



Quality of Service for Today's Industrial Networks

Henry Martel
Field Applications Engineer

Industrial communications have come a long way in recent years. No longer are the days of Fieldbus cards & serial connectors. Today's industrial networks are intelligent and robust. They can transmit data across high-speed wireless bridges, high-performance industrialized gigabit switches, and backhaul 10-gigabit fiber links.

But this hasn't always been the case. Up until recently, industrial networks were mainly closed-looped networks, consisting of simple communications between integrated digital circuits, microprocessors, and logic controllers. These simplified forms of communication were the industrial industry standards for many years.

However, as advancements in technology and communications were taking place, digital circuits were becoming cumbersome, limiting, and expensive to maintain. The various industrial industries needed faster more robust ways of communicating that would allow for expansion and growth. This eventually led to the introduction of Ethernet technologies into once closed-off digital looped networks.

This improved form of communication was a major leap forward for engineers. This new way of transmitting data gave engineers the ability to expand their once closed-off digital networks and incorporate new features such as remote management and segmentation, as well as PC-based hardware and software into their networks.

Ethernet-based communications were transformative; however, it did present challenges. The IEEE 802.3 standards used in traditional Ethernet communications did not meet the requirements needed for real-time industrial communications. Ethernet TCP was too slow. Its error-checking features that guarantee packet delivery caused latency and couldn't support real-time communications. Ethernet UDP had a much quicker packet delivery than TCP, however, the UDP protocol by design is unreliable and did not provide the guaranteed packet delivery needed for real-time data streams. These lacks of features eventually led to the creation of industrial protocols that could provide guaranteed packet delivery in the sub-milliseconds needed for synchronized industrial communication streams.

Switching technology has also gone through several changes over the years. Hubs and repeaters that once held communications together became obsolete. The lack of quality of

service during data transmissions caused signaling issues and applications would often time out. Carrier Sense Multiple Access with Collision Detection was added to improve data flow, but hub and repeaters eventually fell by the wayside as multilayer switches with advanced feature sets took over. Eventually, industrialized networking equipment came to pass. Designed specifically for industrial environments, these feature-rich, ruggedized networking switches would provide the advanced communications needed for industrial industries.

“Switching technology has also gone through several changes over the years. Hubs and repeaters that once held communication together became obsolete.”

Growth Hurdles

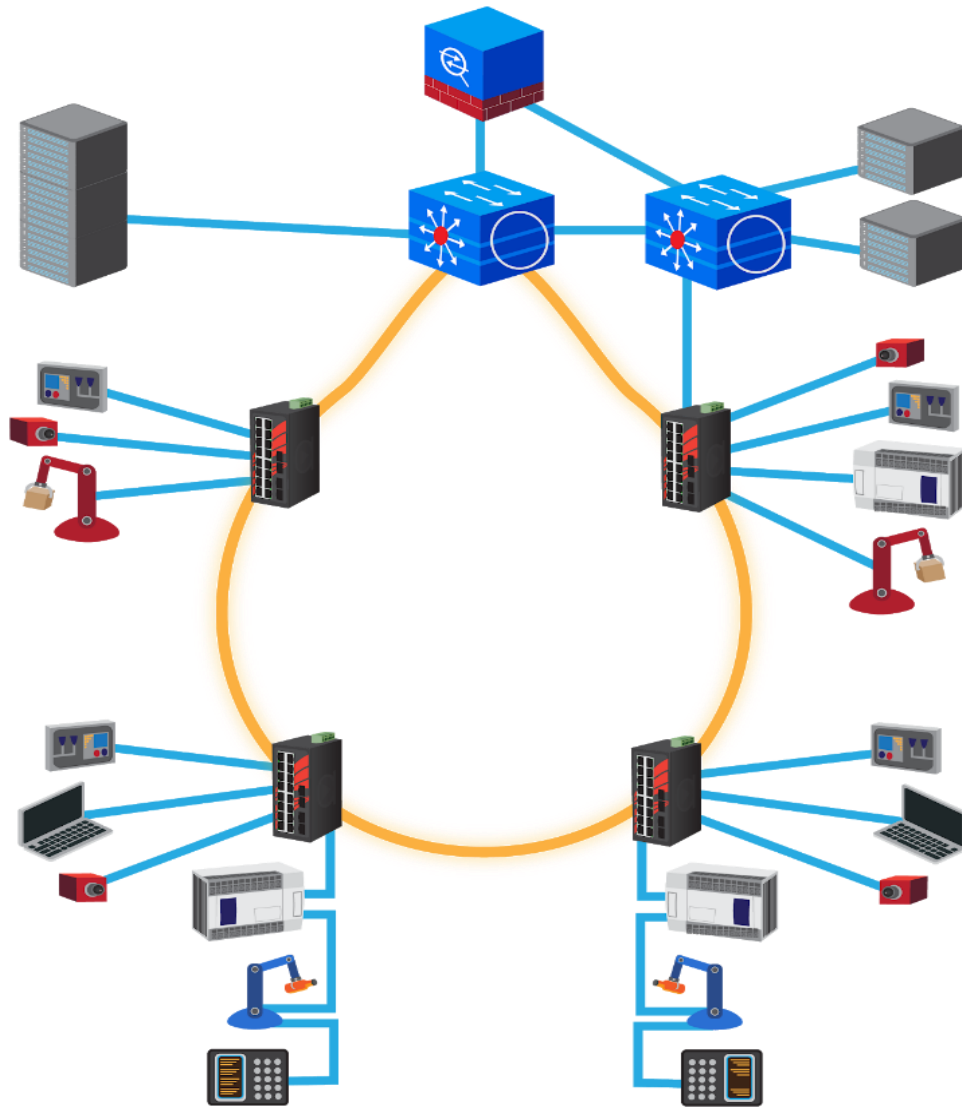
The advancements in switching technologies have really opened up the door for industrial networking. Larger processor chips with increased internal memory have allowed manufacturers to increase data throughput at higher rates. We now see industrial networking switches integrated with 1 gigabit and 10-gigabit switch ports and up to 40-gigabit backplane switching. This increase in switching capabilities has created an explosion of intelligent industrial devices that rely heavily on bandwidth availability.

