# **Traditional vs Coverged Networks**

* On old traditional networks, data, voice and video had their own separate network infrastructure and did not impact each other
* On modern networks, data, voice and video run over the same shared infrastructure
* This enables cost savings and advanced features for voice and video
* Data, voice and video are all fighting for the same shared bandwidth

# **Quality Requirements for Voice and Video**

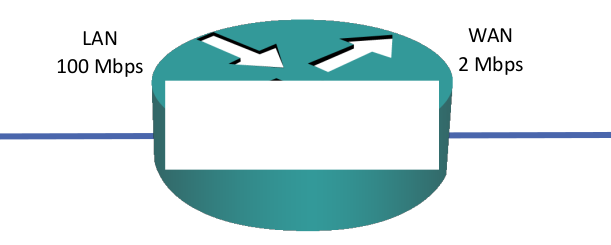
* Voice and traditional standard definition video packets must meet these recommended requirements to be an acceptable quality call:
  + Latency (delay) ≤ 150 ms
  + Jitter (variation in delay) ≤ 30 ms
  + Loss ≤ 1%
* These are one way requirements, meaning a packet sent from a phone in HQ has 150ms to reach the phone in the branch, and vice versa
* HD video has stricter requirements

# **FIFO First In First Out**

* Whenever congestion is experienced on a router or switch, packets are sent out in a First In First Out (FIFO) manner by default
* Congestion can be experienced whenever it is possible for packets to come in quicker than they can be sent out

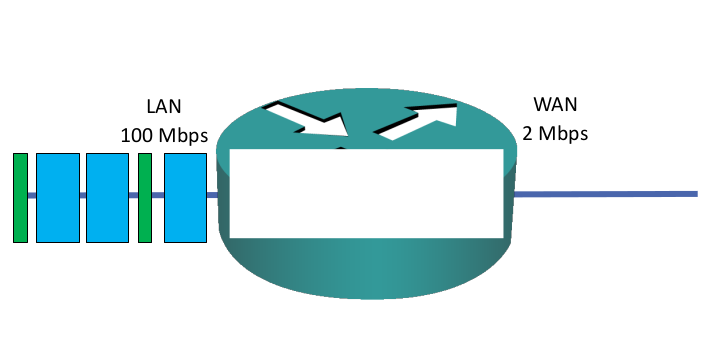
# **Congestion Examples**

* Traffic is going left to right from the HQ to the branch
* The WAN edge router has a FastEthernet interface on the inside LAN interface and an E1 interface on the outside WAN interface

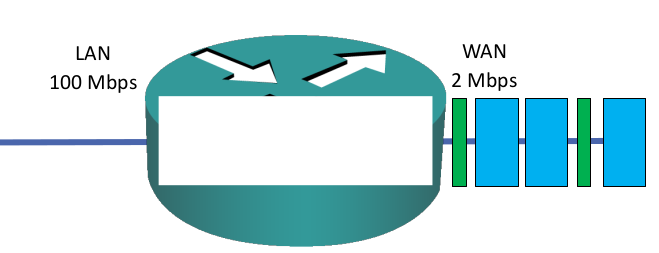


* Traffic destined for the branch comes in on the LAN interface at a rate

lower than 2 Mbps



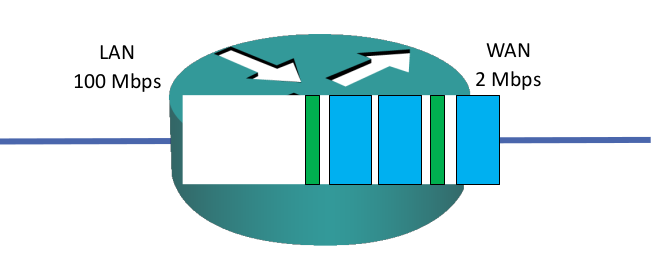
* Packets can be sent out immediately as they arrive – there is no congestion



* Traffic destined for the branch comes in on the LAN interface at a rate

higher than 2 Mbps

* Packets are arriving faster than they can be sent out
* Packets wait in the queue to go out
* Packets are sent out FIFO in the order they were received



