffer <regular | large | maximum > command allows the user to specify the level of resource sharing on the switch. This parameter is global and requires a reset to activate a change. This command is in the CLI priv-exec mode.

- 5520-24T-PWR(config)# ***default qos agent buffer***

  The default qos agent buffer command sets the switches agent buffer back to a default setting of regular. In order for this command to take affect, a reset of the switch must occur. This command is in the CLI priv-exec mode.

Resource Sharing Recommendations

Nortel Networks recommends you use the default resource-sharing setting of regular. If you change the setting, the resulting performance may increase for some ports, and at times, decrease for other ports.

Generally speaking, smaller buffers achieve lower latency (RTT) but reduce the throughput ability which is better for VoIP etc. and sensible jitter application.

You should use the Maximum resource sharing setting:

- If you are using your 5520 for big file transfers (like backup of servers)

- If you are using (the AppleTalk Filing Protocol) AFP, use large or maximum resource sharing (AFP use a fix windows size set to 65,535K).You should use the large resource sharing setting:
- If you are using your 5520 for high bandwidth application such as video.
- If you are using large TCP windows for your traffic, use large resource sharing (you can also reduce the TCP windows size on windows operating system - see Microsoft TechNet article 224829).
- If you have 4 or fewer ports connected per group of 12 ports.

You should use the Regular resource sharing setting:

- If you are using your 5520 in a VOIP environment.
- If you have 5 or more ports connected per group of 12 ports.

Egress CoS Queuing

The following charts describe each possible egress CoS queuing setting. The mapping of 802.1p priority to egress CoS queue, dequeuing algorithm, and queue weight is given. Additionally, the memory and maximum number of packets which can be buffered per egress CoS queue and resource sharing settings is shown.

Table 5: Ethernet Routing Switch 5500 Egress CoS Queuing

Setting	Internal Priority	Egress CoS Queue	Dequeuing Algorithm	Weight	Regular Memory/ # of 1518 Byte Packets	Large Memory/ # of 1518 Byte Packets	Max Memory/ # of 1518 Byte Packets
8 CoS	7	1	Strict	100%	36864B 24	49152B 32	131072B 86
	6	2	Weighted Round Robin	41%	36864B 24	47104B 31	123392B 81
	5	3		19%	27648B 18	45056B 29	115712B 76
	4	4		13%	18432B 12	43008B 28	108032B 71
	3	5		11%	18432B 12	39936B 26	97792B 64
	2	6		8%	18432B 12	36864B 24	85504B 56
	1	7		5%	18432B 12	33792B 22	70656B 46
	0	8		3%	18432B 12	30720B 20	54272B 35
7 CoS	7	1	Strict	100%	36864B 24	49152B 32	144640B 95
	6	2	Weighted Round Robin	45%	32768B 21	46080B 30	131840B 86
	5	3		21%	26624B 17	39936B 26	120064B 79
	4	4		15%	19968B 13	33280B 21	109824B 72

	3	5		10%	18432B	31232B	100864B
					12	20	66
	2	6		6%	18432B	31232B	92800B
					12	20	61
	1	7		3%	18432B	31232B	86400B
	0				12	20	56

6 CoS	7	1	Strict	100%	36864B	51200B	163840B
					24	33	107
	6	2	Weighted Round Robin	52%	33792B	49152B	151040B
					22	32	99
	5	3		24%	31744B	47104B	137472B
					20	31	90
	4	4		14%	26624B	43008B	124160B
					17	28	81
	3	5		7%	21504B	37376B	111360B
	2				14	24	73
	1	6		3%	18432B	34304B	98560B
	0				12	22	64

5 CoS	7	1	Strict	100%	46080B	64000B	199680B
					30	42	131
	6	2	Weighted Round Robin	58%	41984B	59904B	181760B
					27	39	119
	5	3		27%	35840B	53760B	158720B
	4				23	35	104
	3	4		11%	28160B	46080B	133120B
	2				18	30	87
	1	5		4%	19968B	38400B	113152B
	0				13	25	74

4 CoS	7	1	Strict	100%	57344B	81920B	262912B
	6				37	53	173
	5	2	Weighted Round Robin	65%	51200B	74240B	209920B
	4				33	48	138
	3	3		26%	38912B	61440B	176640B
	2				25	40	116
	1	4		9%	24576B	44544B	136960B
	0				16	29	90

3 CoS	7	1	Strict	100%	65536B	109568B	393316B
	6				43	72	259
	5	2	Weighted Round Robin	75%	57344B	87040B	262144B
	4				37	57	172
	3						
	2	3		25%	49152B	65536B	131072B
	1				32	43	86

2 CoS	7	1	Strict	100%	106496B	180224B	524288B
	6						
	5				70	118	345
	4						
	3	2	Weighted Round Robin	100%	61440B	81920B	262144B
	2						
	1				40	53	172

1 CoS	7	1	Strict	100%	131072B	262144B	786432B
	6						
	5						
	4						
	3				86	172	518

Egress CoS Queuing CLI Commands

- 5520-24T-PWR(config)#***show qos queue-set-assignment***

  The show qos queue-set-assignment command displays in the CLI the 802.1p priority to egress CoS and QoS queue mapping for CoS setting 1-8. This command is in the CLI priv-exec mode.

- 5520-24T-PWR(config)#***show qos queue-set***

  The show qos queue-set command displays the queue set configuration. The display includes the general discipline of the queue, the percent bandwidth (Kbps), and the queues size in bytes. This command is in the CLI priv-exec mode.

- 5520-24T-PWR(config)#***qos agent queue set <1-8>***

  The qos agent queue set <1-8> command sets the egress CoS and QoS queue mode (1-8) in which the switch will operate. This parameter is global and requires a reset to activate a change. This command is in the CLI priv-exec mode.

- 5520-24T-PWR(config)#***qos queue-set-assignment queue-set <1-8> 1p <0-7> queue <1-8>***

The qos queue-set-assignment queue-set <1-8> 1p <0-7> queue <1-8> command gives the user the ability to specify the queue to associate an 802.1p priority. This command is in the CLI priv-exec mode.

- 5520-24T-PWR(config)#***default qos agent queue-set***

  The default qos agent queue-set command will default the egress CoS and QoS queue set. The default CoS/QoS queue mode is 8. This command is in the CLI priv-exec mode.

- 5520-24T-PWR(config)#***show qos agent***

  The show qos agent command displays the current attributes for egress CoS and QoS queue mode, resource sharing mode and QoS NVRAM commit delay. This command is in the CLI priv-exec mode.

- 5520-24T-PWR(config)#***qos agent nvram delay***

  The qos agent nvram delay command will modify the maximum time in seconds to write config data to non-volatile storage. This command is in the CLI priv-exec mode.

- 5520-24T-PWR(config)#***qos agent reset-default***

  The qos agent reset-default command resets QoS to its configuration default. This command is in the CLI priv-exec mode.

Egress Queue Recommendations

If you are running all untagged traffic and do not change default port priority settings, use setting 1 CoS.

5. Traffic Meter and Shaping

The Ethernet Routing Switch 5500 supports both policing/metering of ingress traffic in addition to egress port shaping. The meter and shape range is as shown in table 6 below. Please note that all QoS levels are respected and honoured on a shaped interface.

Table 6: Meter and Shaping Range and Granularity

Product	Meter/Shaper Range	Granularity	Bucket Size
ERS5510	1 Mbps to 1023 Mbps	1 Mbps	8 buckets
ERS5520	1 Mbps to 1023 Mbps	1 Mbps	8 buckets
ERS5530 (10M/100M,1G)	64 Kbps to 1023 Mbps	64 Kbps	8 buckets
ERS5530 (10G)	1 Mbps to 1023 Gbps	1 Mbps	12 buckets

When configuring traffic metering or shaping, a committed rate, a maximum burst size and burst duration is entered. The maximum burst rate and burst duration is used along with the committed rate to setup a fixed token bucket where each token represents 1 byte. Up to eight fixed bucket sizes are supported for all 10/100 Mbps and GigE ports. Up to twelve fixed bucket sizes are supported on the ERS5530 only via the 10 GigE interface. The token bucket allows a committed burst to occur up to the token bucket size.

For traffic metering, an in profile and an out of profile action is configured and is expressed as an id. You can use one of the default actions or create a new action prior to configuring a meter. To view the action id's, please use the command shown below. For example, if you wish to remark the in profile traffic with a QoS level of Bronze and drop traffic for out of profile traffic, select id 3 and 1 respectively. Please note that you must associate the classifier to identify IP traffic since the DSCP value is being remarked.

- 5530-24TFD(config)#***show qos action***

```
 Id         Name          Drop  Update    802.1p     Set Drop   Extension Storage
                            DSCP    Priority   Precedence             Type
_____ _________________ _____ _____ ____________ _________ _________ _______
1     Drop_Traffic      Yes   Ignore Ignore       High Drop            ReadOnl
2     Standard_Service  No    0x0    Priority 0   High Drop            ReadOnl
3     Bronze_Service    No    0xA    Priority 2   Low Drop             ReadOnl
4     Silver_Service    No    0x12   Priority 3   Low Drop             ReadOnl
5     Gold_Service      No    0x1A   Priority 4   Low Drop             ReadOnl
6     Platinum_Service  No    0x22   Priority 5   Low Drop             ReadOnl
7     Premium_Service   No    0x2E   Priority 6   Low Drop             ReadOnl
8     Network_Service   No    0x30   Priority 7   Low Drop             ReadOnl
9     Null_Action       No    Ignore Ignore       Low Drop             ReadOnl
55001 UntrustedClfrs1   DPass Ing 1p Ignore       Low Drop             Other
55002 UntrustedClfrs2   DPass 0x0    Priority 0   High Drop            Other
```

.

5.1 Actual Bucket Size

When configuring a meter or shape rate, a fixed token bucket is also configured which is derived from the committed rate, burst rate, and burst duration configured. If a burst duration is not configured, the largest bucket size is automatically selected which would be 512K for a 10/100 Mbps or 1 GigE port. If you wish to use another bucket size, you must calculate the burst duration by using the actual size of the bucket - Sections 5.2 and 5.3 provide examples. The following table, Table 7, shown below displays the actual bucket size in bytes.

Table 7: Actual Bucket Size in Bytes

Bucket Size	Actual size in bytes	Interface
4K	4,096	10/100 Mbps and GigE
8K	8,192	10/100 Mbps and GigE
16K	16,384	10/100 Mbps and GigE
32K	32,768	10/100 Mbps and GigE
64K	65,536	10/100 Mbps and GigE
128K	131,072	10/100 Mbps and GigE
256K	262,144	10/100 Mbps and GigE
512K	524,288	10/100 Mbps and GigE
1024K	1,048,576	10 GigE (5530)
4096K	2,097,152	10 GigE (5530)
8192K	8,388,608	10 GigE (5530)

5.2 Policing Traffic

When configuring traffic policing, the committed rate, burst rate, and burst duration can be configured using the following command:

- 5530-24TFD(config)#***qos meter <1-55000> committed-rate <64-10230000 Kbits/sec> max-burst-rate <64-4294967295 Kbits/sec> max-burst-duration <1-4294967295 Milliseconds> in-profile-action <1-55000> out-profile-action [<1-1>|<9-55000>]***

QoS parameters:

Parameter	Description
<1-55000>	Enter an integer to specify the QoS meter; range is 1 to 55000.
name <WORD>	Specify name for meter; maximum is 16 alphanumeric characters.
committed-rate <64-10230000>	Specifies rate that traffic must not exceed for extended periods to be considered in-profile. Enter the rate in Kb/s for in-profile traffic in increments of 1000 Kbits/sec; range is 64 to 10230000 Kbits/sec.
max-burst-rate <64-4294967295>	Specifies the largest burst of traffic that can be received in a given time for the traffic to be considered in-profile. Used in calculating the committed burst size. Enter the burst size in Kb/s for in-profile traffic; range is 64 to 294967295 Kbits/sec
max-burst-duration <1-4294967295>	Specifies the amount of time that the largest burst of traffic can be received for the traffic to be considered in-profile. Used in calculating the committed burst size. Enter the burst duration in ms for in-profile traffic; range is 1 to 4294967295 ms.
in-profile-action <1-55000>	Specify the in-profile action ID; range is 1 to 55000.
in-profile-action-name <WORD>	Specify the in-profile action name.

out-profile-action <1,9-55000>	Specify the out-of-profile action ID; range is 1, 9 to 55000.

When configuring a meter, please note the following:

- The maximum burst rate cannot be configured the same as the committed or metered rate. You must always specify a higher maximum burst rate than the committed or metered rate
- The maximum burst rate and burst duration is used to calculate the bucket size or committed burst in bytes
    - Duration = ((bucketSize*8) / (max-burst-rate – committed-rate))
- Bucket sizes in bytes are 4K, 8K, 16k, 32K, 64K, 128K, 256K, and 512K
- For the 10 GigE module only, available for the Ethernet Routing Switch 5530, it supports bucket sizes of 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, 1024K, 2048K, 4096K, and 8192K.
- If you do not specify maximum burst duration when setting up a meter, the maximum bucket size will be automatically set. For all 10/100 Mbps and 1 GigE ports, the maximum bucket size is 512K. Also, it does not matter what value you enter for the maximum burst rate as long as it is larger than the committed rate.