However, as industrial networks have become sophisticated and more bandwidth dependent devices are brought online, link congestions from oversubscribed switch ports have become a real problem. Engineers are now having to deal with enterprise-class networking issues in their industrial networks. As such, they are reaching into the administrator's tool bag and using management features like Quality of Service (QoS) for network stabilization.

Enterprise Integration

Modernized industrial networks have blurred the lines between the once separated enterprise and industrial network. Now instead of two physically separated networks, enterprise and

industrial networks are virtually separated while being interconnected at the core and distribution levels of the network. To add further complexities, these networks commonly share virtual LAN segments or VLANs that often carry security policies, routing policies, and bandwidth policies with them.



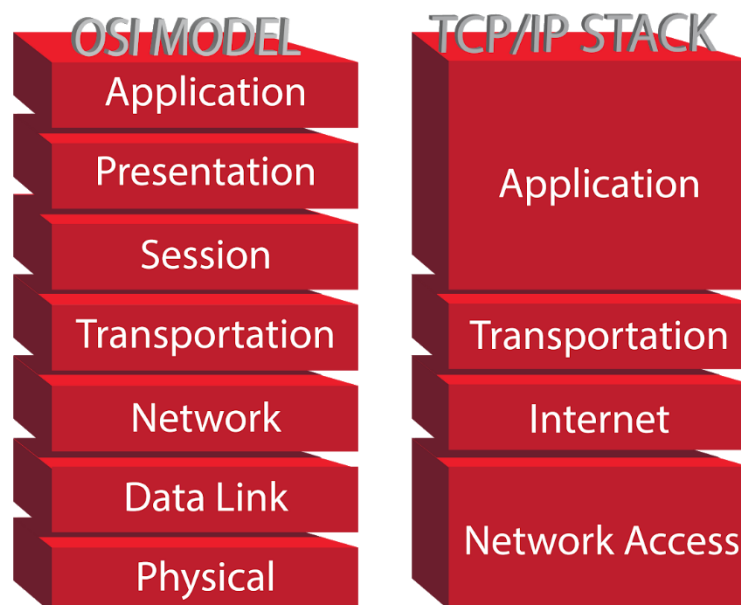
What Can QoS do for Industrial Communications?

Inside your typical network, data-flows or packet transmissions are based on best-effort delivery. Meaning that all transmitted data have the same chances of being delivered and dropped during times of congestion. For non-critical data-flows or traffic, this method of data delivery is adequate. However, certain types of data traffic, such as control and synchronization, have specific time periods for packet delivery.

QoS offers mechanisms for packet prioritization and bandwidth control during times of congestion. These mechanisms apply traffic filters to maintain the quality of service for specific types of data streams such as VoIP and Precision-Time-Protocol.