# **Effects of Congestion**

* Congestion causes delay to packets as they wait in the queue
* As the size of the queue changes it causes jitter
* There is a limit to the size of the queue. If a packet arrives when the

queue is full the router will drop it

* Voice and video calls (and applications) will be unacceptable quality if they do not met their delay, jitter and loss requirements

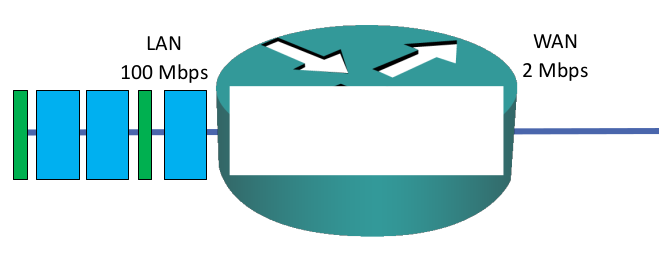
# **How to Mitigate Congestion**

* Add more bandwidth (this costs money)
* Use Quality of Service techniques to give better service to the traffic

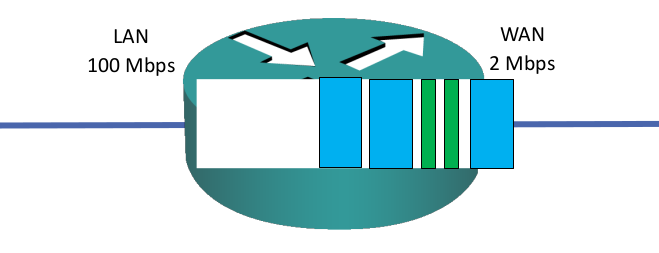
which needs it

# **Congestion Example with QoS Queuing**

* Traffic destined for the branch comes in on the LAN interface at a rate higher than 2 Mbps



* Packets are arriving faster than they can be sent out
* Packets wait in the queue to go out
* The router recognises the voice packets and moves them to the front of
* the queue to minimise their delay



# **Effects of QoS Queuing**

* QoS queuing can reduce latency, jitter and loss for particular traffic
* The original driver for QoS was Voice over IP but it can also be used to give better service to data applications
* If you’re giving one type of traffic better service on the same link you started with, the other traffic types must get worse service
* The point is to give each type of traffic the service it requires
* QoS queuing is not a magic bullet and is designed to mitigate temporary periods of congestion. If a link is permanently congested the bandwidth should be increased