Example:

Let's assume you wish to set the committed rate to 10M and set the committed burst (bucket size) to 128K. We also wish to mark all in profile traffic to Bronze and drop all out of profile traffic. To accomplish this, please use the following commands:

1. Calculate the duration, expressed in milliseconds.

Using the actual bucket size from table 7 and a maximum burst rate of 15M

- Duration = ((bucketSize*8) / (max-burst-rate – committed-rate))
- Duration = ((131,072* 8) / (15,000,000 – 10,000,000))
- Duration = 209.7152 ms
- Rounded up, the duration value is 210 ms

2. Next, enter the following command on the Ethernet Switch 5500. Enter an in profile action id of 3 for an in profile action of Bronze. Enter an out of profile action of 1 for an out of profile action of drop traffic.
    - 5530-24TFD(config)#***qos meter 1 name meter_1 committed-rate 10000 max-burst-rate 15000 max-burst-duration 210 in-profile-action 3 out-profile-action 1***
3. Use the following command to view the meter just configured.
    - 5530-24TFD(config)#***show qos meter***

```
 Id          Name        Commit    Commit     In-Profile       Out-Profile  Storage
                          Rate      Burst       Action           Action       Type
                         (Kbps)   (Bytes)

_____ _______________ _______ ________ _______________ _______________ ______
1     meter_1         10000    131072   Bronze_Service  Drop_Traffic    NonVol
```

4. Next, you will need to configure a policy and add this meter to the policy.

The following table displays all various bucket size and duration values available using the committed and maximum burst values used in this example.

Table 8: Meter Bucket Size and Duration

Bucket Size	Max burst rate	Committed rate	Duration	Value to enter (mSec)
4,096	15000000	10000000	0.0065536	7
8,192	15000000	10000000	0.0131072	13
16,384	15000000	10000000	0.0262144	26
32,768	15000000	10000000	0.0524288	52
65,536	15000000	10000000	0.1048576	105
131,072	15000000	10000000	0.2097152	210
262,144	15000000	10000000	0.4194304	419
524,288	15000000	10000000	0.8388608	839
1,048,576*	15000000	10000000	1.6777216	1678
2,097,152*	15000000	10000000	3.3554432	3355
8,388,608*	15000000	10000000	13.4217728	13422

* ERS5530 10GE only

5.3 Interface Shaper

When configuring interface shaping, the shape rate, burst rate, and burst duration can be configured using the following command:

- 5530-24TFD(config)#***interface fastEthernet all***
- 5530-24TFD(config-if)#***qos if-shaper port <port #> shape-rate <64-10230000 Kbits/sec> max-burst-rate <64-4294967295 Kbits/sec> max-burst-duration <1-4294967295 milliseconds>***

QoS interface shaping parameters:

Parameter	Description
<portlist>	Ports to configure shaping parameters.
<WORD>	Specify name for if-shaper; maximum is 16 alphanumeric characters.
shape-rate <64-10230000>	Shaping rate in kilobits/sec; range is 64-10230000 kilobits/sec.
max-burst-rate <64-4294967295>	Maximum burst rate in kilobits/sec; range is 64-4294967295Kbits/sec.
max-burst-duration <1-4294967295>	Maximum burst duration in milliseconds; range is 1 to 4294967295 ms.

When configuring interface shaping on an interface, please note the following:

- The maximum burst rate cannot be configured the same as the shape rate. You must always specify a higher maximum burst rate than the shape rate
- The maximum burst rate and burst duration is used to calculate the bucket size or committed burst in bytes
- The maximum burst rate and burst duration is used to calculate the bucket size or committed burst in bytes
    - Duration = ((bucketSize*8) / (max-burst-rate – committed-rate))
- Bucket sizes in bytes are 4K, 8K, 16k, 32K, 64K, 128K, 256K, and 512K

- For the 10 GigE module only, available for the Ethernet Routing Switch 5530, it supports bucket sizes of 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, 1024K, 2048K, 4096K, and 8192K.
- If you do not specify maximum burst duration when setting up a shaper, the maximum bucket size will be automatically set. For all 10/100 Mbps and 1 GigE ports, the maximum bucket size is 512K. Also, it does not matter what value you enter for the maximum burst rate as long as it is larger than the committed rate.

Example

Let's assume you wish to set the committed rate to 40M and set the bucket size to 4K for port 8. To accomplish this, please use the following commands:

1. Calculate the duration, expressed in milliseconds.

Using the actual bucket size from table 7 and a maximum burst rate of 50M

- Duration = ((bucketSize*8) / (max-burst-rate – committed-rate))
- Duration = ((4,096 * 8) / (50,000,000 – 40,000,000))
- Duration = 3.2768 ms
- Rounded down, the duration value is 3 ms

2. Next, enter the following commands on the Ethernet Switch 5500. Enter an in profile action id of 3 for an in profile action of Bronze. Enter an out of profile action of 1 for an out of profile action of drop traffic.

- 5530-24TFD(config)#***interface fastEthernet all***
- 5530-24TFD(config-if)# ***qos if-shaper port 8 shape-rate 40000 max-burst-rate 50000 max-burst-duration 3***

3. Use the following command to view the shaper just configured.

- 5530-24TFD(config)# ***show qos if-shaper port 8***

```
Unit Port IfIndex       Name          Rate    Burst
                                            Size
                                    (Kbps)  (Bytes)
____ ____ ________ __________________ ________ ________
1    8    8                         40000    4096
```

6. Default Nortel Class of Service

The following table shows the default Nortel Class of Service marking.

Table 9: Default Nortel CoS Markings

DSCP		TOS	Binary	NNSC	PHB
Hex	**Decimal**				
0x0	0	0x0	000000 **00**	Standard	CS0
0x0	0	0x0	000000 **00**		DE
0x8	8	0x20	001000 **00**	Bronze	CS1
0xA	10	0x28	001010 **00**		AF11
0x10	16	0x40	010000 **00**	Silver	CS2
0x12	18	0x48	010010 **00**		AF21
0x18	24	0x60	011000 **00**	Gold	CS3
0x1A	26	0x68	011010 **00**		AF31
0x20	32	0x80	100000 **00**	Platinum	CS4
0x22	34	0x88	100010 **00**		AF41
0x28	40	0xA0	101000 **00**	Premium	CS5
0x2E	46	0xB8	101110 **00**		EF
0x30	48	0xC0	110000 **00**	Network	CS6
0x38	56	0xE0	111000 **00**	Critical	CS7

7. QoS Access Lists (ACL)

As of software release 5.0, the ERS55xx can be configured using access lists (ACL). You can choose to use policies and/or ACL's to configure the ERS5500 switch. Up to a maximum of 15 precedence levels are supported using policies whereas ACL's allows up to a maximum of 8 precedence levels.

Please be aware of the following when using ACLs:

- By default, ACL's are always terminated by an implicit action of "drop all non-matching traffic". The default action of "drop all non-matching traffic" cannot be changed.
- ACL precedence is always in the order the ACL's are entered
- ACL's are applied at a port level
- Up to 8 precedence levels are supported, however, you can use ACL blocks if you have similar filter rules - please see classifier block explanation in section 3.2
- When an ACL is assigned to a port, the ACL is assigned the highest precedence value available on the port. Each additional ACL that is added is then assigned decreasing precedence levels. Any policies (QoS or non-QoS) already associated with a port dictate the starting and subsequent precedence values for the ACL(s).
- You cannot assign traffic meters
- IP and L2 ACL's cannot be combined. If you wish to combine L2 and L3, policies must be used
- ACL's cannot be modified; you must first remove the ACL-assign configuration at a port level, then delete the ACL or ACL's you wish to modify and reconfigure the ACL or ACL's.
- ACL's can be enabled or disabled. However, you cannot update or change the associated precedence values when the ACL is disabled.
- You can only configure ACL's using CLI or http (QoS Wizard). Although JDM will display the ACL configuration, you cannot use JDM to either configure or delete ACL's.

7.1 ACL Configuration

7.1.1 IP-ACL Configuration

IP ACL's are added using the following command:

- 5500 (config)#***qos ip-acl name <1..16 character string> ?***

```
addr-type       Specify the address type (IPv4, IPv6) classifier criteria
block           Specify the label to identify access-list elements that are of
                the same block
drop-action     Specify the drop action
ds-field        Specify the DSCP classifier criteria
dst-ip          Specify the destination IP classifier criteria
dst-port-min    Specify the L4 destination port minimum value classifier
                criteria
flow-id         Specify the IPv6 flow identifier classifier criteria
next-header     Specify the IPv6 next header classifier criteria
protocol        Specify the IPv4 protocol classifier criteria
set-drop-prec   Specify the set drop precedence
src-ip          Specify the source IP classifier criteria
src-port-min    Specify the L4 source port minimum value classifier criteria
update-1p       Specify the update user priority
update-dscp     Specify the update DSCP
<cr>
```

7.1.2 L2-ACL Configuration

L2 ACL's are added using the following command:

- 5500 (config)#***qos l2-acl name <1..16 character string> ?***

```
block          Specify the label to identify access-list elements that are of
               the same block
drop-action    Specify the drop action
dst-mac        Specify the destination MAC classifier criteria
dst-mac-mask   Specify the destination MAC mask classifier criteria
ethertype      Specify the ethertype classifier criteria
priority       Specify the user priority classifier criteria
set-drop-prec  Specify the set drop precedence
src-mac        Specify the source MAC classifier criteria
src-mac-mask   Specify the source MAC mask classifier criteria
update-1p      Specify the update user priority
update-dscp    Specify the update DSCP
vlan-min       Specify the Vlan ID minimum value classifier criteria
vlan-tag       Specify the vlan tag classifier criteria
<cr>
```

7.1.3 ACL-Assign Configuration

Once you have completed the ACL configuration, the ACL name is then assigned at a port level using the following command:

- 5500 (config)#***qos acl-assign port <port # or port #'s> acl-type <ip|l2> name <acl name>***

7.1.4 ACL Configuration Example

7.1.4.1 Configuration

Assuming we wish to configure the following:

- remark host 172.1.1.10 ftp traffic to CoS class of Silver
- remark host 172.1.1.10 http traffic to CoS class of Gold
- apply the ACL to port 1/19

To accomplish the above, please enter the following commands:

- 5500 (config)#***qos ip-acl name host src-ip 172.1.1.10/32 protocol 6 src-port-min 21 src-port-max 21 update-dscp 18 block tcpcommon***
- 5500 (config)#***qos ip-acl name host src-ip 172.1.1.10/32 protocol 6 src-port-min 80 src-port-max 80 update-dscp 26 block tcpcommon***
- 5500 (config)#***qos ip-acl name host drop-action disable***
- 5500 (config)#***qos acl-assign port 1/19 acl-type ip name host***

Please note the following:

- The first two IP-ACL's are assigned to a block named *tcpcommand*. Since we are only allowed up to eight precedence levels, it is a good idea to use block configuration whenever possible.
- The third IP-ACL is required to match all other traffic. As the default implicit action is drop all non-matching traffic, if this command is not entered, only ftp and http traffic from host 172.1.1.10 would be allowed.
- Protocol 6 refer to TCP traffic

- The DSCP value are entered in decimal; please refer to section 6 for details

The following table displays the various protocol numbers:

Protocol Number	Protocol
1	ICMP
2	IGMP
6	TCP
17	UDP
46	RSVP

7.1.4.2 Verification

To view the ACL configuration and assignment, enter the following commands:

- 5530H-24TFD#***show qos acl-assign***

```
Id               Name                 State    ACL  Unit/Port Storage
                                                Type             Type

_____ ___________________________ ________ ____ _________ _______
1     host                        Enabled  IP   1/19      NonVol
```

- 5530H-24TFD#***show qos ip-acl***

```
Name: host
Block: tcpcommon
Address Type: IPv4
Destination Addr/Mask: Ignore
Source Addr/Mask: 172.1.1.10/32
DSCP: Ignore
IPv4 Protocol / IPv6 Next Header: TCP
Destination L4 Port Min: Ignore
Destination L4 Port Max: Ignore
Source L4 Port Min: 21
Source L4 Port Max: 21
IPv6 Flow Id: Ignore
Action Drop: No
Action Update DSCP: 0x12
Action Update 802.1p Priority: Ignore
Action Set Drop Precedence: Low Drop
Type: Access List
Storage Type: NonVolatile

Id: 2
Name: host
Block: tcpcommon
Address Type: IPv4
Destination Addr/Mask: Ignore
Source Addr/Mask: 172.1.1.10/32
DSCP: Ignore
IPv4 Protocol / IPv6 Next Header: TCP
Destination L4 Port Min: Ignore
Destination L4 Port Max: Ignore
Source L4 Port Min: 80
Source L4 Port Max: 80
IPv6 Flow Id: Ignore
Action Drop: No
Action Update DSCP: 0x1A
Action Update 802.1p Priority: Ignore
Action Set Drop Precedence: Low Drop
Type: Access List
Storage Type: NonVolatile

Id: 3
Name: host
Block:
Address Type: IPv4
Destination Addr/Mask: Ignore
Source Addr/Mask: Ignore
```

```
DSCP: Ignore
IPv4 Protocol / IPv6 Next Header: Ignore
Destination L4 Port Min: Ignore
Destination L4 Port Max: Ignore
Source L4 Port Min: Ignore
Source L4 Port Max: Ignore
IPv6 Flow Id: Ignore
Action Drop: No
Action Update DSCP: Ignore
Action Update 802.1p Priority: Ignore
Action Set Drop Precedence: Low Drop
Type: Access List
Storage Type: NonVolatile
```

- 5530H-24TFD#***show qos policy***

```
Id: 55001
Policy Name: UntrustedClfrs1
State: Enabled
Classifier Type: Block
Classifier Name: UntrustedClfrs1
Classifier Id: 55001
Role Combination: allQoSPolicyIfcs
Meter:
Meter Id:
In-Profile Action: UntrustedClfrs1
In-Profile Action Id: 55001
Non-Match Action:
Non-Match Action Id:
Track Statistics: Aggregate
Precedence: 2
Session Id: 0
Storage Type: Other

Id: 55002
Policy Name: UntrustedClfrs2
State: Enabled
Classifier Type: Block
Classifier Name: UntrustedClfrs2
Classifier Id: 55002
Role Combination: allQoSPolicyIfcs
Meter:
Meter Id:
In-Profile Action: UntrustedClfrs2
In-Profile Action Id: 55002
Non-Match Action:
Non-Match Action Id:
Track Statistics: Aggregate
Precedence: 1
Session Id: 0
Storage Type: Other

Id: 55003
Policy Name: host
State: Enabled
Classifier Type: Block
Classifier Name: tcpcommon
Classifier Id: 55003
Unit/Port: 1/19
Meter:
Meter Id:
In-Profile Action:
In-Profile Action Id:
Non-Match Action:
Non-Match Action Id:
Track Statistics: Aggregate
Precedence: 12
Session Id: 0
Storage Type: Other
```

```
Id: 55004
Policy Name: host
State: Enabled
Classifier Type: Classifier
Classifier Name: host
Classifier Id: 55005
Unit/Port: 1/19
Meter:
Meter Id:
In-Profile Action: host
In-Profile Action Id: 55005
Non-Match Action: Drop_Traffic
Non-Match Action Id: 1
Track Statistics: Aggregate
Precedence: 11
Session Id: 0
Storage Type: Other
```

7.1.4.3 Changing ACL

Assuming we wish to change the http marking from CoS level of Gold to CoS level of Bronze, enter the following command shown below.

