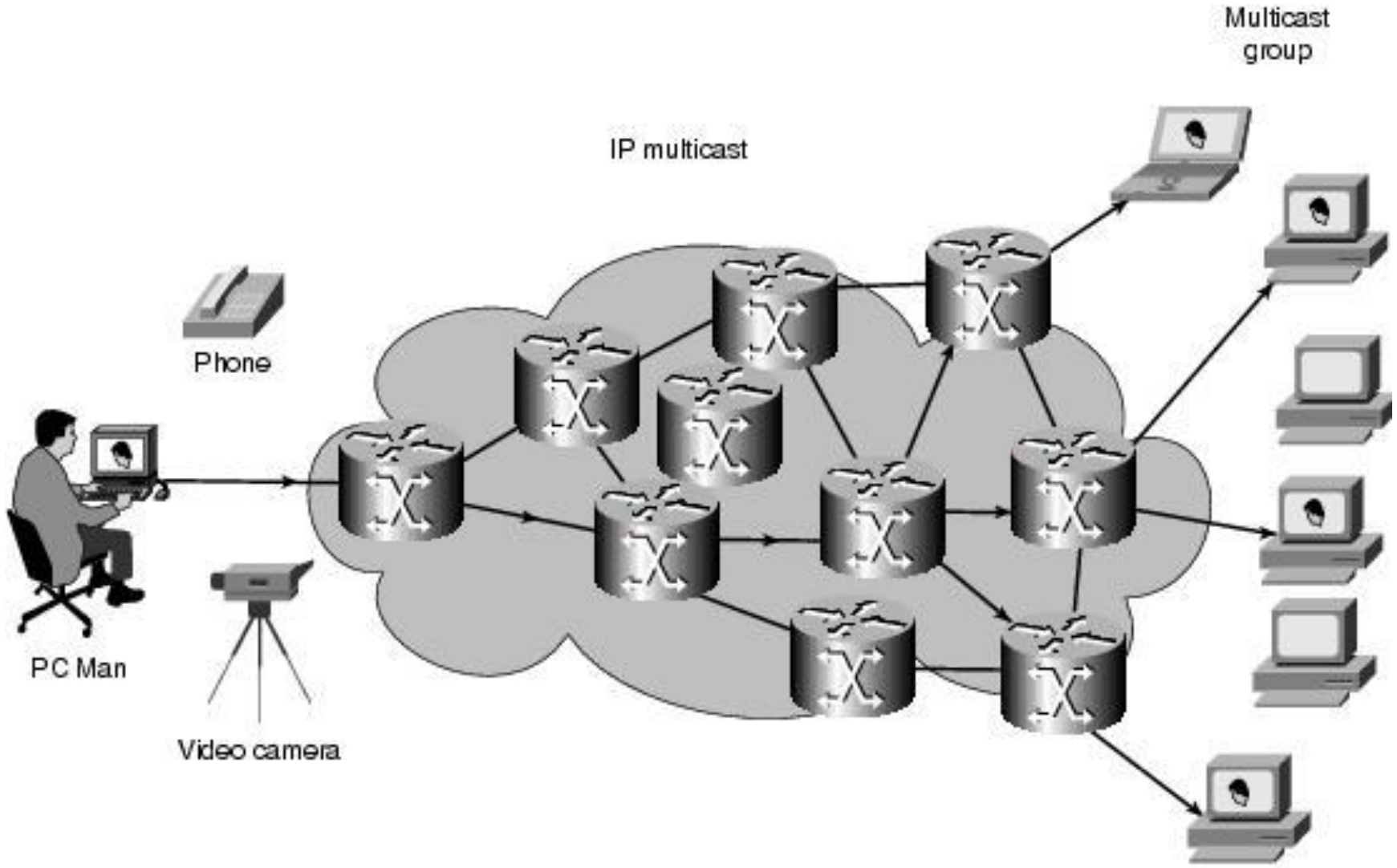
Multicasting


Multicast
group
IP multicast
Phone
PC Man
Video camera

BASE

- Базируется на концепции групп
- Группа не имеет физических и географических ограничений
- Группа заинтересована в получении определенного потока данных
- Хост должен подключится к группе с помощью специального протокола (IGMP)
- Хост должен быть членом группы чтобы получать поток.

Addressing

- The Internet Assigned Numbers Authority (IANA) controls the assignment of IP multicast addresses. It has assigned the old Class D address space to be used for IP multicast. This means that all IP multicast group addresses will fall in the range of 224.0.0.0 to 239.255.255.255.