Understanding QoS

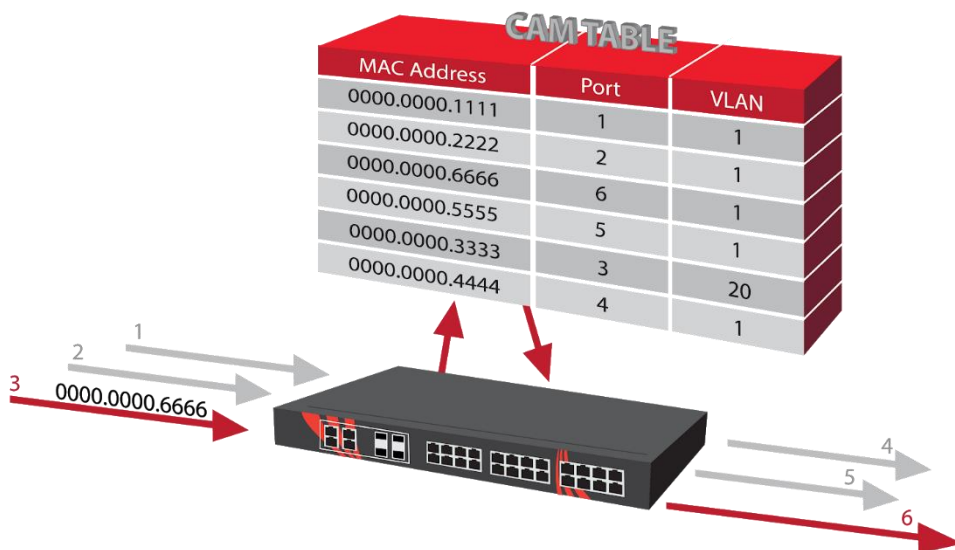
To understand QoS you must first be familiar with the 7-layer OSI model and the 4-layer TCP/IP stack. More importantly, you must understand the layer 2 & 3 functionality of networking in order to create an efficient QoS implementation.



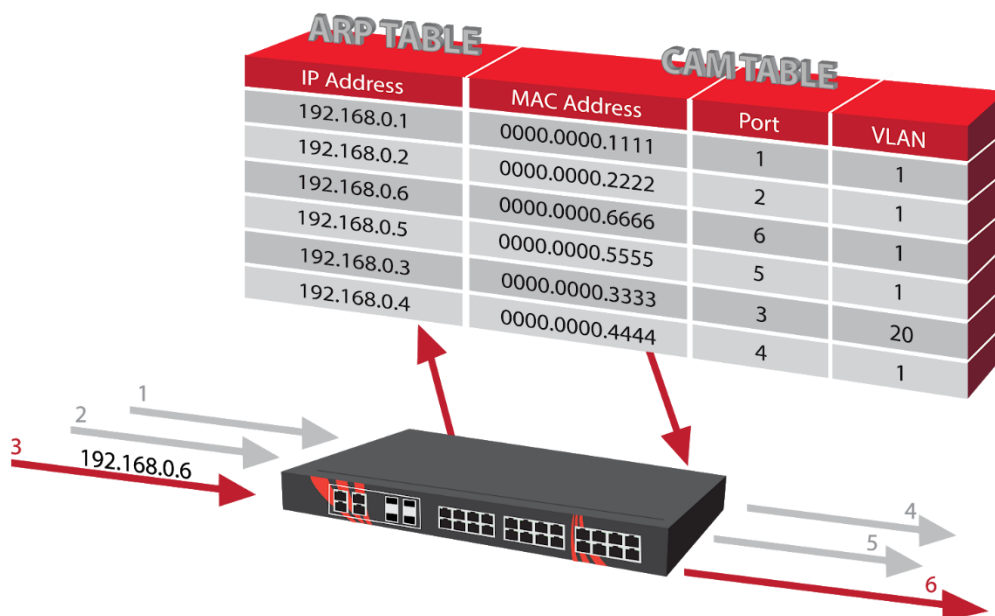
To begin with, layer 2 and layer 3 have different sets of architectures and deal with data streams differently. Layer 2 deals with data streams in terms of frames whereas layer 3 deals with

packets. Layer 2 frames use MAC addresses as source and destinations to forward frames and layer 3 packets use IP addresses for the same purposes.