From using the show command above, we know that port 1/19 as been assigned ACL-Assign ID of 1. Hence, we need to remove this id first using the following command:

- 5500(config)#***no qos acl-assign 1***

or if you wish to remove the setting on an individual port; we only used one port for this example, so either command can be used.

- 5500(config)#***no qos acl-assign 1 port 1/19***

Next, we need to delete IP-ACL id 2:

- 5500(config)#***no qos ip-acl 2***

Next, we need to create a new IP-ACL with the new filter criteria:

- 5500 (config)#***qos ip-acl name host src-ip 172.1.1.10/32 protocol 6 src-port-min 80 src-port-max 80 update-dscp 10 block tcpcommon***

Finally, re-apply the IP-ACL back to port 1/19:

- 5500 (config)#***qos acl-assign port 1/19 acl-type ip name host***

8. IP Security Features

This section covers the security features DHCP Snooping, ARP-Inspection, and IP Source Guard. DHCP Snooping and ARP-Inspection where added in the 5.0 software release while IP Source Guard was added in the 5.1 software release. If you are using a software release prior to 5.0, please see the next section.

8.1 DHCP Snooping

DHCP snooping is a security feature that builds a binding table on untrusted ports by monitoring DHCP messages. On core or uplink ports, the port(s) is considered trusted and should be configured as such. The DHCP snooping binding table consists of the leased IP address, MAC address, lease time, port number, and VLAN ID. DHCP snooping is configured at a per VLAN basis where, by default, all ports are set to untrusted. You must configure the uplink ports as trusted.

Overall, DHCP snooping operates as follows:

- Allows only DHCP requests form untrusted ports.
- DHCP replies and all other DHCP messages from untrusted ports are dropped
- Verifies the DHCP snooping binding table on untrusted ports to verify the traffic entering a port by comparing the source MAC address against the DHCP lease IP address. If there is no match, the packet is dropped

8.1.1 DHCP Snooping Configuration

To enable DHCP snooping, enter the following command assuming we wish to enable DHCP snooping on VLANs 100 and 200 and the uplink port is 1/24.

- `5500(config)#`***`ip dhcp-snooping vlan 100`***
- `5500(config)#`***`ip dhcp-snooping vlan 200`***
- `5500(config)#`***`ip dhcp-snooping enable`***
- `5500(config)#`***`interface fastEthernet 1/24`***
- `5500(config-if)#`***`ip dhcp-snooping trusted`***
- `5500(config-if)#`***`exit`***

8.2 Dynamic ARP Inspection

Dynamic ARP Inspection verifies the ARP packets to prevent man-in-the-middle (MITM) types of attacks. Without dynamic ARP inspection, a malicious user can attack hosts in a local subnet by poisoning the ARP cache of hosts connected to this subnet by intercepting traffic intended for other hosts on the subnet. This normally takes place on VLAN with multiple hosts connected. Dynamic ARP inspection is used together with DHCP snooping by using the binding table to validate the host MAC address to IP address binding on untrusted ports. ARP packets on untrusted ports are only forward if they match the source MAC to IP address in the binding table. DHCP snooping must be enable prior to enabling dynamic ARP inspection.

8.2.1 Dynamic ARP Inspection Configuration

Assuming DHCP snooping is already enable for VLANs 100 and 200 and port 1/19 is the uplink port, enter the following commands:

- `5500(config)#`***`ip arp-inspection vlan 100`***
- `5500(config)#`***`ip arp-inspection vlan 200`***
- `5500(config)#`***`interface fastEthernet 1/24`***
- `5500(config-if)#`***`ip arp-inspection trusted`***
- `5500(config-if)#`***`exit`***

8.3 IP Source Guard

IP source guard works together with the DHCP snooping binding table by providing security against invalid source IP addresses. If enabled, the source IP address is checked against the source IP address in the binding table on untrusted ports. If the incoming source IP address does not match the IP address in the binding table, the packet is dropped. Please note that manual (static) assignment of IP addresses is not allowed as DHCP snooping does not support static binding entries

8.3.1 IP Source Guard Configuration

Assuming DHCP snooping is already configured with untrusted port members 2-20, enter the following commands:

- `5500(config)#`***`interface fastEthernet 2-20`***
- `5500(config-if)#`***`ip verify source`***
- `5500(config-if)#`***`exit`***

9. BPDU Filtering

BPDU filtering is a feature that when enabled at a port level, will either shutdown a port for a specific time period or forever when it receives a Spanning Tree BPDU. For all user access ports, it is recommended to enable Spanning Tree Fast Start in addition to BPDU filtering. If you select to shut down the port forever, manual intervention is required to bring the port back up by disabling and then re-enabling the port state.

BPDU filter is enabled at an interface level using the following commands:

- `5520-1(config-if)#`***`spanning-tree bpdu-filtering timeout <10-65535 seconds or 0 for infinity>`***
- `5520-1(config-if)#`***`spanning-tree bpdu-filtering enable`***

9.1 BPDU Filtering Configuration

Assuming we wish to enable BPDU filtering with the timer set to infinity (set to 0) on access ports 1/1 to 1/10, enter the following commands:

- `5520-1(config)#`***`interface fastEthernet 1/1-10`***
- `5520-1(config-if)#`***`spanning-tree learning fast`***
- `5520-1(config-if)#`***`spanning-tree bpdu-filtering timeout 0`***
- `5520-1(config-if)#`***`spanning-tree bpdu-filtering enable`***
- `5520-1(config-if)#`***`exit`***

10. QoS Interface Applications

In the 4.2 software release or higher, several new QoS applications designed to enhance security have been added to the switch. These QoS security applications target several of the most common denial of service (DoS) launched against networks today. The following items have been added:

- ARP Spoofing
- DHCP Snooping
- DHCP Spoofing
- SQLSlam
- Nachia
- Xmas
- TCP SynFinScan
- TCP FtpPort
- TCP DnsPort
- BPDU Blocker

When using any of the QoS applications listed above, a number of classifiers are required per QoS applications. Please refer to table 10 shown below.

Table 10: QoS Applications – Number of Classifiers Used

Feature	Number of Classifiers
ARP Spoofing	5
DHCP Snooping	1
DHCP Spoofing	2
DoS SQLSlam	1
DoS Nachia	1
DoS Xmas	1
DoS TCP SynFinScan	1
DoS TCP FTPPort	2
DoS TCP DNS Port	2
BPDUBlock	1

For more details on Layer 2 security, please refer to the Technical Configuration guide titled ‘Layer Security Solutions for ES and ERS Switches’ for more details in regards to security and adding security filters for the Ethernet Routing Switch prior to release 4.2. This document can be found by going to www.nortel.com/support and can be found under any Ethernet Switch or Ethernet Routing Switch folder.

10.1 ARP Spoofing

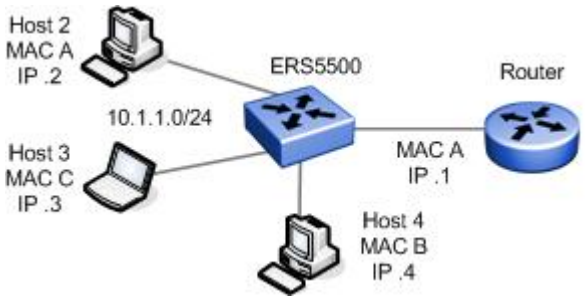

Figure 3: Arp Spoofing Example

Considering Figure 3 above, host 4 wishes to perform an ARP spoofing man-in-the-middle (MITM) attack. When hosts 2 or 3 wish to communicate with the router, they will send an ARP request for the router's MAC address. The router (.1) will respond, but as soon as host 4 sends a gARP broadcast claiming it to be the router (.1), hosts 2 and 3 will update their ARP entry for .1 to host 4's MAC address. Also, host 4 can send a gARP to the router using its MAC address for either host 2 or host 3. Now traffic forwarded or received off the 10.1.1.0/24 for either host 2 or host 3 will go to host 4's MAC address. Host 4 could then forward the traffic to the real router, drop the traffic, sniff the traffic, or modify the contents of a packet.

It is possible to prevent ARP/MAC spoofing using off-set filters to block any gratuitous ARPs (gARP). Basically, you have to allow broadcast ARP, block any ARP messages using the source IP or target IP of the default gateway, and then allow ARP reply; these filters should not be applied to the router port(s), only on the user ports. In the 4.2 release or higher, a new command has been added to prevent ARP Spoofing between hosts and the router default gateway.

Configuration Example

Assuming the following:

- The default gateway is 10.1.25.1
- The user ports are ports 26 to 30; we will create an interface group named vlan10 for these ports

In software release 4.2 or higher, you can now use the CLI or WEB interface to enable ARP Spoofing Detection. Continuing from the example above, in release 4.2 or higher, enter the following commands:

- 5530-24TFD(config)#***interface fastEthernet all***
- 5530-24TFD(config-if)#***qos arp spoofing port 26-30 default-gateway 10.1.25.1***

Overall, using either method above, the ARP Spoofing QoS application performs the following operations:

1. Pass all broadcast ARP requests.
2. Drop all non-broadcast ARP requests.
3. Drop all ARP packets with a source IP address equal to the identified default gateway.
4. Drop all ARP packets with a target IP address equal to the identified default gateway.
5. Pass all ARP responses.

10.2 DHCP Attacks

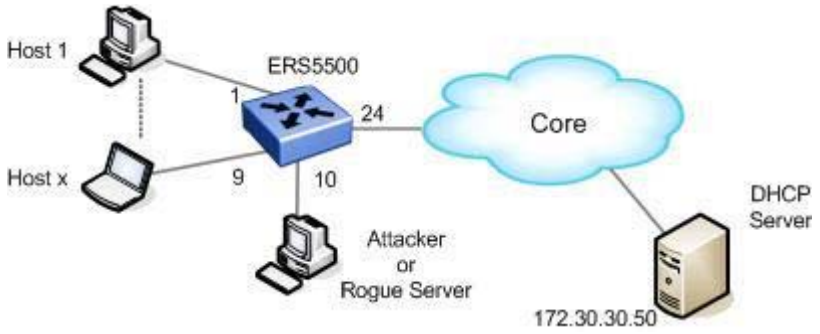

Figure 4: DHCP Attack Example

There are two types of attacks that can occur with DHCP:

- An attacker could request multiple IP addresses from a DHCP server by spoofing its source MAC address. This can be achieved by using a tool such as gobbler: http://www.networkpenetration.com/downloads.html. If the attack is successful, all leases on the DHCP server will be exhausted.
- The second method is where the network attacker sets up a rogue DHCP server and responds to new DHCP requests from clients on the network. The attackers DHCP server could be setup to send DHCP responses using its address for the default gateway and DNS server. This would allow the attacker to sniff out the client's traffic and allowing for a 'man-in-the-middle' attack.

The Ethernet Routing Switch 5500 offers the following solutions to overcome the issues raised above.

DHCP Snooping

The DHCP Snooping QoS Application operates by classifying ports as access (untrusted) and core (trusted) and only allowing DHCP requests from the access ports. All other types of DHCP messages received on access ports are discarded. This prevents rogue DHCP servers from being set-up by attackers on access ports and generating DHCP responses that provide the rogue server's address for the default gateway and DNS server. This helps prevent DHCP "man-in-the-middle" attacks. The user will need to specify the interface type for the ports on which they wish to enable this support.

