Overview

QoS has been enhanced to be more efficient in later code. To take advantage of some new QoS features please see the descriptions below.

Description

The following are additional enhancements made in code build 5.1.4.113r03 and 5.1.5.398r01 and above. It is recommended to use the latest 5.1.4r03 or 5.1.5r01 or above when using the features below. Contact customer support if there are any questions. The features below only apply to the 7700/7800 and the 8800.

Early drop function for tcp/udp ports which helps prevent PCAM entry exhaustion when subjected to attack which targets a specific TCP port.

This feature is enabled on a per slice/NI (or vlan) basis. All of the traffic that matches the tcp/udp port will be dropped.

The keyword word "DropServices" must be used for the feature above to work.
To do this make a policy that specifies where to do the "DropServices". QOS will accept two kinds of policies using the DropServices group:

policy condition c1 source vlan <vlan> service group DropServices
policy condition c2 source port group <portgroup> service group DropServices

This allows two conditions that apply to Drop Services one based on source physical ports and a second based on the source VLAN. To apply Drop services to a particular set of port groups use a source port group condition. To exempt certain VLANs on those physical ports then assign exception VLANs using the condition source VLAN. For example:
> policy rule r1 condition c1 action drop
> policy rule r2 condition c2 action accept

The restrictions are:
When using a port or port group with the DropServices, only a drop action can be used.
When using a source VLAN with the DropServices, only an allow action can be used.
The accept rule takes precedence over the drop rule. The DropServices rules are essentially the highest precedence rule when a magic service group is present. Other types of qos policies can not be implemented to allow packets that already match specified DropServices.

Here is an example of implementation on a per slice basis-

policy service t135 destination tcp port 135
policy service t139 destination tcp port 139
policy service t445 destination tcp port 445
policy service t1025 destination tcp port 1025
policy service t2745 destination tcp port 2745
policy service t3127 destination tcp port 3127
policy service t5000 destination tcp port 5000
policy service t6129 destination tcp port 6129
policy service u135 destination udp port 135

policy service group DropServices t135 t139 t445 t1025 t2745 t3127 t5000 t6129 u135

policy port group g1 1/1-12 2/1-12 3/1-12 4/1-12 5/1-12 11/1-2 12/1-2 13/1-2 (these are the ingress NI's where you want the traffic dropped)

policy condition c1 source vlan 2 service group DropServices
policy condition c2 source port group g1 service group DropServices

policy action drop disposition deny
policy action allow

policy rule r1 condition c1 action allow
policy rule r2 condition c2 action drop

qos apply

Preventing users from spoofing addresses that are not on the local network.

Users could be identified by the source MAC address, but this address is easily spoofed. The one thing that users cannot spoof and is easily identifiable is the port on which the user is entering the switch/router. User ports should never legitimately have a source IP address that is not in the defined subnet for that port as opposed to router ports, which could. User ports are defined in a QOS port group rule using the keyword “UserPorts”

Example:
policy port group UserPorts <slot>/<port-port>
For example:
policy port group UserPorts 2/5 3/1-10
Defines ports 2/5 and ports 1 thru 10 on slot 3 as user ports.

“UserPorts” is a magic port group. The "UserPorts" groups works like any other port group as far as the CLI is concerned. DHCP packets are never checked for spoofing since the will typically have the source IP set to 0.0.0.0.
There is no command for turning on spoofing prevention, all ports that are identified as “UserPorts” will automatically do spoofing prevention.
If QOS is not enabled on the switch, no spoofing prevention will be done.
A count is kept of packets dropped because of spoofing as seen at the bottom of the “show ip traffic” output. This count does not indicate all packets dropped, but will give an idea of what addresses are spoofing.

Preventing User pings and reducing DOS exposure from Pings.

In order to reduce Ping traffic on a network without excessively impacting NI traffic a ping drop QOS command is defined. The effect of this command is that an NI will drop all ICMP echo request and ICMP echo reply packets.
The example below will drop all ICMP echo request/reply on that VLAN.

Example configuration:
policy condition ping10 source vlan 10 ip protocol 1
policy action drop disposition drop
policy rule noping10 condition ping10 action drop

Combined Example of QoS Features

Here is an example of the above rules combined for the 7700/7800 and 8800.
This would accomplish the following items -

1. Drop icmp for vlan's 2,3 and 4
2. Early drop for TCP ports 69,445, and 4444 - the IP flows would not be learned.
3. Drop TCP/UDP ports 135,137,138 and 139 - the IP flows will be learned as an HRE PCAM entry.
4. Antispoofing on the specified UserPorts
5. Allows communication to server IP's 169.10.64.10, and 169.10.64.11 for TCP/UDP ports 135, 137, 138, and 139, but drops traffic to these ports when not communicating with these IP's.
6. Allows all traffic on vlan 2 except icmp.

```
policy service t135 destination tcp port 135
policy service t137 destination tcp port 137
policy service t138 destination tcp port 138
policy service t139 destination tcp port 139
policy service t4444 destination tcp port 4444
policy service t445 destination tcp port 445
policy service t69 destination tcp port 69
policy service u135 destination udp port 135
policy service u137 destination udp port 137
policy service u138 destination udp port 138
policy service u139 destination udp port 139
policy service group DropServices t4444 t445 t69
policy service group tcp_udp_group t135 t137 t138 t139 u135
policy service group tcp_udp_group u137 u138 u139
policy network group internal_network 169.10.64.0 mask 255.255.240.0
169.10.32.0 mask 255.255.224.0 169.10.80.0 mask 255.255.240.0 169.10.176.0
mask 255.255.240.0 169.10.160.0 mask 255.255.240.0
policy network group servers 169.10.64.10 169.10.64.11
policy port group g1 1/1-12 2/1-12 3/1-12 4/1-12 5/1-12
policy port group g1 11/1-2 12/1-2 13/1-2
policy condition allow_vlan source vlan 2 service group DropServices
policy condition early_drop source port group g1 service group DropServices
policy condition tcp_udp_drop destination network group internal_network
service group tcp_udp_group
policy condition icmp2 source vlan 2 ip protocol 1
policy condition icmp3 source vlan 3 ip protocol 1
policy condition icmp4 source vlan 4 ip protocol 1
policy condition servers source network group servers
policy condition users_to_servers destination network group servers service
group tcp_udp_group
policy action allow
policy action drop disposition drop
policy rule servers precedence 200 condition servers action allow
policy rule users_to_servers precedence 200 condition users_to_servers
action allow
policy rule allow_vlan precedence 100 condition allow_vlan action allow
policy rule early_drop condition early_drop action drop
policy rule tcp_udp_drop condition tcp_udp_drop action drop
policy rule vlan2 condition icmp2 action drop
policy rule vlan3 condition icmp3 action drop
policy rule vlan4 condition icmp4 action drop
qos apply
```

If you have any questions, the following contact information should be used:

Web Links
Customers: http://eservice.ind.alcatel.com/
EMEAI Business Partners: http://www.businesspartner.alcatel.com/

Email
support@ind.alcatel.com
EMEAI Business Partners: mailto:support.center@alcatel.fr

Phone
North America 1 800-995-2696
Latin America 1 877-919-9526
Europe (EMEAI) +33-388-55-69-04
Asia Pacific +65-394-7933
Other International +1-818-878-4507

Alcatel customers under maintenance contracts have access to troubleshooting tools on the Intranet found at the web addresses listed above.