Layer 2: Packet Forwarding



Layer 3: Packet Forwarding



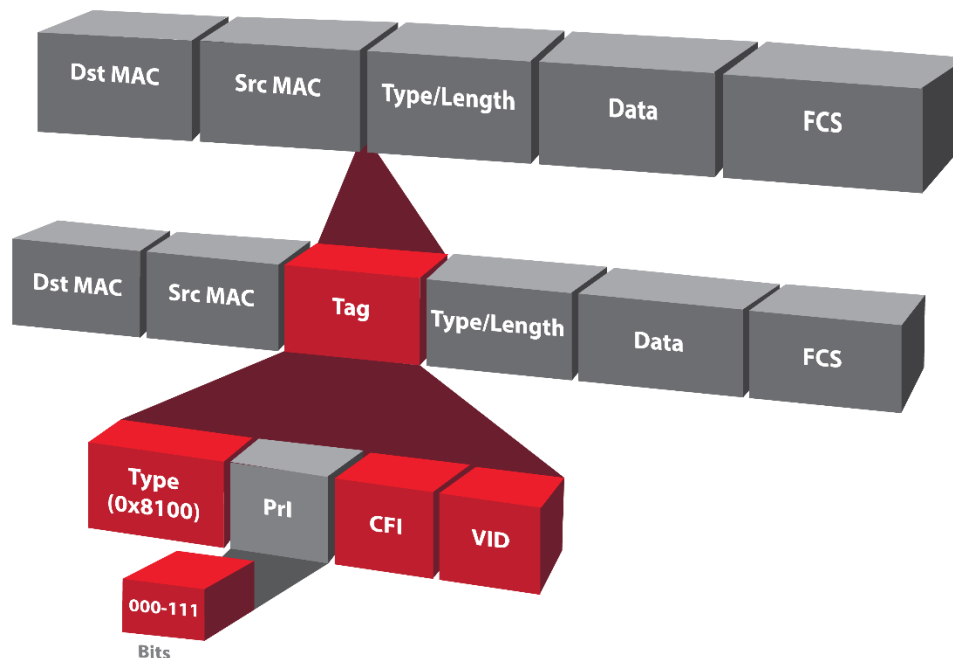
QoS Overview

QoS provided two basic methods of guaranteed data delivery, stateful load control, known as Integrated Services (IntServ) and stateless load control, known as Differentiated Services (DiffServ). IntServ uses the signaling method to verify network resources are available before data transmissions. DiffServ uses the provisioning method for marking packets. For the purpose of this white paper, we will be using the Differentiated Services (Diff-Serv) for QoS management.

Differentiated Services (Diff-Serv) architecture specifies that each packet is classified upon entering the network and processed before exiting the network. Depending on the type of traffic being transmitted, the classification will be done inside the layer 2 or layer 3 header.