Based on Figure 4 above, enter the following commands to enable DHCP Snooping

- 5530-24TFD(config)#***interface fastEthernet all***
- 5530-24TFD(config-if)#***qos dhcp snooping port 1-10 interface-type access***
- 5530-24TFD(config-if)#***qos dhcp snooping port 24 interface-type core***

DHCP Spoofing

Another method that is used to combat rogue DHCP servers is to restrict traffic destined for a client's DHCP port (UDP port 68) to that which originated from a known DHCP server's IP address.

The DHCP Spoofing QoS Application will require the identification of the valid DHCP server address and the ports on which the DHCP Spoofing support should be applied. This will cause two policies to be installed on these interfaces to perform the following operations:

1. Pass DHCP traffic originated by the valid DHCP server.
2. Drop DHCP traffic originated by all other hosts.

Based on the diagram above, enter the following commands to enable DHCP Snooping

- 5530-24TFD(config)#***interface fastEthernet all***
- 5530-24TFD(config-if)#***qos dhcp spoofing port 2-10 dhcp-server 172.30.30.50***

10.3 DoS

The following command is used to enable the various DoS QoS Applications

- 5530-24TFD(config)#***interface fastEthernet all***
- 5530-24TFD(config-if)#***qos dos <nachia|sqlslam|tcp-dnsport|tcp-ftpport|tcp-synfinscan|xmas> port <port #> enable***

SQLSlam

The worm targeting SQL Server computers is a self-propagating, malicious code that exploits a vulnerability that allows for the execution of arbitrary code on the SQL Server computer due to a stack buffer overflow. Once the worm compromises a machine it will try to propagate itself by crafting packets of 376 bytes and send them to randomly chosen IP addresses on UDP port 1434. If the packet is sent to a vulnerable machine, this victim machine will become infected and will also begin to propagate. Beyond the scanning activity for new hosts, the current variant of this worm has no Configuring Quality of Service and IP Filtering for Nortel Ethernet Routing Switch 5500 Series, Software Release 4.2 other payload. Activity of this worm is readily identifiable on a network by the presence of 376 byte UDP packets. These packets will appear to be originating from seemingly random IP addresses and destined for UDP port 1434.

When enabled, the DoS SQLSlam QoS Application will drop UDP traffic whose destination port is 1434 with the byte pattern of 0x040101010101 starting at byte 47 of a tagged packet.

Nachia

The W32/Nachi variants W32/Nachi-A and W32/Nachi-B are worms that spread using the RPC DCOM vulnerability in a similar fashion to the W32/Blaster-A worm. Both rely upon two vulnerabilities in Microsoft's software.

When enabled, the DoS Nachia QoS Application will drop ICMP traffic with the byte pattern of 0xaaaaaa) starting at byte 48 of a tagged packet.

Xmas

Xmas is a DoS attack that sends TCP packets with all TCP flags set in the same packet; which is illegal. When enabled, the DoS Xmas QoS Application will drop TCP traffic with the URG:PSH TCP flags set.TCP

SynFinScan

TCP SynFinScan is a DoS attack that sends both a TCP SYN and FIN in the same packet; which is illegal. When enabled, the TCP SynFinScan QoS Application will drop TCP traffic with the SYN:FIN TCP flags set.

TCP FtpPort

A TCP FtpPort attack is identified by TCP packets with a source port of 20 and a destination port less than 1024; which is illegal. A legal FTP request would have been initiated with a TCP port greater than 1024. When enabled, the TCP FtpPort QoS Application will drop TCP traffic with the TCP SYN flag set and a source port of 20 with a destination port less than or equal to 1024.

TCP DnsPort

The TCP DnsPort QoS Application is similar to the TCP FtpPort application but for DNS port 53. When enabled, this application will drop TCP traffic with the TCP SYN flag set and a source port of 53 with a destination port less than or equal to 1024.BPDU

10.4 BPDU Blocking

There are certain scenarios in a bridged (switched) environment when the user may wish to drop incoming BPDUs on a specific interface. When enabled, the BPDU Blocker QoS Application will drop traffic with a specific multicast destination MAC address. Currently targeted BPDU multicast destination addresses are 01:80:c2:00:00:00 and 01:00:0c:cc:cc:cd.

The following commands are used to enable BPDU blocking

- 5530-24TFD(config)#***interface fastEthernet all***
- 5530-24TFD(config-if)# ***qos bpdu blocker port <port #> enable***

11. Configuration Steps – Policy Configuration

11.1 Role Combination

A role combination is formed by assigning one or more physical ports to the role and by designating the interface class (Trusted, Untrusted, Un-restricted) for the role and associated ports. By default, when using the WEB interface, all ports on the Ethernet Routing Switch 5500 are assigned to the default interface group named 'allBayStacklfcs' which has an interface class of untrusted. A port on the Ethernet Routing Switch 5500 can only belong to one role combination.

When configuring a policy, an interface group will be assigned to the policy.

To add a new role combination, complete the following steps:

a) Add a new Interface Group:

- ERS5500-48T(config)#***qos if-group name <name> class <trusted|unrestricted|untrusted>***

b) Assign the physical ports to the Interface Group:

- ERS5500-48T(config)# ***qos if-assign port <port #> name <if-group name>***

Example:

- ERS5500-48T(config)#***qos if-group name role_one class untrusted***
- ERS5500-48T(config)# ***qos if-assign port 1/5 name role_one***

c) View Role Combination:

To view the Role Combination, enter the following command:

- ERS5500-48T#***show qos if-assign***

```
Unit  Port  IfIndex  Role Combination  Queue Set
____  ____  _______  ________________  _________
1     1     1        allBayStackIfcs   8
1     2     2        allBayStackIfcs   8
1     3     3        allBayStackIfcs   8
1     4     4        allBayStackIfcs   8
1     5     5        role_one          8
```

- ERS5500-48T#***show qos if-group***

```
            Role                  Interface      Capabilities       Storage
         Combination                Class                           Type
_____________________________ ____________ ___________________ ___________
allBayStackIfcs               Untrusted    Input 802, Input IP ReadOnly
role_one                      Untrusted    Input 802, Input IP NonVolatile
```

11.2 Classification

Classification consists of adding the following items:

- Add IP or L2 or both classifier elements
- Add a classifier. As mentioned above in the overview section, a classifier can be made up of one of the following items:
  - One IP classifier element
  - One L2 classifier element
  - One IP and one L2 classifier element
- Optional: Create Classifier Block where a block contains two or more classifier elements. Please see restrictions below.

When adding a new policy, either a classifier or a classifier block can be assigned to the policy. Since there is a limit of 15 classification masks available per port, it is advantageous to use Classifier Blocks whenever possible. Multiple Classifiers can be added to a Classifier Block allowing up to 15 Classifiers and/or Classifier Blocks per port. By using Classifier blocks, up to a total of 114 classifiers can be applied to a port.

a) Adding IP and L2 Element

IP Element

To add an IP element, enter the following command:

- ERS5500-48T(config)#***qos ip-element <1-64000>?***

```
  addr-type     Specify the address type (IPv4, IPv6) classifier criteria
  ds-field      Specify the DSCP classifier criteria
  dst-ip        Specify the destination IP classifier criteria
  dst-port-min  Specify the L4 destination port minimum value classifier
                criteria
  flow-id       Specify the IPv6 flow identifier classifier criteria
  next-header   Specify the IPv6 next header classifier criteria
  protocol      Specify the IPv4 protocol classifier criteria
  src-ip        Specify the source IP classifier criteria
  src-port-min  Specify the L4 source port minimum value classifier criteria
<cr>
```

Example:

- ERS5500-48T(config)#***qos ip-element 1 src-ip 10.62.32.0/19 dst-ip 10.13.196.0/22***

L2 Element

- ERS5500-48T(config)#***qos l2-element <1-64000>***

```
  dst-mac       Specify the destination MAC classifier criteria
  dst-mac-mask  Specify the destination MAC mask classifier criteria
  ethertype     Specify the ethertype classifier criteria
  priority      Specify the user priority classifier criteria
  src-mac       Specify the source MAC classifier criteria
  src-mac-mask  Specify the source MAC mask classifier criteria
  vlan-min      Specify the Vlan ID minimum value classifier criteria
  vlan-tag      Specify the vlan tag classifier criteria

  <cr>
```

Example:

- ERS5500-48T(config)# ***qos l2-element 1 src-mac 00-00-0A-00-00-00 src-mac-mask FF-FF-FF-FF-FF-00 ethertype 0x800***

NOTE: If you wish to combine an IP element and a L2 element for a classifier, the L2 element's EtherType must set configured as 0x0800. The following is an example of a L2 element to match VLAN 1:

- ERS5500-48T(config)#***qos l2-element 1 vlan-min 1 vlan-max 1 ethertype 0x800***

b) Adding a Classifier

To add a new classifier, enter the following command:

- ERS5500-48T(config)#***qos classifier <1-64000> set-id <1-64000> name <name> element-type <ip|l2> element-id <1-64000>***

Where element-id = IP element or L2 element ID.

Example:

Adding an IP element to a classifier:

- ERS5500-48T(config)#***qos classifier 1 set-id 1 name class_1 element-type ip element-id 1***

Adding an IP element and a L2 element to a classifier:

- ERS5500-48T(config)#***qos classifier 2 set-id 2 name class_2 element-type ip element-id 2***
- ERS5500-48T(config)#***qos classifier 3 set-id 2 name class_2 element-type l2 element-id 1***

c) Adding a Classifier Block

To add a new classifier block, enter the following command:

- ERS5500-48T(config)#***qos classifier-block <1-64000> block-number <1-64000> name <name> set-id <1-64000>***

Example:

The following commands add classifiers 1 and 4 to classifier block 1.

- ERS5500-48T(config)#***qos classifier-block 1 block-number 1 name block_1 set-id 1***
- ERS5500-48T(config)#***qos classifier-block 2 block-number 1 name block_1 set-id 4***

11.3 Meters

To add a meter, enter the following command:

- ERS5500-48T(config)#***qos meter <1-64000> name <name> committed-rate <1000-1023000 Kbit/sec> max-burst-rate <1-4294967295> max-burst-duration <1-4294967295> in-profile-action <1-64000> out-profile-action <1-64000>***

To view the action number, enter the following command:

ERS5500-48T(config)#***show qos action***

Id	Name	Drop	Update DSCP	802.1p Priority	Set Drop Precedence	Extension	Storage Type
1	Drop_Traffic	Yes	Ignore	Ignore	High Drop		ReadOnl
2	Standard_Service	DPass	0x0	Priority 0	High Drop		ReadOnl
3	Bronze_Service	DPass	0xA	Priority 2	Low Drop		ReadOnl
4	Silver_Service	DPass	0x12	Priority 3	Low Drop		ReadOnl
5	Gold_Service	DPass	0x1A	Priority 4	Low Drop		ReadOnl
6	Platinum_Service	DPass	0x22	Priority 5	Low Drop		ReadOnl
7	Premium_Service	DPass	0x2E	Priority 6	Low Drop		ReadOnl
8	Network_Service	DPass	0x30	Priority 7	Low Drop		ReadOnl
9	Null_Action	DPass	Ignore	Ignore	Low Drop		ReadOnl
64001	UntrustedClfrs1	DPass	Ing 1p	Ignore	Low Drop		Other
64002	UntrustedClfrs2	DPass	0x0	Priority 0	High Drop		Other

QoS Meter Command Parameters

Parameters and variables	Description
<metid>	Enter an integer to specify the QoS meter; range is 1 to 64000.
name <metname>	Specify name for meter; maximum is 16 alphanumeric characters.
committed-rate <rate>	Specifies rate that traffic must not exceed for extended periods to be considered in-profile. Enter the rate in Kb/s for in-profile traffic in increments of 1000 Kbits/sec; range is 1000 to 1023000 Kbits/sec.
max-burst-rate <burstrate>	Specifies the largest burst of traffic that can be received a given time for the traffic to be considered in-profile. Used in calculating the committed burst size. Enter the burst size in Kb/s for in-profile traffic; range is 1 to 4294967295 Kbits/sec
max-burst-duration <burstdur>	Specifies the amount of time that the largest burst of traffic that can be received for the traffic to be considered in-profile. Used in calculating the committed burst size. Enter the burst duration in ms for in-profile traffic; range is 1 to 4294967295 ms.
in-profile-action <actid>	Specify the in-profile action ID.
in-profile-action-name <actname>	Specify the in-profile action name.
out-profile-action <actid>	Specify the out-of-profile action ID.
out-profile-action-name <actname>	Specify the out-of-profile action name.

Example:

The following example creates a meter with a CIR of 10 Mbps, burst rate of 20 Mbps for 13 msec with an in profile action of Silver Service and an out profile action of drop traffic.

- ERS5500-48T(config)#***qos meter 1 name meter_one committed-rate 10000 max-burst-rate 20000 max-burst-duration 13 in-profile-action 4 out-profile-action 1***

11.4 Add a New Policy

a) To assign a Classifier to a new Policy without a meter, enter the following command:

- ERS5500-48T(config)#***qos policy <1-64000> name <name> if-group <if-group name> clfr-type <block|classifier> clfr-id <1-64000> in-profile-action <1-64000> non-match-action <1-64000> precedence <3-10**> track-statistics <individual/aggregate>***

NOTE: Instead of 'clfr-id' you can also enter the classifier or classifier-block name by using 'clfr-name'.

b) To assign a Classifier to a new Policy with a meter, enter the following command:

- ERS5500-48T(config)# ***qos policy <1-64000> name <name> if-group <if-group name> clfr-type <block|classifier> classifier clfr-id <1-64000> meter <1-64000> non-match-action <1-64000> precedence <3-10**> track-statistics <individual/aggregate>***

Example:

The following adds classifier block 1 to policy 1 with an in profile action of drop if matched and out profile action of Standard Service if not matched.