- Note: This address range is only for the group address or destination address of IP multicast traffic. The source address for multicast datagrams is always the unicast source

Reserved Link Local Addresses

- The IANA has reserved addresses in the 224.0.0.0 through 224.0.0.255 to be used by network protocols on a local network segment.

224.0.0.1 All systems on this subnet

224.0.0.2 All routers on this subnet

224.0.0.5 OSPF routers

224.0.0.6 OSPF designated routers

224.0.0.12 DHCP server/relay agent

Address types

- Globally Scoped Address

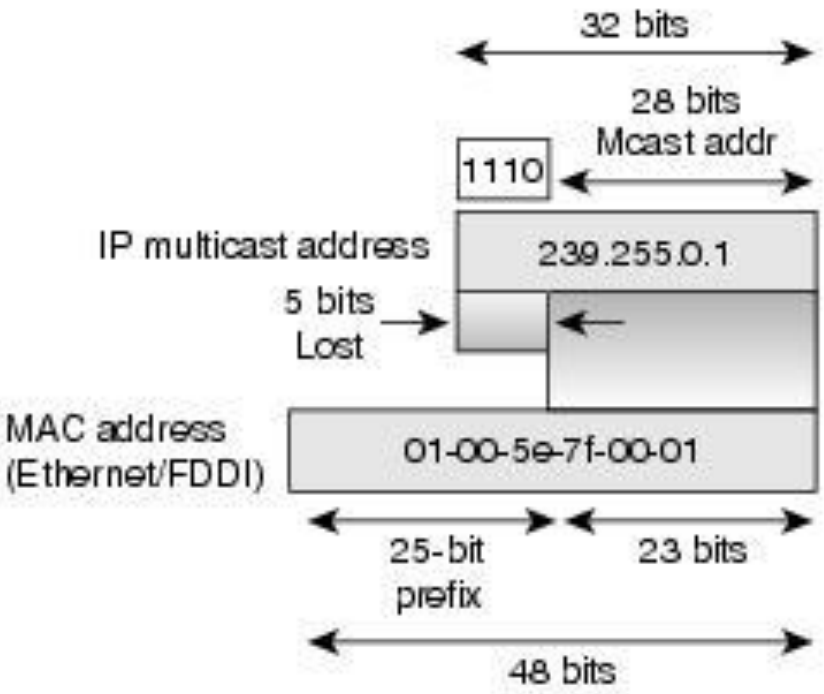
The range of addresses from 224.0.1.0 through 238.255.255.255 are called globally scoped addresses. They can be used to multicast data between organizations and across the Internet.

- Limited Scope Addresses

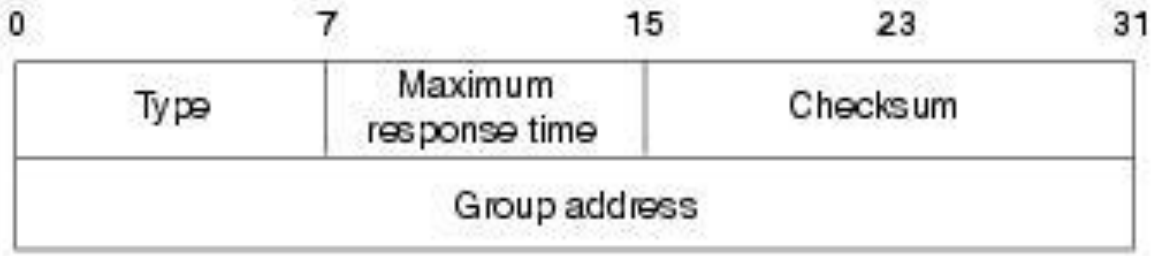
The range of addresses from 239.0.0.0 through 239.255.255.255 contains limited scope addresses or administratively scoped addresses.

Layer 2 Multicast Addresses

- Ethernet MAC addresses to be 0100.5e00.0000 through 0100.5e7f.ffff
- The mapping places the lower 23 bits of the IP multicast group address into these available 23 bits in the Ethernet address


32 bits
28 bits
Mcast addr
1110
IP multicast address
239.255.0.1
5 bits
Lost
MAC address
(Ethernet/FDDI)
01-00-5e-7f-00-01
25-bit
prefix
23 bits
48 bits

