Classification and Marking

- For a router or switch to give a particular level of service to a type of traffic, it has to recognise that traffic first
- Common ways to recognise the traffic are by COS (Class of Service) marking, DSCP (Differentiated Service Code Point) marking, an Access Control List, or NBAR (Network Based Application Recognition)

Layer 2 Marking - CoS Class of Service

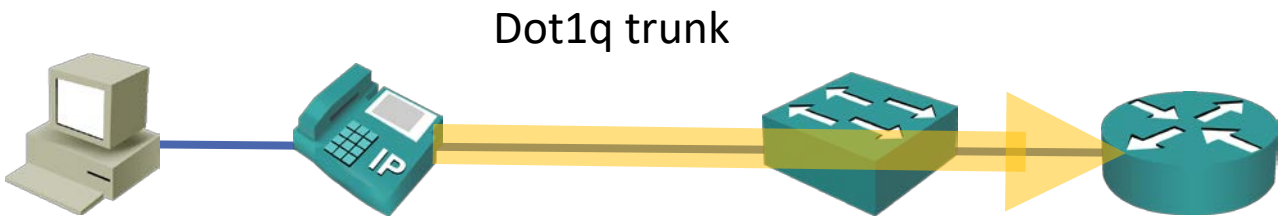
- There is a 3 bit field in the Layer 2 802.1q frame header which is used to carry the CoS QoS marking
- A value of 0 – 7 can be set. The default value is 0 which is designated as Best Effort traffic
- CoS 6 and 7 are reserved for network use
- IP phones mark their call signalling traffic as CoS 3 and their voice payload as CoS 5

Layer 3 Marking - DSCP

- The ToS Type of Service byte in the Layer 3 IP header is used to carry the DSCP QoS marking
- 6 bits are used which gives 64 possible values. The default value is 0 which is designated as Best Effort traffic
- IP phones mark their call signalling traffic as 24 (CS3) and their voice payload as 46 (EF)
- There are standard markings for other traffic types, such as 26 (AF31) for mission critical data, and 34 (AF41) for SD video

The Trust Boundary

- The switch should be configured to trust markings from the IP phone and pass them on unchanged, but mark traffic from the PC down to CoS 0 and DSCP 0



VLAN 20
10.10.20.10

VLAN 10
10.10.10.10

L2	L3	L4	L5	L6	L7
Src MAC Dst MAC CoS 5	Src IP Dst IP DSCP EF	UDP Port No.			

Quality Requirements for Voice and Video

- Voice and video endpoints mark their own traffic with a DSCP value
- If you want to give a particular quality of service to another application running between a workstation and a server, the endpoints will typically be unable to mark their own traffic

Recognising Traffic with an ACL

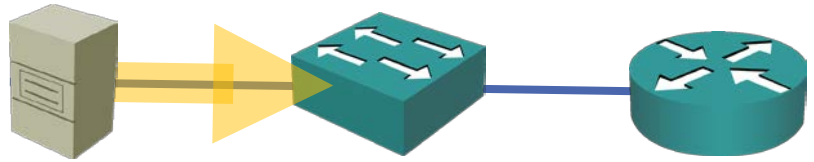
- An Access Control List can be used to recognise traffic based on its Layer 3 and Layer 4 information
- For example SSH traffic going to and from the router 10.10.100.10 on TCP port number 22

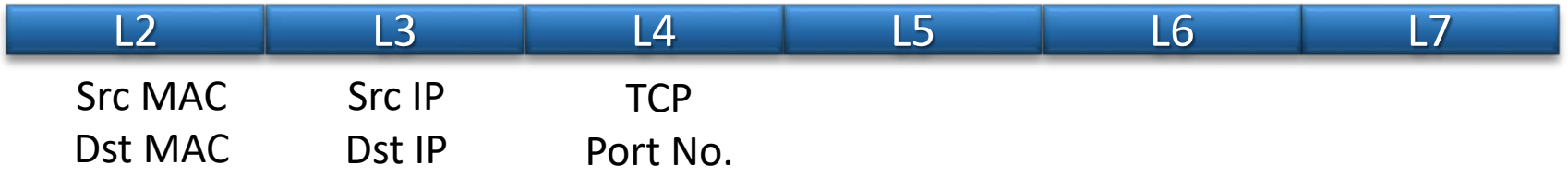
Recognising Traffic with NBAR

- NBAR (Network Based Application Recognition) can be used to recognise traffic based on its Layer 3 to Layer 7 information
- Signatures can be downloaded from Cisco and loaded on your router which recognise well known applications

Classification and marking

- DSCP is the preferred classification and marking method because the router can very quickly gather the information from a single byte in the IP header
- If using another method such as an ACL or NBAR, this should be done as close to the source as possible and then a DSCP value added





Classification and marking

- DSCP is the preferred classification and marking method because the router can very quickly gather the information from a single byte in the IP header
- If using another method such as an ACL or NBAR is being used, this should be done as close to the source as possible and then a DSCP value added