- ERS5500-48T(config)#***qos policy 1 name policy_one if-group role_one clfr-type block clfr-id 1 in-profile-action 1 non-match-action 2 precedence 10***

To add track individual statistics for each classifier, use the following command:

- ERS5500-48T(config)#***qos policy 1 name policy_one if-group role_one clfr-type block clfr-id 1 in-profile-action 1 non-match-action 2 precedence 10 track-statistics individual***

12. Configuration Examples

12.1 Pre-defined Values

QoS Action

Prior to adding a new meter or when configuring a policy, an in-profile and out-profile action is added. The action itself is referenced to by a numeric number. You can use any of the default actions or if you wish, you can create a new action prior to configuring a meter or adding a new policy. Please use the following command to view the QoS actions available.

- 5530-24TFD(config)#***show qos action***

```
 Id         Name          Drop  Update    802.1p      Set Drop    Extension Storage
                            DSCP    Priority    Precedence              Type
_____ _________________ _____ ______ ____________ ___________ _________ _______
1     Drop_Traffic      Yes   Ignore Ignore       High Drop             ReadOnl
2     Standard_Service  No    0x0    Priority 0   High Drop             ReadOnl
3     Bronze_Service    No    0xA    Priority 2   Low Drop              ReadOnl
4     Silver_Service    No    0x12   Priority 3   Low Drop              ReadOnl
5     Gold_Service      No    0x1A   Priority 4   Low Drop              ReadOnl
6     Platinum_Service  No    0x22   Priority 5   Low Drop              ReadOnl
7     Premium_Service   No    0x2E   Priority 6   Low Drop              ReadOnl
8     Network_Service   No    0x30   Priority 7   Low Drop              ReadOnl
9     Null_Action       No    Ignore Ignore       Low Drop              ReadOnl
55001 UntrustedClfrs1   DPass Ing 1p Ignore       Low Drop              Other
55002 UntrustedClfrs2   DPass 0x0    Priority 0   High Drop             Other
```

IP Element

When setting up an ip-element, you have the option of selecting any of the following default parameters. Also, if you wish, you can add user-defined protocol and port numbers.

Table 8: Pre-defined IP Element Values

Feature	Pre-defined Numerical Value	Parameter
DSCP	-1	Ignore
	0 to 63	Decimal DSCP value
Protocol	6	TCP
	1	ICMP
	2	IGMP
	17	UDP
	46	RSVP
Src/Dst Port	69	TFTP
	21	FTP Control
	20	FTP Data
	23	Telnet
	25	SMTP
	80	HTTP
	443	HTTPS

12.2 Configuration Example 1 – Traffic Meter Using Policies

Figure 5: Traffic Meter Example

The following CLI commands show how to configure a QoS Policy using a Classifier-block with three classifiers and traffic meters. Overall, in this example, we will configure the following:

- Setup one Policy with three classifiers metered with the following TCP flows:
  - For UDP dst port 80, meter traffic at 10M
  - For UDP dst port 69, meter traffic at 5M
  - For UDP dst port 137, meter traffic at 1M
- Set the meter bucket size (committed burst) for all meters to maximum value
- Add the policy to ports 5 and 6

NOTE: As all three classifiers use the same mask, we will create a classifier block to group all three classifiers.

At this time, it is only possible to configure traffic meters using policies. It is not possible to add traffic meters via ACL's.

12.2.1 ERS5500 Configuration Using Policies

12.2.1.1 Configure the Interface Role Combination

For this example, we will configure a new role combination with port members 5 and 6. You have the choice of assigning a policy directly at a port level or using an interface role.

By default, all ports are set for untrusted using the allBayStacklfcs Role Combination. In this example, we will configure a new Role Combination as untrusted and assign it to port 5 and 6.

ERS5500 Step 1 – Create the Interface Role Combination and name is "q2"

```
ERS5500-24T(config)#qos if-group name q2 class untrusted
ERS5500-24T(config)#qos if-assign port 5-6 name q2
```

12.2.1.2 Configure the IP elements

Configure three IP elements for UDP destination ports 80, 69, and 137.

ERS5500 Step 1 – Create the IP elements

```
ERS5500-24T(config)#qos ip-element 1 addr-type ipv4 protocol 17 dst-port-min 80
dst-port-max 80
```

```
ERS5500-24T(config)#qos ip-element 2 addr-type ipv4 protocol 17 dst-port-min 69
dst-port-max 69

ERS5500-24T(config)#qos ip-element 3 addr-type ipv4 protocol 17 dst-port-min
137 dst-port-max 137
```

Please note that protocol 17 = UDP.

12.2.1.3 Configure three Classifiers, one for each of the IP elements configured above

ERS5500 Step 1 – Create the an IP Classifier for each IP element created above

```
ERS5500-24T(config)#qos classifier 1 set-id 1 name c1 element-type ip element-
id 1

ERS5500-24T(config)#qos classifier 2 set-id 2 name c2 element-type ip element-
id 2

ERS5500-24T(config)#qos classifier 3 set-id 3 name c3 element-type ip element-
id 3
```

The element-id = the element number you assigned in the previous step above

12.2.1.4 Configure Meters

As mentioned in section 5.2 above, if we do not configure a maximum duration rate, the committed burst will be automatically set to the maximum value. For all 10/100 Mbps and 1 GigE Ethernet ports, the maximum committed burst is 524,288 bytes. Hence, it does not matter what value you enter for the max-burst-rate as long is it is greater than the committed-rate.

ERS5500 Step 1 – Create the QoS meters: "m1" with 10M, "m2" with 5M, and "m3" with 1M

```
ERS5500-24T(config)#qos meter 1 name m1 committed-rate 10000 max-burst-rate
11000 in-profile-action 2 out-profile-action 1

ERS5500-24T(config)#qos meter 2 name m2 committed-rate 5000 max-burst-rate 6000
in-profile-action 2 out-profile-action 1

ERS5500-24T(config)#qos meter 3 name m3 committed-rate 1000 max-burst-rate 2000
in-profile-action 2 out-profile-action 1
```

12.2.1.5 Configure the Classifier Block

For this example, we will create a classifier block named "b1" with the following

- ID 1 with Classifier element 1 and meter 1
- ID 2 with classifier element 2 and meter 2
- ID 3 with classifier element 3 and meter 3

ERS5500 Step 1 – Create the classifier block

```
ERS5500-24T(config)#qos classifier-block 1 block-number 1 name b1 set-id 1
meter 1

ERS5500-24T(config)#qos classifier-block 2 block-number 1 name b1 set-id 2
```

```
meter 2

ERS5500-24T(config)#qos classifier-block 3 block-number 1 name b1 set-id 3
meter 3
```

12.2.1.6 Configure the Policy

The following command creates a policy with the classifier block created in step e above and also enables statistics for each classifier element in the block.

ERS5500 Step 1 – Create the policy

```
ERS5500-24T(config)#qos policy 1 if-group q2 clfr-type block clfr-name b1 non-
match-action 2 precedence 3 track-statistics individual
```

12.2.2 Verify Operations

12.2.2.1 Verify the Role Combination

Step 1 – Verify that the if-group has been configured correctly

```
ERS5500-24T#show qos if-group
```

Result:

```
                Role                    Interface       Capabilities        Storage
            Combination                   Class                             Type
_____________________________________ ____________ ____________________ ___________
allQoSPolicyIfcs                      Untrusted    Input 802, Input IP ReadOnly
unrestricted                          Unrestricted Input 802, Input IP NonVolatile
q2                                    Untrusted    Input 802, Input IP NonVolatile
$remediationIfcs                      Unrestricted Input 802, Input IP Other
$NsnaIfcs                             Unrestricted Input 802, Input IP Other
```

Step 1 – Verify that the correct ports have been assigned to the if-group named “q2”

```
ERS5500-24T#show qos if-assign port 5-6
```

Result:

```
Unit Port IfIndex Role Combination Queue Set Capability
____ ____ _______ __________________ _________ __________
1    5    5       q2                2         Version 1
1    6    6       q2                2         Version 1
```

12.2.2.2 Verify IP-Element Configuration

Step 1 – Verify that the 3 IP Elements

```
ERS5500-24T# show qos ip-element
```

Result:

```
    Id: 1
    Address Type: IPv4
    Destination Addr/Mask: Ignore
    Source Addr/Mask: Ignore
    DSCP: Ignore
    IPv6 Flow Id: Ignore
    IPv4 Protocol / IPv6 Next Header: UDP
    Destination L4 Port Min: 80
    Destination L4 Port Max: 80
    Source L4 Port Min: Ignore
    Source L4 Port Max: Ignore
    Session Id: 0
    Storage Type: NonVolatile

    Id: 2
    Address Type: IPv4
    Destination Addr/Mask: Ignore
    Source Addr/Mask: Ignore
    DSCP: Ignore
    IPv6 Flow Id: Ignore
    IPv4 Protocol / IPv6 Next Header: UDP
    Destination L4 Port Min: 69
    Destination L4 Port Max: 69
    Source L4 Port Min: Ignore
    Source L4 Port Max: Ignore
    Session Id: 0
    Storage Type: NonVolatile

    Id: 3
    Address Type: IPv4
    Destination Addr/Mask: Ignore
    Source Addr/Mask: Ignore
    DSCP: Ignore
    IPv6 Flow Id: Ignore
    IPv4 Protocol / IPv6 Next Header: UDP
    Destination L4 Port Min: 137
    Destination L4 Port Max: 137
    Source L4 Port Min: Ignore
    Source L4 Port Max: Ignore
    Session Id: 0
    Storage Type: NonVolatile
```

12.2.3 Verify Classifier and Classifier Block Configuration

Step 1 – Verify that the 3 Classifiers

```
ERS5500-24T# show qos classifier
```

Result:

```
     Id      Classifier     Classifier Criteria Criteria  Session     Storage
               Name           Set Id     Type      Id        Id        Type

_____ _________________ __________ ________ ________ __________ ___________
1     c1                1          IP       1        0          NonVolatile
2     c2                2          IP       2        0          NonVolatile
3     c3                3          IP       3        0          NonVolatile
55001 UntrustedClfrs1   55001      L2       55001    0          Other
55002 UntrustedClfrs2   55002      L2       55002    0          Other
```

Step 3 – Verify that the Meter Configuration

```
ERS5500-24T#show qos meter
```

Result:

```
Id: 1
Name: m1
```

```
Commit Rate: 10000 Kbps
Commit Burst: 524288 Bytes
In-Profile Action: Standard_Service
Out-Profile Action: Drop_Traffic
Session Id: 0
Storage Type: NonVolatile

Id: 2
Name: m2
Commit Rate: 5000 Kbps
Commit Burst: 524288 Bytes
In-Profile Action: Standard_Service
Out-Profile Action: Drop_Traffic
Session Id: 0
Storage Type: NonVolatile

Id: 3
Name: m3
Commit Rate: 1000 Kbps
Commit Burst: 524288 Bytes
In-Profile Action: Standard_Service
Out-Profile Action: Drop_Traffic
Session Id: 0
Storage Type: NonVolatile
```

Step 3 – Verify that the Classifier Block with the correct classifier and meter number

```
ERS5500-24T#show qos classifier-block
```

Result:

```
    Id: 1
    Block Name: b1
    Block Number: 1
    Classifier Name: c1
    Classifier Set Id: 1
    Meter Name: m1
    Meter Id: 1
    Action Name:
    Action Id:
    Session Id: 0
    Storage Type: NonVolatile

    Id: 2
    Block Name: b1
    Block Number: 1
    Classifier Name: c2
    Classifier Set Id: 2
    Meter Name: m2
    Meter Id: 2
    Action Name:
    Action Id:
    Session Id: 0
    Storage Type: NonVolatile

    Id: 3
    Block Name: b1
    Block Number: 1
    Classifier Name: c3
    Classifier Set Id: 3
    Meter Name: m3
    Meter Id: 3
    Action Name:
    Action Id:
    Session Id: 0
    Storage Type: NonVolatile
```

12.2.3.1 Verify Policy Configuration

Step 1 – Verify that the QoS Policy

```
ERS5500-24T#show qos policy
```

Result:

```
    Policy Name: policy1
    State: Enabled
    Classifier Type: Block
    Classifier Name: b1
    Classifier Id: 1
    Role Combination: q2
    Meter:
    Meter Id:
    In-Profile Action:
    In-Profile Action Id:
    Non-Match Action: Standard_Service
    Non-Match Action Id: 2
    Track Statistics: Individual
    Precedence: 3
    Session Id: 0
    Storage Type: NonVolatile
```