# **Classification and Marking**

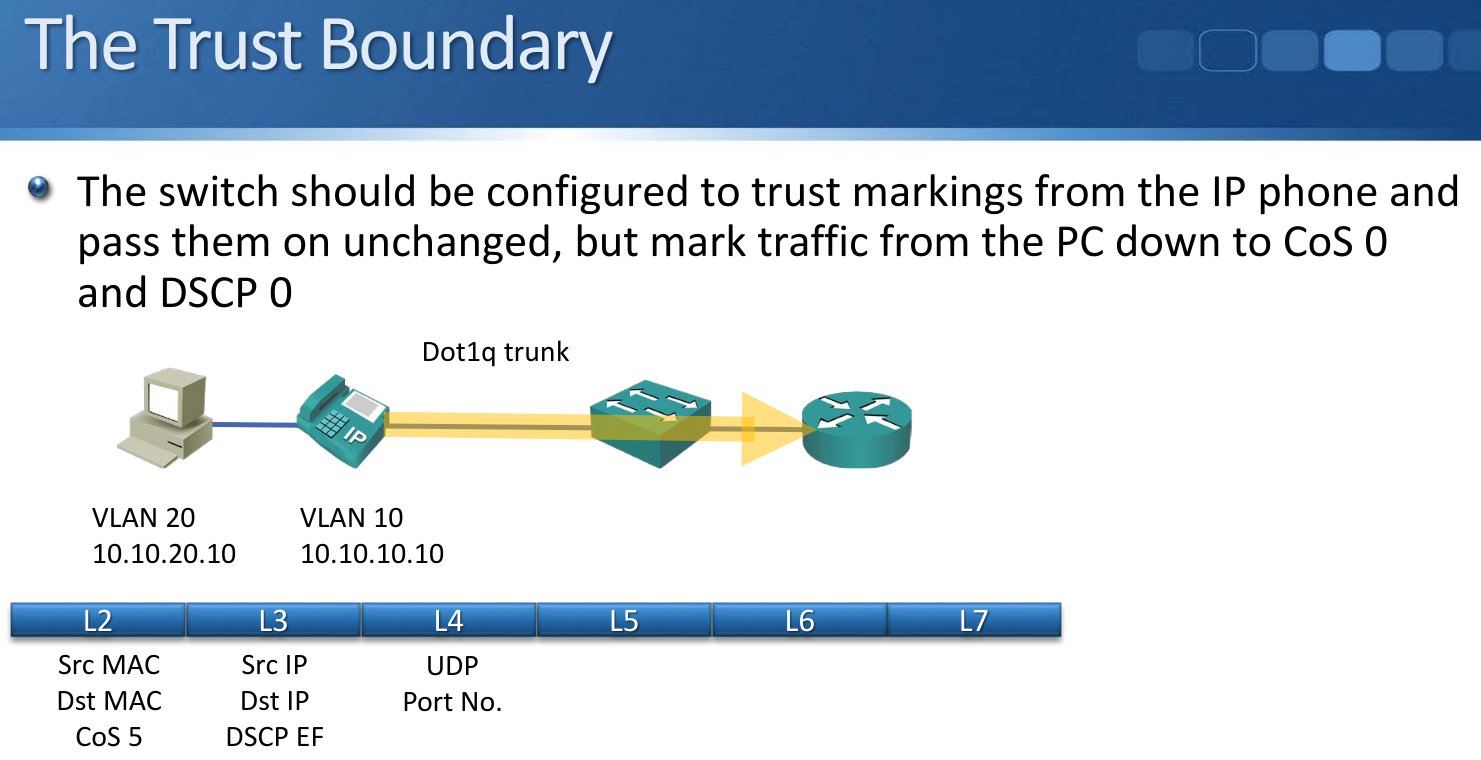
* For a router or switch to give a particular level of service to a type of traffic, it has to recognise that traffic first
* Common ways to recognise the traffic are by COS (Class of Service) marking, DSCP (Differentiated Service Code Point) marking, an Access Control List, or NBAR (Network Based Application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