IGMP. IGMP Version 2



Membership query

Version 1 membership report

Version 2 membership report

Leave group

L3 Multicasting

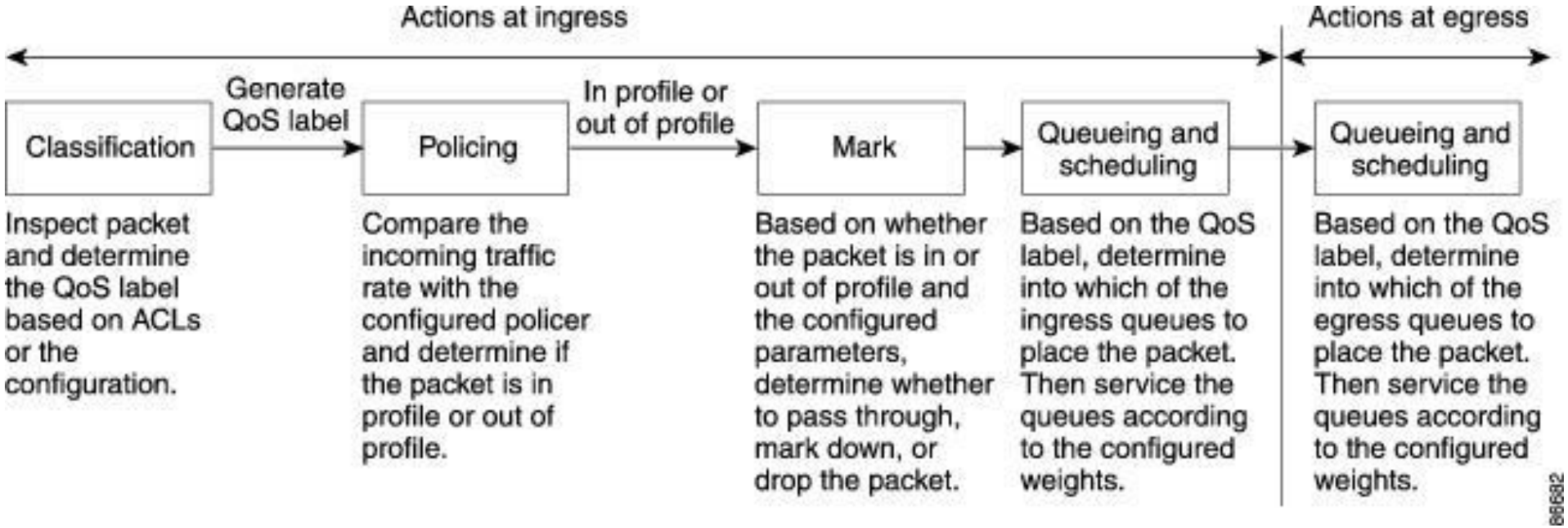
- PIM SM (sparse mode)
- PIM DM (dense mode)