12.3 Configuration Example – IP ACL, DHCP Snooping, ARP Inspection, BPDU Filtering, and Source Guard

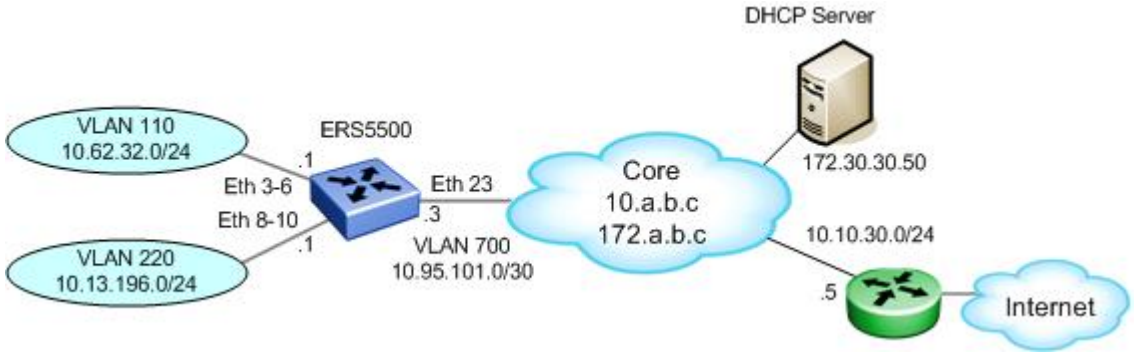

Figure 4: IP ACL, DHCP Snooping, ARP Inspection, and Source Guard

Overall, we wish to accomplish the following in regards to VLAN 110:

- Only allow ICMP and DHCP traffic to the DHCP server (172.30.30.50) and deny all other traffic to the 172.x.x.x network
- For the 10.x.x.x network, only allow access to the local network (10.62.32.0/24) and to the 10.10.30/0/24 network for full access to the internet
- Enable DHCP Snooping, ARP-Inspection, and

In regards to VLAN 220, we wish to accomplish the following:

- Allow full access to the core network 172.0.0.0/8 and 10.0.0.0/8
- Only allow only ICMP, HTTP and HTTPS traffic to the internet

12.3.1 ERS5500 Configuration

12.3.1.1 Create VLAN's and Add Port Members

ERS5500: Step 1 – Add VLANs 110, 220, and 700

```
5500(config)#vlan create 700 name core type port
5500(config)#vlan create 110 type port
5500(config)#vlan create 220 type port
5500(config)#vlan members remove 1 3-6,8-10,23
5500(config)#vlan ports 23 tagging tagall
5500(config)#vlan members 110 3-6
5500(config)#vlan members 220 8-10
5500(config)#vlan members 700 23
```

12.3.1.2 Add IP Address and Enable OSPF

ERS5500: Step 1 – Add IP address to VLAN 110 and enable OSPF with interface type of passive

```
5500(config)# interface vlan 110
5500(config-if)#ip address 10.62.32.1 255.255.255.0
5500(config-if)#ip ospf network passive
5500(config-if)#ip ospf enable
5500(config-if)#exit
```

ERS5500: Step 2– Add IP address to VLAN 220 and enable OSPF with interface type of passive

```
5500(config)# interface vlan 220
5500(config-if)#ip address 10.13.196.1 255.255.255.0
5500(config-if)#ip ospf network passive
5500(config-if)#ip ospf enable
5500(config-if)#exit
```

ERS5500: Step 3– Add IP address to VLAN 700 and enable OSPF

```
5500(config)# interface vlan 700
5500(config-if)#ip address 10.95.101.3 255.255.255.0
5500(config-if)#ip ospf enable
5500(config-if)#exit
```

12.3.1.3 Enable IP Routing and OSPF Globally

ERS5500: Step 1 – Enable IP routing and OSPF Globally

```
5500(config)#ip routing
5500(config)# router ospf enable
```

12.3.1.4 Enable DHCP Relay

ERS5500: Step 1 – Enable STP Fast Start and BPDU Filtering

```
5500(config)#ip dhcp-relay fwd-path 10.62.32.1 172.30.30.50 mode dhcp
5500(config)#ip dhcp-relay fwd-path 10.13.196.1 172.30.30.50 mode dhcp
```

12.3.1.5 Enable STP Fast Start, BPDU Filtering and Broadcast/Multicast Rate Limiting

ERS5500: Step 1 – Enable STP Fast Start and BPDU Filtering

```
5500(config)#interface fastEthernet 3-6,8-10
5500(config-if)#spanning-tree learning fast
5500(config-if)#spanning-tree bpdu-filtering timeout 0
5500(config-if)#spanning-tree bpdu-filtering enable
5500(config-if)#exit
```

ERS5500: Step 2 – Enable Rate Limiting to 10% of total traffic for both broadcast and multicast traffic

```
5500(config)#interface fastEthernet all
5500(config-if)#rate-limit port 1-10 both 10
5500(config-if)#exit
```

Please note that the rate limit parameter on the ERS5500 is expressed as percentage of total traffic. The values used in this example are just a suggestion and may vary depending on your needs.

12.3.1.6 Enable DHCP-Snooping and ARP-Inspection

ERS5500: Step 1 – Enable DHCP-Snooping for VLAN's 110 and 220 and enable DHCP-Snooping globally

```
5500(config)#ip dhcp-snooping vlan 110
5500(config)#ip dhcp-snooping vlan 220
5500(config)#ip dhcp-snooping enable
```

ERS5500: Step 1 – Enable ARP-Inspection for VLAN's 110 and 220

```
5500(config)# ip arp-inspection vlan 110
5500(config)# ip arp-inspection vlan 220
```

12.3.1.7 Enable IP Source Guard

ERS5500: Step 1 – Enable IP Source Guard on access port members from VLAN 110 and 220

```
5500(config)#interface fastEthernet 3-6,8-10
5500(config-if)#ip verify source
5500(config-if)#exit
```

12.3.1.8 Create ACL's for VLAN 110 Port Members

ERS5500: Step 1 – Create IP-ACL's pertaining to VLAN 110 VLAN port members

```
5500(config)#qos ip-acl name one dst-ip 172.30.30.50/32 protocol 1
5500(config)#qos ip-acl name one dst-ip 172.30.30.50/32 protocol 17 dst-port-min 67 dst-port-max 67
5500(config)#qos ip-acl name one dst-ip 10.10.30.0/24 block b1
5500(config)#qos ip-acl name one dst-ip 10.62.32.0/24 block b1
5500(config)#qos ip-acl name one dst-ip 10.0.0.0/8 drop-action enable block b2
```

```
5500(config)#qos ip-acl name one dst-ip 172.0.0.0/8 drop-action enable
block b2
5500(config)#qos ip-acl name one drop-action disable
```

ERS5500: Step 2 – Assign the IP-ACL's to ports 3-6

```
5500(config)#qos acl-assign port 3-6 acl-type ip name one
```

If you do not assign a drop-action to the individual IP-ACL configuration, the default action of disable will be used. The non-match global action is always drop.

Protocol 1 refers to ICMP while protocol 17 refers to UDP.

12.3.1.9 Create ACL's for VLAN 220 Port Members

ERS5500: Step 1 – Create IP-ACL's pertaining to VLAN 220 VLAN port members

```
5500(config)#qos ip-acl name two dst-ip 10.0.0.0/8 block b3
5500(config)#qos ip-acl name two dst-ip 172.0.0.0/8 block b3
5500(config)# qos ip-acl name two protocol 6 dst-port-min 80 dst-port-max
80 block b4
5500(config)# qos ip-acl name two protocol 6 dst-port-min 443 dst-port-
max 443 block b4
5500(config)# qos ip-acl name two protocol 1
```

ERS5500: Step 2 – Assign the IP-ACL's to ports 8-10

```
5500(config)#qos acl-assign port 8-10 acl-type ip name two
```

12.3.2 Verify Operations

12.3.2.1 Verify DHCP-Snooping

Step 1 – Verify that DHCP-Snooping is enabled for VLAN's 110 and 220

```
ERS5500-24T# show ip dhcp-snooping
```

Result:

```
    Global DHCP snooping state: Enabled
           DHCP
    VLAN Snooping
    ---- --------
    1    Disabled
    99   Disabled
    110  Enabled
    220  Enabled
    700  Disabled
```

Step 2 – Verify all the access port are configured for 'untrusted' – this is the default setting

```
ERS5500-24T# show ip dhcp-snooping interface 3-6,8-10
```

Result:

```
          DHCP
    Port Snooping
    ---- --------
    3    Untrusted
    4    Untrusted
    5    Untrusted
    6    Untrusted
    8    Untrusted
    9    Untrusted
    10   Untrusted
```

Step 3 – To view the DHCP-Snoop binding, enter the following command, assuming we have port member on ports 6 and 9

```
ERS5500-24T#show ip dhcp-snooping binding
```

Result:

```
    MAC                IP              Lease (sec)  VID   Port
    ------------------------------------------------------------------
    00-50-8b-e1-58-e8  10.62.32.10     691200       110   6
    00-02-a5-e9-00-28  10.13.196.10    691200       220   9
    Total Entries: 2
```

12.3.2.2 Verify ARP Inspection

Step 1 – Verify that ARP Inspection is enabled for VLAN's 110 and 220

```
ERS5500-24T# show ip arp-inspection vlan
```

Result:

```
          ARP
    VLAN Inspection
    ---- ----------
    1    Disabled
    99   Disabled
    110  Enabled
    220  Enabled
    700  Disabled
```

Step 2 – Verify all the access ports are configured for 'untrusted' – this is the default setting

```
ERS5500-24T# show ip arp-inspection interface 3-6,8-10
```

Result:

```
          ARP
    Port Inspection
    ---- ----------
    3    Untrusted
    4    Untrusted
    5    Untrusted
    6    Untrusted
    8    Untrusted
    9    Untrusted
    10   Untrusted
```

12.3.2.3 Verify IP Source Guard

Step 1 – To view the IP Source Guard binding, enter the following command, assuming we have port member on ports 6 and 9

```
ERS5500-24T# show ip source binding
```

Result:

```
    Port Address
    ---- ---------------
    6    10.62.32.10
    9    10.13.196.10
```

An IP source Guard or ARP Inspection event will be logged (local and remote if enabled) indicated by the message, i.e. from port 6: "*ARP packet with invalid IP/MAC binding on un-trusted port 1/6*".

12.3.2.4 Verify ACL Configuration

Step 1 – To view the IP ACL configuration, enter the following command:

```
ERS5500-24T#show qos ip-acl
```