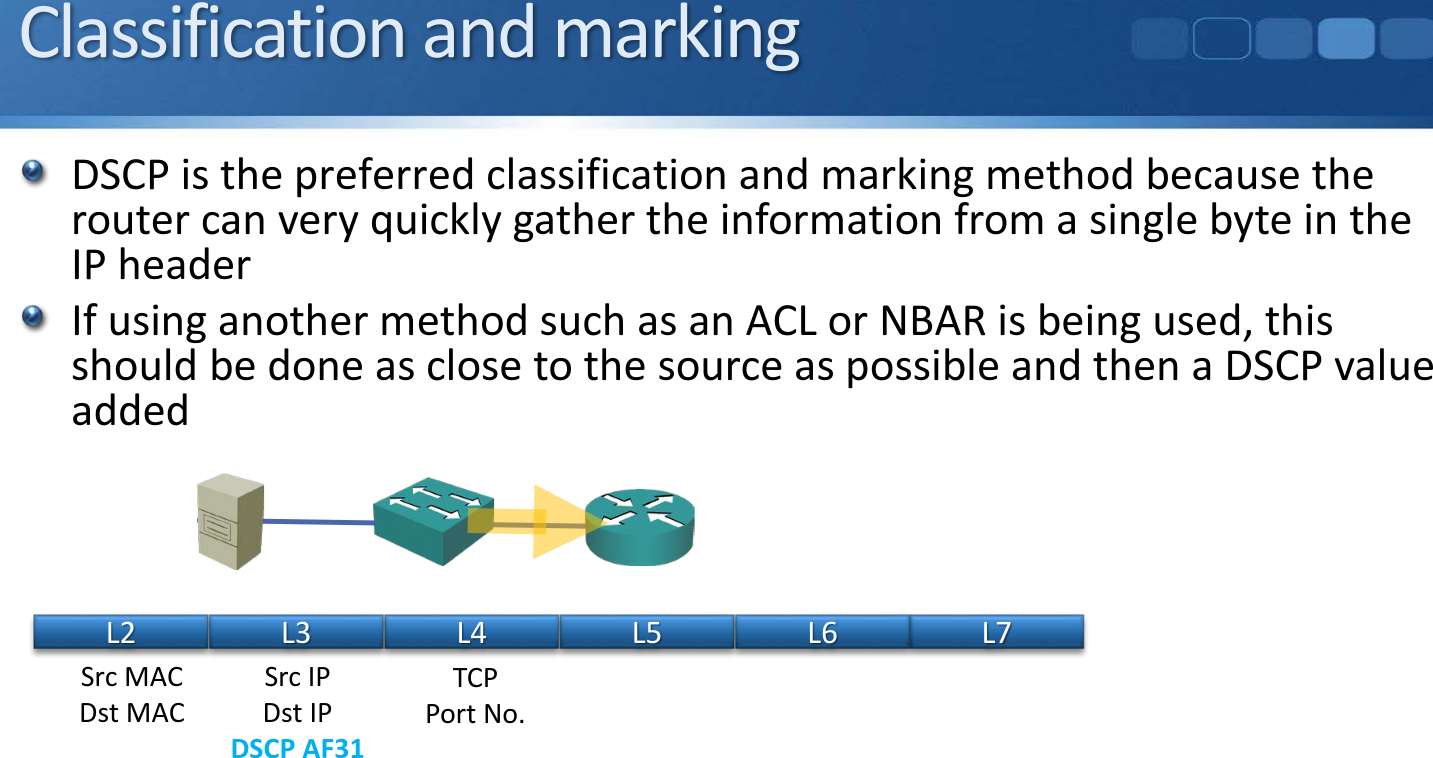


## **Recognising Traffic with an ACL**

* 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

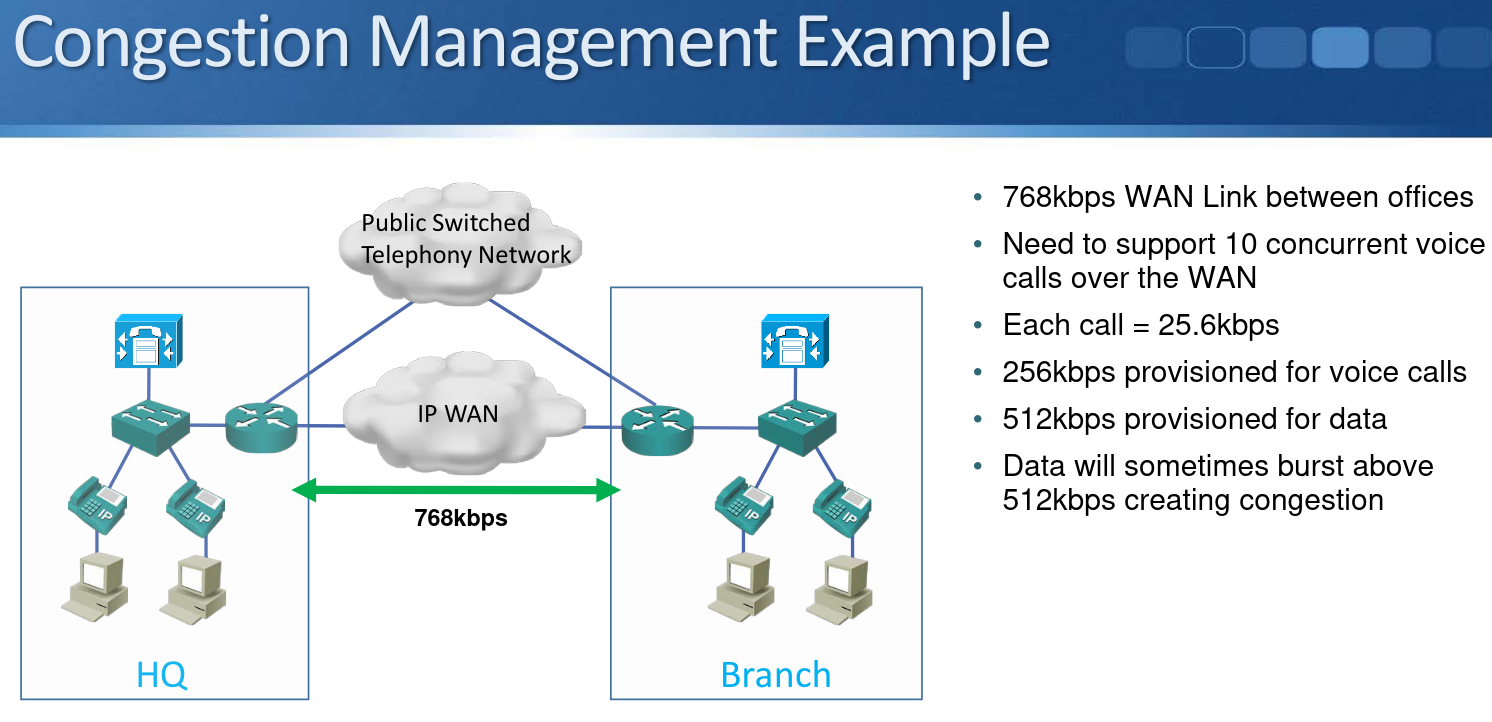


# **Congestion Management**

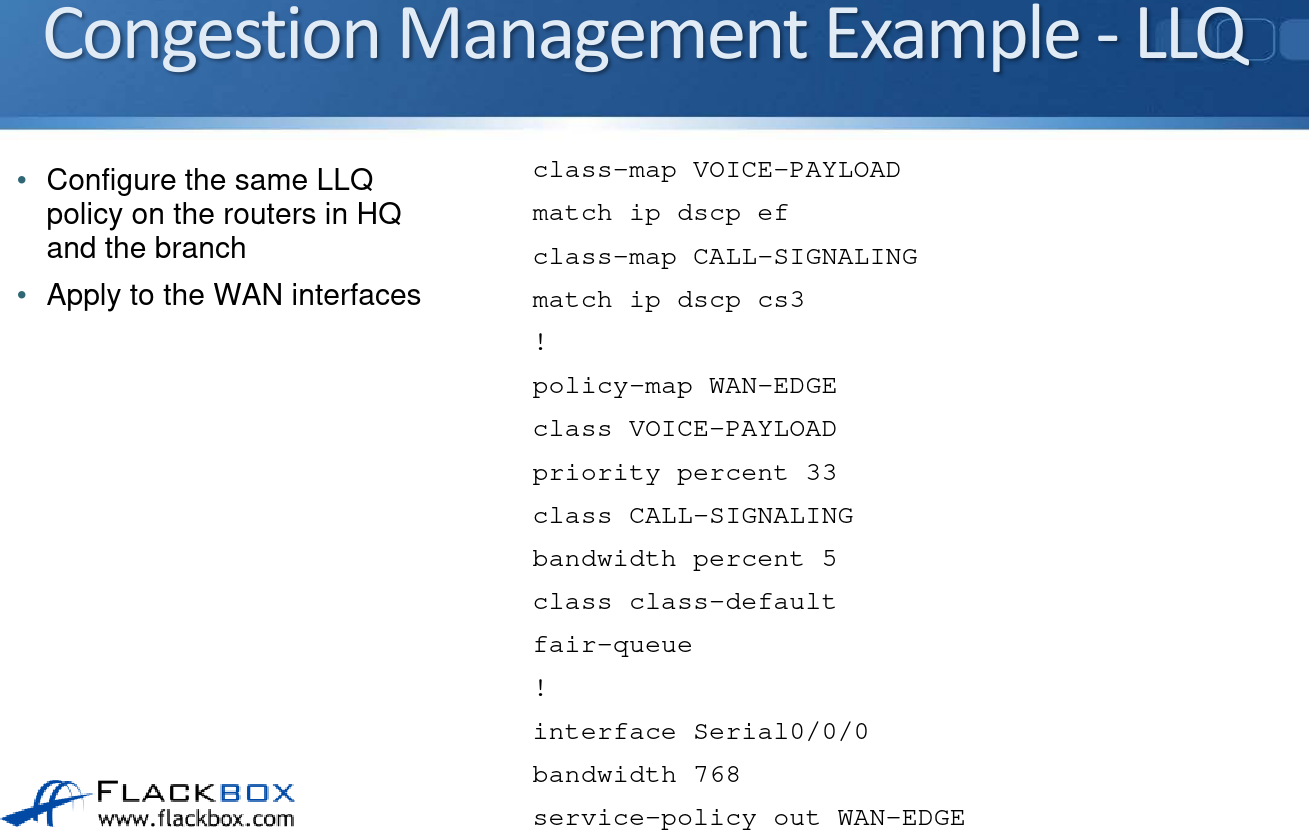
* Queuing can be used to manage congestion on routers and switches
* CBWFQ (Class Based Weighted Fair Queuing) gives bandwidth guarantees to specified traffic types
* LLQ (Low Latency Queuing) is CBWFQ with a priority queue
* Traffic in the priority queue is sent before other traffic