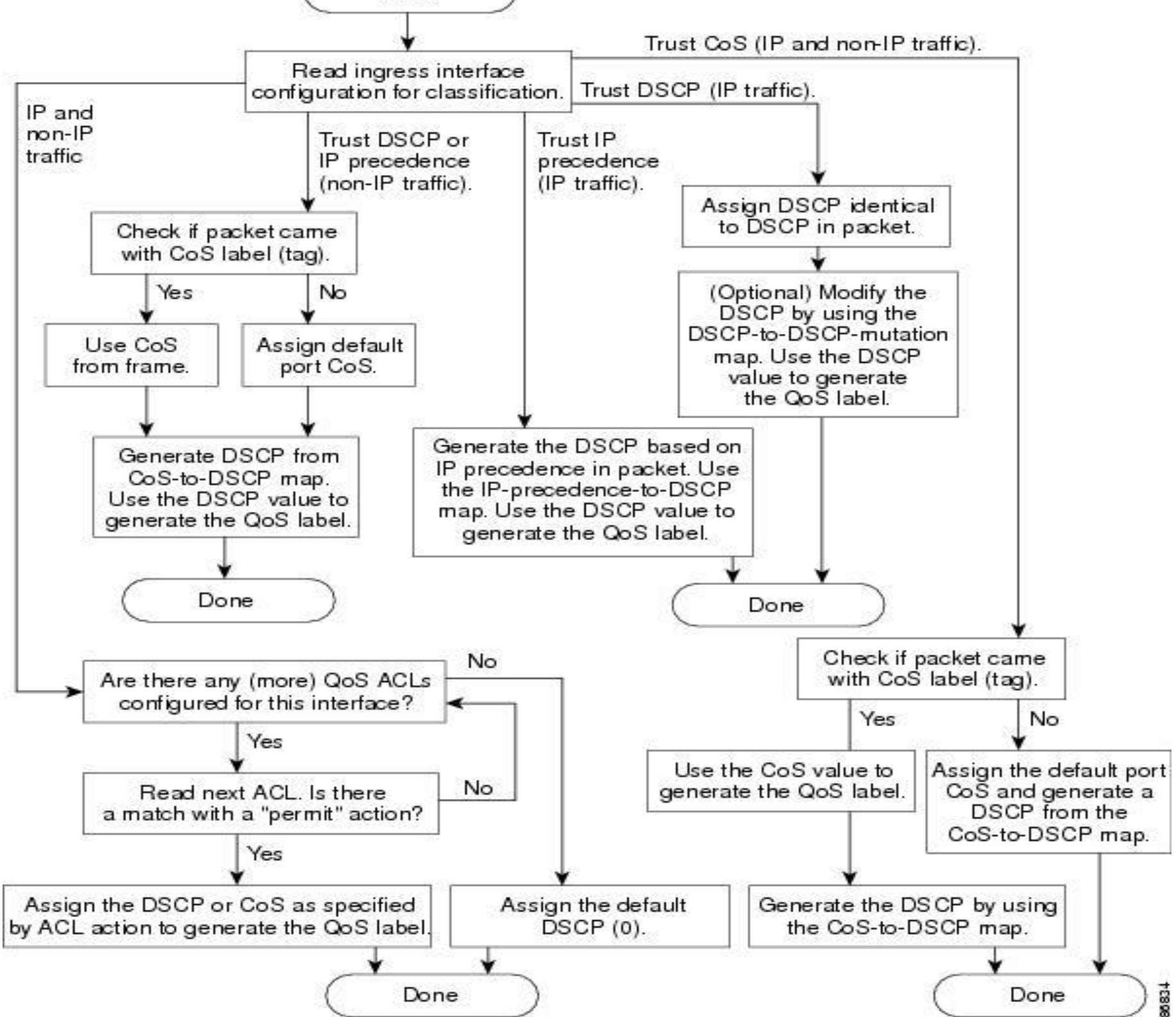
- ip multicast-routing
- dyn3(config-if)# ip pim sparse-mode[dense-mode]
- dyn4(config)# ip pim rp-address 4.4.4.4 1 override
- dyn4(config)# access-list 1 permit 224.1.1.1

Base troubleshooting

	Source	Network	Receivers
Signaling	NA	Check Network Signaling	Check Receiver Signaling
Packet Flow	Check Source Packet Flow	Check Network Packet Flow	Check Receiver Packet Flow

QoS


Actions at ingress
Actions at egress
Generate QoS label
In profile or out of profile
Classification
Policing
Mark
Queueing and scheduling
Queueing and scheduling
Inspect packet and determine the QoS label based on ACLs or the configuration.
Compare the incoming traffic rate with the configured policer and determine if the packet is in profile or out of profile.
Based on whether the packet is in or out of profile and the configured parameters, determine whether to pass through, mark down, or drop the packet.
Based on the QoS label, determine into which of the ingress queues to place the packet. Then service the queues according to the configured weights.
Based on the QoS label, determine into which of the egress queues to place the packet. Then service the queues according to the configured weights.
86682


Read ingress interface configuration for classification.
Trust CoS (IP and non-IP traffic).
Trust DSCP (IP traffic).
IP and non-IP traffic
Trust DSCP or IP precedence (non-IP traffic).
Trust IP precedence (IP traffic).
Check if packet came with CoS label (tag).
Yes
No
Use CoS from frame.
Assign default port CoS.
Generate DSCP from CoS-to-DSCP map. Use the DSCP value to generate the QoS label.
Done
Assign DSCP identical to DSCP in packet.
(Optional) Modify the DSCP by using the DSCP-to-DSCP-mutation map. Use the DSCP value to generate the QoS label.
Generate the DSCP based on IP precedence in packet. Use the IP-precedence-to-DSCP map. Use the DSCP value to generate the QoS label.
Done
Are there any (more) QoS ACLs configured for this interface?
No
Yes
Read next ACL. Is there a match with a "permit" action?
No
Yes
Assign the DSCP or CoS as specified by ACL action to generate the QoS label.
Assign the default DSCP (0).
Done
Check if packet came with CoS label (tag).
Yes
No
Use the CoS value to generate the QoS label.
Assign the default port CoS and generate a DSCP from the CoS-to-DSCP map.
Generate the DSCP by using the CoS-to-DSCP map.
Done
86834