Result:

```
    Id: 1
    Name: one
    Block:
    Address Type: IPv4
    Destination Addr/Mask: 172.30.30.50/32
    Source Addr/Mask: Ignore
    DSCP: Ignore
    IPv4 Protocol / IPv6 Next Header: ICMP
    Destination L4 Port Min: Ignore
    Destination L4 Port Max: Ignore
    Source L4 Port Min: Ignore
    Source L4 Port Max: Ignore
    IPv6 Flow Id: Ignore
    Action Drop: No
    Action Update DSCP: Ignore
    Action Update 802.1p Priority: Ignore
    Action Set Drop Precedence: Low Drop
    Type: Access List
    Storage Type: NonVolatile

    Id: 2
    Name: one
    Block:
    Address Type: IPv4
    Destination Addr/Mask: 172.30.30.50/32
    Source Addr/Mask: Ignore
    DSCP: Ignore
    IPv4 Protocol / IPv6 Next Header: UDP
    Destination L4 Port Min: 67
    Destination L4 Port Max: 67
    Source L4 Port Min: Ignore
    Source L4 Port Max: Ignore
    IPv6 Flow Id: Ignore
    Action Drop: No
    Action Update DSCP: Ignore
    Action Update 802.1p Priority: Ignore
    Action Set Drop Precedence: Low Drop
    Type: Access List
    Storage Type: NonVolatile
```

```
Id: 3
Name: one
Block: b1
Address Type: IPv4
Destination Addr/Mask: 10.10.30.0/24
Source Addr/Mask: Ignore
DSCP: Ignore
IPv4 Protocol / IPv6 Next Header: Ignore
Destination L4 Port Min: Ignore
Destination L4 Port Max: Ignore
Source L4 Port Min: Ignore
Source L4 Port Max: Ignore
IPv6 Flow Id: Ignore
Action Drop: No
Action Update DSCP: Ignore
Action Update 802.1p Priority: Ignore
Action Set Drop Precedence: Low Drop
Type: Access List
Storage Type: NonVolatile

Id: 4
Name: one
Block: b1
Address Type: IPv4
Destination Addr/Mask: 10.62.32.0/24
Source Addr/Mask: Ignore
DSCP: Ignore
IPv4 Protocol / IPv6 Next Header: Ignore
Destination L4 Port Min: Ignore
Destination L4 Port Max: Ignore
Source L4 Port Min: Ignore
Source L4 Port Max: Ignore
IPv6 Flow Id: Ignore
Action Drop: No
Action Update DSCP: Ignore
Action Update 802.1p Priority: Ignore
Action Set Drop Precedence: Low Drop
Type: Access List
Storage Type: NonVolatile

Id: 5
Name: one
Block: b2
Address Type: IPv4
Destination Addr/Mask: 10.0.0.0/8
Source Addr/Mask: Ignore
DSCP: Ignore
IPv4 Protocol / IPv6 Next Header: Ignore
Destination L4 Port Min: Ignore
Destination L4 Port Max: Ignore
Source L4 Port Min: Ignore
Source L4 Port Max: Ignore
IPv6 Flow Id: Ignore
Action Drop: Yes
Action Update DSCP: Ignore
Action Update 802.1p Priority: Ignore
Action Set Drop Precedence: Low Drop
Type: Access List
Storage Type: NonVolatile

Id: 6
Name: one
Block: b2
Address Type: IPv4
Destination Addr/Mask: 172.0.0.0/8
Source Addr/Mask: Ignore
DSCP: Ignore
IPv4 Protocol / IPv6 Next Header: Ignore
Destination L4 Port Min: Ignore
```

```
    Destination L4 Port Max: Ignore
    Source L4 Port Min: Ignore
    Source L4 Port Max: Ignore
    IPv6 Flow Id: Ignore
    Action Drop: Yes
    Action Update DSCP: Ignore
    Action Update 802.1p Priority: Ignore
    Action Set Drop Precedence: Low Drop
    Type: Access List
    Storage Type: NonVolatile

    Id: 7
    Name: one
    Block:
    Address Type: IPv4
    Destination Addr/Mask: Ignore
    Source Addr/Mask: Ignore
    DSCP: Ignore
    IPv4 Protocol / IPv6 Next Header: Ignore
    Destination L4 Port Min: Ignore
    Destination L4 Port Max: Ignore
    Source L4 Port Min: Ignore
    Source L4 Port Max: Ignore
    IPv6 Flow Id: Ignore
    Action Drop: No
    Action Update DSCP: Ignore
    Action Update 802.1p Priority: Ignore
    Action Set Drop Precedence: Low Drop
    Type: Access List
    Storage Type: NonVolatile

    Id: 8
    Name: two
    Block: b3
    Address Type: IPv4
    Destination Addr/Mask: 10.0.0.0/8
    Source Addr/Mask: Ignore
    DSCP: Ignore
    IPv4 Protocol / IPv6 Next Header: Ignore
    Destination L4 Port Min: Ignore
    Destination L4 Port Max: Ignore
    Source L4 Port Min: Ignore
    Source L4 Port Max: Ignore
    IPv6 Flow Id: Ignore
    Action Drop: No
    Action Update DSCP: Ignore
    Action Update 802.1p Priority: Ignore
    Action Set Drop Precedence: Low Drop
    Type: Access List
    Storage Type: NonVolatile

    Id: 9
    Name: two
    Block: b3
    Address Type: IPv4
    Destination Addr/Mask: 172.0.0.0/8
    Source Addr/Mask: Ignore
    DSCP: Ignore
    IPv4 Protocol / IPv6 Next Header: Ignore
    Destination L4 Port Min: Ignore
    Destination L4 Port Max: Ignore
    Source L4 Port Min: Ignore
    Source L4 Port Max: Ignore
    IPv6 Flow Id: Ignore
    Action Drop: No
    Action Update DSCP: Ignore
    Action Update 802.1p Priority: Ignore
    Action Set Drop Precedence: Low Drop
    Type: Access List
    Storage Type: NonVolatile
```

```
    Id: 10
    Name: two
    Block: b4
    Address Type: IPv4
    Destination Addr/Mask: Ignore
    Source Addr/Mask: Ignore
    DSCP: Ignore
    IPv4 Protocol / IPv6 Next Header: TCP
    Destination L4 Port Min: 80
    Destination L4 Port Max: 80
    Source L4 Port Min: Ignore
    Source L4 Port Max: Ignore
    IPv6 Flow Id: Ignore
    Action Drop: No
    Action Update DSCP: Ignore
    Action Update 802.1p Priority: Ignore
    Action Set Drop Precedence: Low Drop
    Type: Access List
    Storage Type: NonVolatile

    Id: 11
    Name: two
    Block: b4
    Address Type: IPv4
    Destination Addr/Mask: Ignore
    Source Addr/Mask: Ignore
    DSCP: Ignore
    IPv4 Protocol / IPv6 Next Header: TCP
    Destination L4 Port Min: 443
    Destination L4 Port Max: 443
    Source L4 Port Min: Ignore
    Source L4 Port Max: Ignore
    IPv6 Flow Id: Ignore
    Action Drop: No
    Action Update DSCP: Ignore
    Action Update 802.1p Priority: Ignore
    Action Set Drop Precedence: Low Drop
    Type: Access List
    Storage Type: NonVolatile

    Id: 12
    Name: two
    Block:
    Address Type: IPv4
    Destination Addr/Mask: Ignore
    Source Addr/Mask: Ignore
    DSCP: Ignore
    IPv4 Protocol / IPv6 Next Header: ICMP
    Destination L4 Port Min: Ignore
    Destination L4 Port Max: Ignore
    Source L4 Port Min: Ignore
    Source L4 Port Max: Ignore
    IPv6 Flow Id: Ignore
    Action Drop: No
    Action Update DSCP: Ignore
    Action Update 802.1p Priority: Ignore
    Action Set Drop Precedence: Low Drop
    Type: Access List
    Storage Type: NonVolatile
```

Step 2 – To view the IP ACL assignment, enter the following command:

```
ERS5500-24T#show qos acl-assign
```

Result:

```
    Id              Name              State    ACL  Unit/Port Storage
                                               Type            Type
```

```
_____ ____________________________ _______ ___ _______ _______
1     one                          Enabled IP  1/3     NonVol
2     one                          Enabled IP  1/4     NonVol
3     one                          Enabled IP  1/5     NonVol
4     one                          Enabled IP  1/6     NonVol
5     two                          Enabled IP  1/8     NonVol
6     two                          Enabled IP  1/9     NonVol
7     two                          Enabled IP  1/10    NonVol
```

12.4 Configuration Example 3: Port Range Using ACL or Policy

Assuming we wish to filter on the following port ranges and remark the traffic to CoS level shown below:

- TCP dst-port 80-127 with CoS level of Gold
- UDP dst-port 2000-2047 with CoS level of Silver

As mentioned in section 3.3, a port range must start with an even minimum number while the maximum number rightmost consecutive 0's are replaced with 1's. The table shown below displays the valid ranges that can be configured.

Table 9: Port Range

Protocol	Port or Port Range	Min/Max Range Binary Value	Valid Ranges ((Port Min + 2n) -1))
TCP Port Range: 80-127			
TCP	80-95	Min = 1010000 Max = 1011111	*Max Port Range*: 80-95 *Other valid ranges*: 80 to 80 80 to 81 80 to 83 80 to 87
TCP	96-127	Min = 1100000 Max = 1111111	*Max Port Range*: 96-127 *Other valid ranges*: 96 to 96 96 to 97 96 to 99 96 to 103 96 to 111
UDP Port Range: 2000-2047			
UDP	2000-2015	Min = 11111010000 Max = 11111011111	*Max Port Range*: 2000-2015 *Other valid ranges*: 000 to 2000 000 to 2001 000 to 2003 000 to 2007
UDP	2016-2047	Min = 11111100000 Max = 11111111111	*Max Port Range*: 2016-2047 *Other valid ranges*: 2016 to 2016 2016 to 2017 2016 to 2019 2016 to 2023 2016 to 2031

12.4.1 Configuration – Using Policies

12.4.1.1 Configure the Interface Role Combination

For this example, we will configure a new role combination with port members 3 to 6. You have the choice of assigning a policy directly at a port level or using an interface role.

By default, all ports are set for untrusted using the allBayStacklfcs Role Combination. In this example, we will configure a new Role Combination as unrestricted and assign it to port 3 to 6.

ERS5500 Step 1 – Create the Interface Role Combination and name is "ifx"

```
ERS5500-24T(config)# qos if-group name ifx class unrestricted
ERS5500-24T(config)#qos if-assign port 3-6 name ifx
```

12.4.1.2 Add new IP element pertaining to the port ranges above

ERS5500: Step 1 – Create IP elements for TCP port range 80-127

```
5500(config)#qos ip-element 1 protocol 6 dst-port-min 80 dst-port-max 95
5500(config)#qos ip-element 2 protocol 6 dst-port-min 96 dst-port-max 127
```

ERS5500: Step 1 – Create IP elements for UDP port range 2000-2027

```
5500(config)#qos ip-element 3 protocol 17 dst-port-min 2000 dst-port-max 2015
5500(config)#qos ip-element 4 protocol 17 dst-port-min 2016 dst-port-max 2047
```

12.4.1.3 Configure Classifiers, one for each of the IP elements configured above

ERS5500 Step 1 – Create the an IP Classifier for each IP element created above

```
5500(config)#qos classifier 1 set-id 1 name c1 element-type ip element-id 1
5500(config)#qos classifier 2 set-id 2 name c2 element-type ip element-id 2
5500(config)#qos classifier 3 set-id 3 name c3 element-type ip element-id 3
5500(config)#qos classifier 4 set-id 4 name c4 element-type ip element-id 4
```

12.4.1.4 Configure the Policies

Create the policies with the classifiers created above. Please refer to table 3 in reference to the policy action.

ERS5500 Step 1 – Create the policy

```
5500(config)#qos policy 1 name range_tcp_1 if-group ifx clfr-type classifier
clfr-id 1 in-profile-action 5 non-match-action 9 precedence 11
5500(config)#qos policy 2 name range_tcp_2 if-group ifx clfr-type classifier
clfr-id 2 in-profile-action 5 non-match-action 9 precedence 10
5500(config)#qos policy 3 name range_udp_1 if-group ifx clfr-type classifier
clfr-id 3 in-profile-action 4 non-match-action 9 precedence 9
5500(config)#qos policy 4 name range_udp_2 if-group ifx clfr-type classifier
clfr-id 4 in-profile-action 4 non-match-action 3 precedence 8
```

12.4.2 Configuration – Using IP-ACL's

12.4.2.1 Create ACL's for TCP Range 80-127

ERS5500: Step 1 – Create IP-ACL's for TCP port range 80-127 to remark traffic to CoS level of Gold (DSCP = decimal 26)
5500(config)#***qos ip-acl name range protocol 6 dst-port-min 80 dst-port-max 95 update-dscp 26***
5500(config)#***qos ip-acl name range protocol 6 dst-port-min 96 dst-port-max 127 update-dscp 26***
ERS5500: Step 2 – Create IP-ACL's for UDP port range 2000-2047 to remark traffic to CoS level of Silver (DSCP = decimal 18)
5500(config)#***qos ip-acl name range protocol 17 dst-port-min 2000 dst-port-max 2015 update-dscp 18***
5500(config)#***qos ip-acl name range protocol 17 dst-port-min 2016 dst-port-max 2047 update-dscp 18***
ERS5500: Step 3 – Remark all other traffic to Bronze
5500(config)# ***qos ip-acl name range update-dscp 10***
ERS5500: Step 2 – Assign the IP-ACL's to ports 3-6
5500(config)#***qos acl-assign port 3-6 acl-type ip name range***

If you do not assign a drop-action to the individual IP-ACL configuration, the default action of disable will be used. The non-match global action is always drop.

Protocol 17 refers to UDP and protocol 6 refers to TCP.

12.5 Configuration Example 4 – L2 Classification Based on MAC Address

In this configuration example, we wish to set the service class for any MAC address from 00:00:0A:00:00:00 to 00:00:0A:00:00:ff to a Service Class of Gold and all other traffic with a Service Class of Bronze. This in effect will change the 802.1p value to 4, if the port is set for tagged, and also set the DSCP value to AF31 (0x1A).

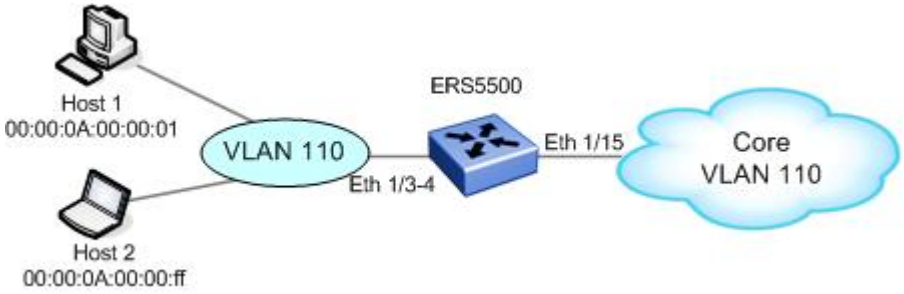

Figure 5: L2 Classification Based on MAC Address Example

12.5.1 ERS5500 Configuration – Using Policies

12.5.1.1 Configure the Interface Role Combination

ERS5500 Step 1 – Create the Interface Role Combination and name is "vlan_110"
ERS5500-24T(config)#***qos if-group name vlan_110 class unrestricted***
ERS5500-24T(config)#***qos if-assign port 1/3-4 name vlan_110***

12.5.1.2 Add new L2 element

ERS5500: Step 1 – Add an L2 element for VLAN 110 and specify MAC address
5500(config)#***qos l2-element 1 src-mac 00:00:0a:00:00:00 src-mac-mask ff:ff:ff:ff:ff:00 ethertype 0x800***

12.5.1.3 Configure Classifier

ERS5500 Step 1 – The following steps add the L2 element created above to an L2 classifier element
5500(config)#***qos classifier 1 set-id 1 name c1 element-type l2 element-id 1***

12.5.1.4 Create Policy

Create the policies with the classifiers created above. Please refer to table 3 in reference to the policy action.