# **MQC Modular QoS CLI**

* Cisco QoS configuration uses the MQC Modular QoS CLI
* It has 3 main sections
* Class Maps define the traffic to take an action on
* Policy Maps take the action on that traffic
* Service Policies apply the policy to an interface

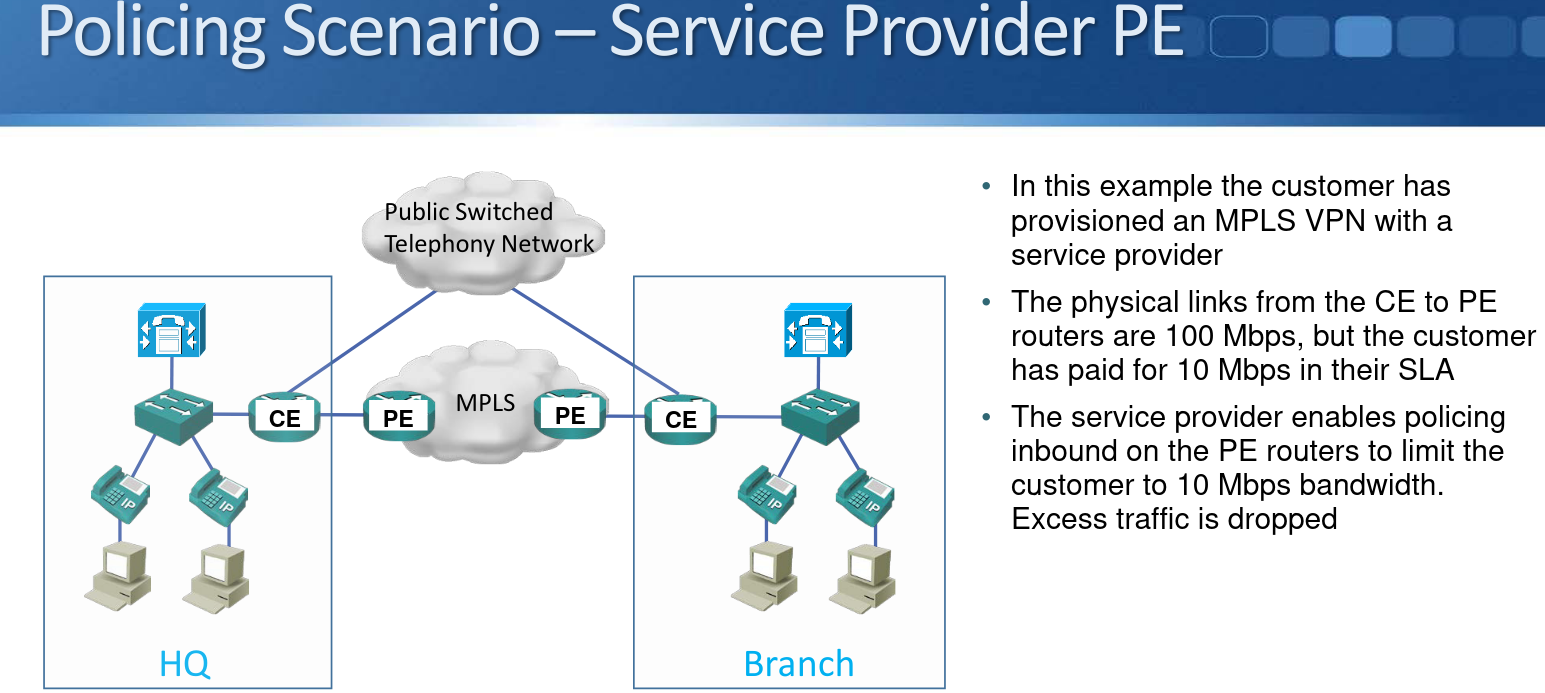


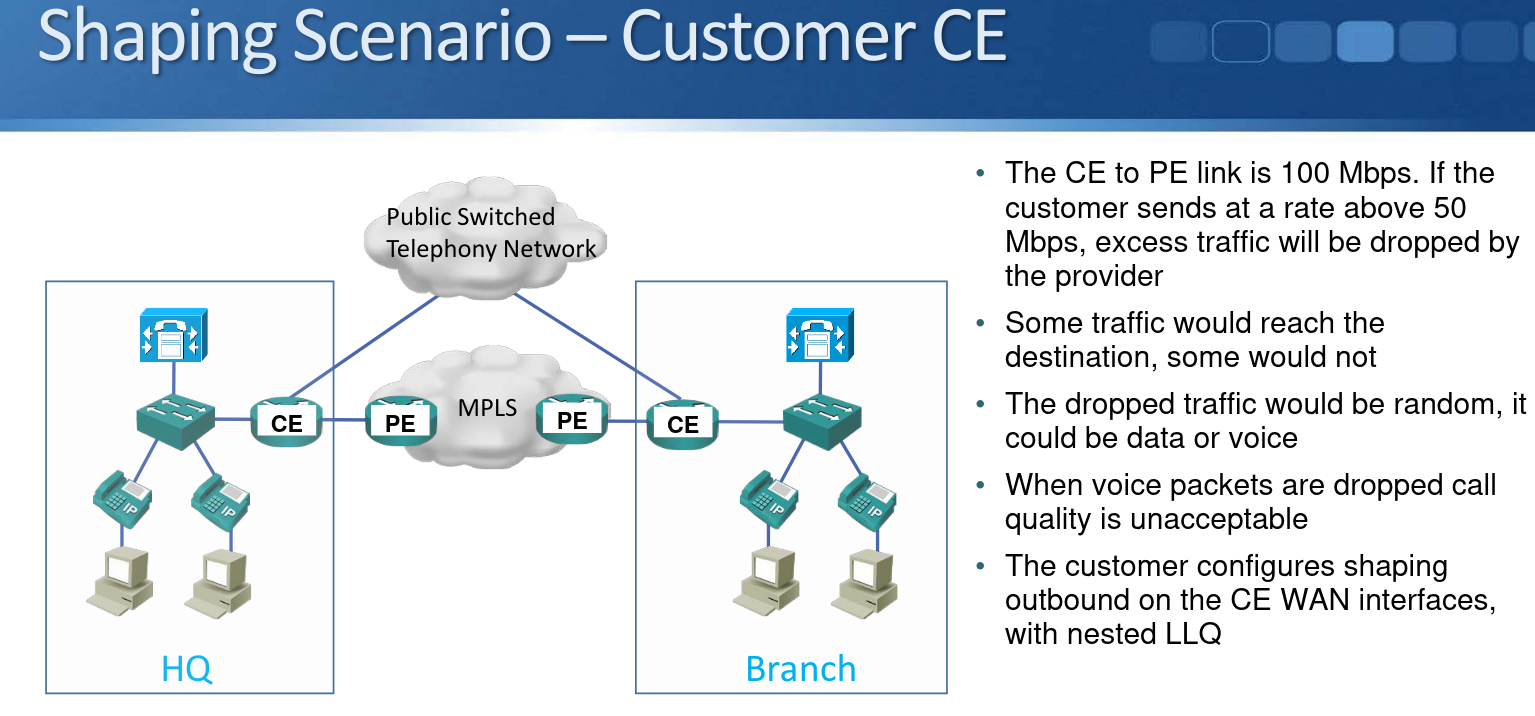
(This config isn’t required on the CCNA)



# **Shaping and Policing**

* Traffic Shaping and Policing can be used to control traffic rate.
* They both measure the rate of traffic through an interface and take an action if the rate is above a configured limit.
* Traffic shaping buffers any excess traffic so the overall traffic stays within the desired rate limit.
* Traffic policing drops or re-marks excess traffic to enforce the specified rate limit.
* Classification can be used to allow different rates for different traffic types.





(This config isn’t required on the CCNA)