ERS5500 Step 1 – Add policy for L2 classifier created above and apply it to role combination vlan_110 with an in-profile action of service class Gold and non-match action of service class bronze
5500(config)# ***qos policy 1 name "pol_1" if-group "vlan_110" clfr-type classifier***

```
clfr-id 1 in-profile-action 5 non-match-action 3 precedence 11
```

12.5.2 ERS5500 Configuration – Using IP-ACL's

12.5.2.1 Create L2 ACL's for MAC Address Range

ERS5500: Step 1 – Create L2-ACL's for MAC address range 00:00:01:00:00:00 to 00:00:01:00:00:ff

```
5500(config)# qos l2-acl name vlan_110 src-mac 00:00:0a:00:00:00 src-mac-mask
fff.fff.f00 ethertype 0x800 update-dscp 10
```

ERS5500: Step 2 – Pass all other traffic with standard CoS

```
5500(config)#qos l2-acl name vlan_110 drop-action disable
```

ERS5500: Step 3 – Assign the L2-ACL's to ports 3-4

```
5500(config)# qos acl-assign port 1/3-4 acl-type l2 name vlan_110
```

12.6 Configuration Example 5 – L2 and L3 Classification

In this configuration example, the Ethernet Routing Switch is used as L2 switch with two VLANs providing L2 private VLAN services. Both VLAN's have the same over-lapping IP addresses where workstation 1 and 2 are used to provide high-touch services. Overall, we wish to accomplish the following tasks:

- Setup a policy to provide Gold service for host 1 and Silver service for host 2
- For all other non-match traffic, set the default service class to Bronze service.

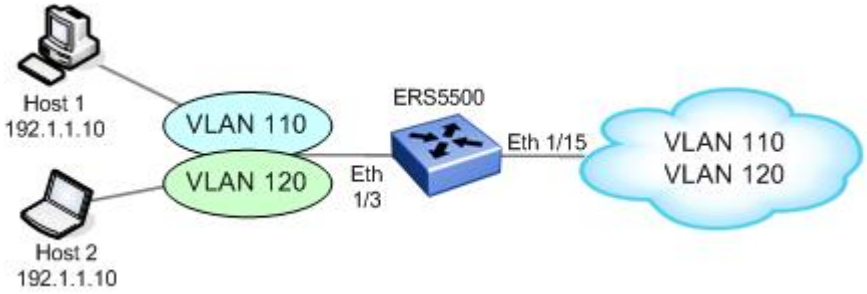

Figure 8: L2 and L3 Classification Example

The best way to accomplish these tasks is to:

- Create a Role Combination for port 1/3
- Create the first classifiers element with host 1's IP address and VLAN 110 and add to Classifier Block 1 with an in-profile action of Gold Service
- Create a second classifier element with host 2's IP address and VLAN 120 and add to Classifier Block 1 with an in-profile action of Silver Service
- Create a Policy with Classifier block 1 and the Role Combination for port 1/3 with a non-match action of Bronze Service

At this time, it is only possible to combine L2 and L3 filters using policies. It is not possible to combine IP-ACL's with L2-ACL's.

12.6.1 ERS5500 Configuration – Using Policies

12.6.1.1 Create a Separate Role Combination for Port 1/3

ERS5500 Step 1 – Add new role combination for port 1/3 configured as untrusted and add port member 1/3

```
ERS5500-24T(config)# qos if-group name Int_group_2  class untrustted
ERS5500-24T(config)# qos if-assign port 1/3 name Int_group_2
```

12.6.1.2 Add IP and L2 Classifiers Elements

ERS5500: Step 1 – Add IP elements with source address of 192.1.1.10

```
5500(config)#qos ip-element 1 src-ip 192.1.1.10/32
```

ERS5500: Step 2 – Add L2 elements for VLAN 110 and 120

```
5500(config)#qos l2-element 1 vlan-min 110 vlan-max 110 vlan-tag tagged
ethertype 0x800
5500(config)#qos l2-element 1 vlan-min 120 vlan-max 120 vlan-tag tagged
ethertype 0x800
```

12.6.1.3 Configure Classifier and Classifier Blocks

The following steps add two classifiers, one with IP element 1 and L2 element 1 and the second with IP element 1 and L2 element 2. We will also create a classifier block with two members, representing classifier id 1 and 2

ERS5500 Step 1 – The following commands add a classifier with IP element 1 and L2 element 1

```
5500(config)#qos classifier 1 set-id 1 name c1 element-type ip element-id 1
5500(config)# qos classifier 2 set-id 1 name c1 element-type l2 element-id 1
```

ERS5500 Step 2 – The next two commands add the second classifier with IP element 1 and L2 element 2

```
5500(config)#qos classifier 3 set-id 2 name c2 element-type ip element-id 1
5500(config)#qos classifier 4 set-id 2 name c2 element-type l2 element-id 2
```

ERS5500 Step 3 – Add a classifier block with classifier 1 with an in-provide action of Gold service and classifier 2 with an in-profile action of Silver service

```
5500(config)# qos classifier-block 1 block-number 1 name Pol_1 set-id 1 in-
profile-action 5
5500(config)# qos classifier-block 2 block-number 1 name Pol_1 set-id 2 in-
profile-action 4
```

12.6.1.4 Create Policy

Create the policies with the classifiers created above. Please refer to table 3 in reference to the policy action.

ERS5500 Step 1 – create a new policy with classifier block 1 with a non-match-action of Bronze service

```
5500(config)#qos policy 1 name Pol_1 if-group Int_group_2 clfr-type block clfr-
id 1 non-match-action 3 precedence 10
```

12.7 Configuration Example 6 - QoS Marking with Port Role Combination set for Un-restricted using ACL's

With a port role combination of un-restricted, the DSCP value is passed as-is and is not looked at by the ERS5500 internal QoS mapping. This does not apply to the p-bit which is looked at, honoured, and mapped according to the QoS priority mapping table. If you wish to apply QoS to the DSCP value on an unrestricted port member, either ACL's or policies must be defined where you need to map the DSCP value to the appropriate egress queue. For this example, we will demonstrate how to configure the ERS5500 to support internal QoS mapping for various DSCP values.

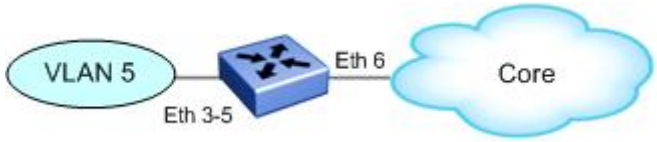

Figure 6: DSCP Mapping via Un-restricted Port Role

For this example, assume we wish to accomplish the following in regarded to the untagged VLAN 5 ingress port members:

- Set a port role of un-restricted with port members 3 to 6
- Select queue set 8 with 8 queues
- For ingress port members 3-5, we wish to map the following DSCP values. Please use the "*show qos queue-set-assignment*" command to display the
  - For DSCP 0x12 (Silver CoS), map to egress queue 5
  - For DSCP 0x1a (Gold CoS), map to egress queue 4
  - For DSCP 0x22 (Platinum CoS), map to egress queue 3

To accomplish the above, please follow the configuration steps below.

12.7.1 ERS5500 Configuration

12.7.1.1 Create VLAN 5

ERS5500: Step 1 – Remove port members from default VLAN and create VLAN 5
5500(config)#***vlan members remove 1 3-6***
5500(config)#***vlan create 5 type port***
5500(config)# ***vlan members add 5 3-6***

12.7.1.2 Create Queue Set 8

ERS5500: Step 1 – Add queue set 8; please note that you must reboot the switch for the queue set to take effect
5500(config)#***qos agent queue-set 8***
5500(config)#***boot***

12.7.1.3 Create New Unrestricted Interface Role

ERS5500: Step 1 – Add new unrestricted interface role with port members 3-6

```
5500(config)# qos if-group name unrestricted class unrestricted
5500(config)# qos if-assign port 3-6 name unrestricted
```

12.7.2 ACL Configuration

12.7.2.1 Create ACL's to Remark DSCP

ERS5500: Step 1 – Create IP-ACL's

```
5500(config)#qos ip-acl name pbit ds-field 18 update-1p 3 block pbit
5500(config)#qos ip-acl name pbit ds-field 26 update-1p 4 block pbit
5500(config)#qos ip-acl name pbit ds-field 34 update-1p 5 block pbit
5500(config)#qos ip-acl name pbit drop-action disable
```

ERS5500: Step 2 – Assign the IP-ACL's to ports 3-5

```
5500(config)#qos acl-assign port 3-5 acl-type ip name pbit
```

12.7.3 Policy Configuration

12.7.3.1 IP Element Configuration

ERS5500: Step 1 – Create IP Classifiers

```
5500(config)# qos ip-element 1 ds-field 18
5500(config)#qos ip-element 2 ds-field 26
5500(config)#qos ip-element 3 ds-field 34
```

12.7.3.2 Configure Classifier and Classifier Block

For the classifier block, we will match the following and set the following

IP Element ID	Classifier ID	Block ID	Action ID
1 (match DSCP 18)	1	Block 1, ID 1	4 – Silver CoS
2 match DSCP 26	2	Block 1, ID 2	5 – Gold CoS
3 – match DSCP 34	3	Block 1, ID 3	6 – Platinum CoS

ERS5500 Step 1 – Crete a Classifier for each of the IP Element above

```
5500(config)#qos classifier 1 set-id 1 name c1 element-type ip element-id 1
5500(config)#qos classifier 2 set-id 2 name c2 element-type ip element-id 2
5500(config)#qos classifier 3 set-id 3 name c3 element-type ip element-id 3
```

ERS5500 Step 1 – Create a Classifier Block

```
5500(config)# qos classifier-block 1 block-number 1 name b1 set-id 1 in-profile-
```

```
action 4
5500(config)# qos classifier-block 2 block-number 1 name b1 set-id 2 in-profile-action 5
5500(config)# qos classifier-block 3 block-number 1 name b1 set-id 3 in-profile-action 6
```

12.7.3.3 Create Policy

ERS5500 Step 1 – create a new policy with classifier block 1 with a non-match-action of Bronze service

```
5500(config)# qos policy 1 name pbit if-group unrestricted clfr-type block clfr-id 1 non-match-action 9 precedence 11
```

12.7.4 Verify Operations

12.7.4.1 View the Queue Assignments

The following commands are useful to display the queue mapping pertaining to the ACL configuration from above.

Step 1 – Use the following command to view the internal mapping of p-bit to queue for queue set 8; note, results are only shown for queue set 8

```
ERS5500-24T# show qos queue-set-assignment
```

Result:

```
Queue Set 8
802.1p Priority Queue
_______________ _____
0               8
1               7
2               6
3               5
4               4
5               3
6               1
7               2
```

Step 2 – Use the following command to display queue set 8; ; note, results are only shown for queue set 8

```
ERS5500-24T# show qos queue-set
```

Result:

```
Set Queue        General          Bandwidth Absolute  Bandwidth  Service  Size
ID   ID        Discipline          (%)    Bandwidth Allocation  Order  (Bytes)
                                   (Kbps)

___ _____ _____________________ _________ _________ __________ _______ _______
8   1     Priority Queuing      100       0         Relative   1       49152
8   2     Weighted Round Robin  41        0         Relative   2       47104
8   3     Weighted Round Robin  19        0         Relative   2       45056
8   4     Weighted Round Robin  13        0         Relative   2       43008
8   5     Weighted Round Robin  11        0         Relative   2       39936
8   6     Weighted Round Robin  8         0         Relative   2       36864
8   7     Weighted Round Robin  5         0         Relative   2       33792
8   8     Weighted Round Robin  3         0         Relative   2       30720
```

12.8 Configuration Example 7 – Interface Shaping

In this configuration example, we wish to add port shaping to port 8 and set the shaped rate to 40 Mbps. Also, we wish to use the maximum bucket size (burst duration) available of 512M.

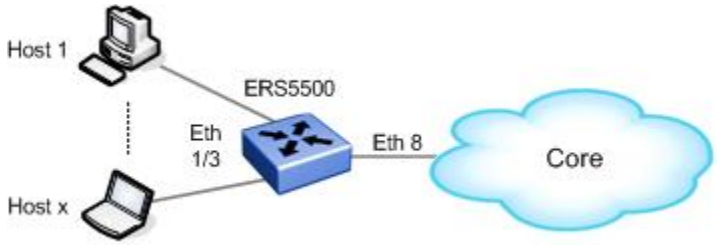

Figure 9: Port Shaping Example

To add port shaping to port 8, please enter the following commands:

12.8.1.1 Enable Shaping on Port 8

As mentioned in section 5.3, if you do not specify maximum burst duration, the maximum bucket size will automatically be configured. For a 10/100 Mbps or 1 GigE port, the value will be 524,288 bytes. Hence, it does not matter what value you enter as the max-burst-rate as long as it is greater than the shaped-rate.

ERS5500 Step 1 – Configure port 8 with a committed shape rate of 40 Mbps and a burst rate of 50 Mbps

```
ERS5500-24T(config)#interface fastEthernet all
ERS5500-24T(config-if)#qos if-shaper port 8 shape-rate 40000 max-burst-rate 50000
ERS5500-24T(config-if)#exit
```

12.8.2 Verify Operations

12.8.2.1 Verify Shape Rate Configuration

Step 1 –View the shape rate configured on port 8

```
ERS5500-24T#show qos if-shaper port 8
```

Result:

```
    Unit Port IfIndex       Name          Rate    Burst
                                                  Size
                                          (Kbps)  (Bytes)

____ ____ _______ _________________ _______ _______
1    8    8                        40000    524288
```

13. Software Baseline

All configuration examples are based on software release 5.1.

14. Reference Documentation

Document Title	Publication Number	Description
Configuration - Quality of Service	NN47200-504 (217466-C)	Nortel Ethernet Routing Switch 5500 Series updated for software release 5.1

Contact us

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact Nortel Technical Support. To obtain contact information online, go to www.nortel.com/contactus.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to www.nortel.com/erc.