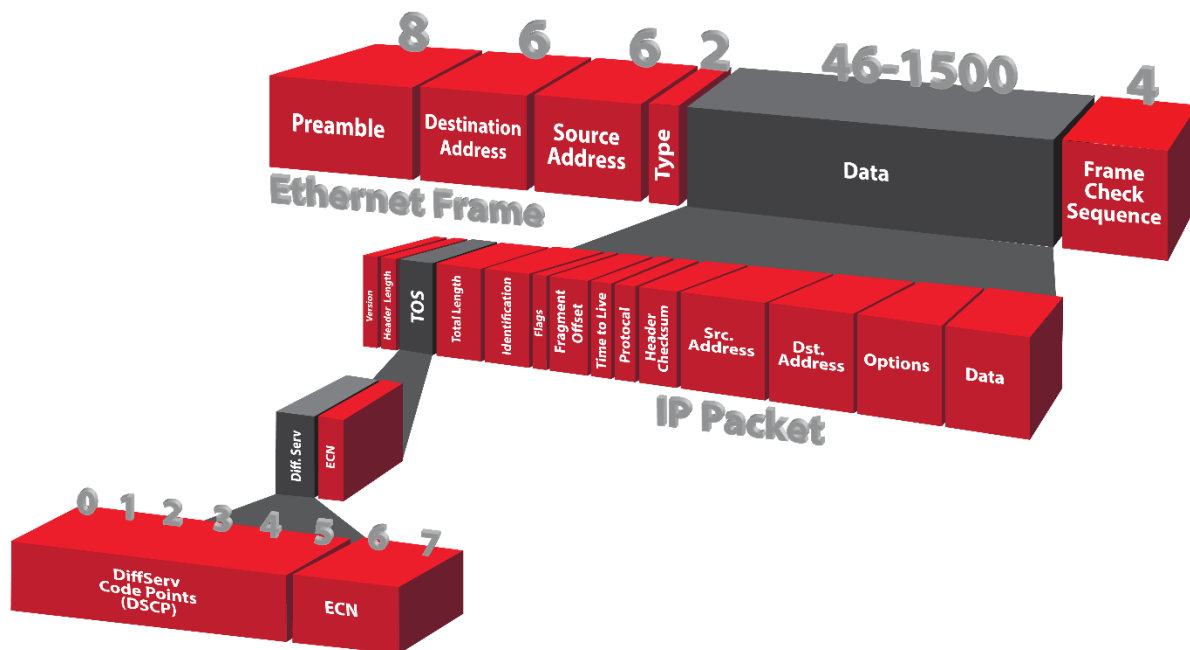
Layer-2 Frame Classification

Layer-2 frame classification is done inside of the IEEE 802.1Q frame header and uses 802.1p Class of Service (CoS) specifications for traffic prioritization. By assigning a value from 0-7 in the 3-bit User Priority found in 802.1Q tagged Ethernet frames, traffic can be categorized with a low priority or high priority.



Layer-3 IP Packet Classification

Layer-3 packets classification uses a Differentiated Service Code Point or DSCP values. These values are located inside of the Type of Service field that's part of the IP Packet header. The Type of Service (TOS) is one set of attributes used for traffic classification.



DSCP values can be numeric values or standards-based names called Per-Hop Behaviors. There are several broad classes of DSCP markings: Best Effort (BE), Class Selectors (CS), Assured Forwarding (AF), and Expedited Forwarding (EF). The details for each of these standards and configurations methods are beyond the scope of this paper.

Mechanics Behind QoS

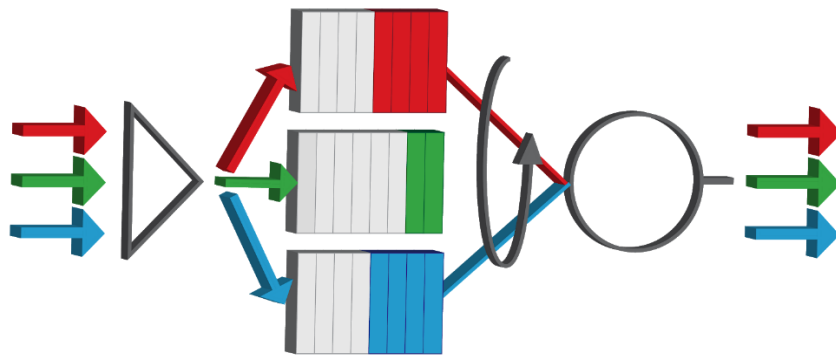
During times of congestion, network traffic entering the switch on configured QoS ports will be separated and processed. The incoming traffic is first classified with CoS or DSCP value according to their specifications and then separated.

Next, the separated traffic is forwarded to the Policer for bandwidth control. The Policer determines what type of bandwidth requirements are needed and what actions to take on a

packet-by-packet basis. The actions which include forwarding, modifying or dropping, are then carried out by the Marker. The packets are then placed into queues according to their specifications on the egress interfaces and forwarded to their destination.

Round Robin Queuing

Ethernet ports on routers and switches have sets of queues or buffers where data packets are stored while awaiting transmission. There are several ways for these queues to drain out but the two most common are Strict and Round Robin. Strict queueing will make sure the high priority queue is empty before a single frame is released from the low priority queue. This works great for testing QoS in a lab, but in most real-world applications this does not fare well. The application sending low priority frames will time-out and fail as it waits for higher priority queues to empty.



Round Robin queueing allows transmissions of low priority queues in conjunction with higher priority queues. This method keeps low priority applications such as email or web traffic from timing out during times of congestion. Round Robin queueing will transmit data in a sequence of high priority and low priority queues, for example, 10-1 will send 10 high priority frames to 1 low priority frame before going back to sending another 10 sets of frames. Round Robin keeps rotating transmissions between queues until they're emptied. You might see a router or switches with 4 priority queues and the round robin settings might be seen as 10-7-5-1. This would be the number of frames that the round robin releases as it goes from one queue to the next.

Know Your Network

The goal of creating an efficient QoS implementation into your networks for traffic management and robust connectivity requires many detailed steps. Having a few tools in your belt can help shorten those steps by saving time and avoiding costly mistakes.

1) Create a detailed layered network map

This is one of the most important and most overlooked items in the administrators' tool belt.

Having a detailed, well-documented network map will not only clear up any misconceptions you have of the network, but it will also become an asset in your planning.

Your map should include the following:

- **Layer 1- Physical Hardware:** Outline as much as possible (networking equipment, control equipment, O/I devices and stations) and the physical ports being used as interconnected links or aggregated trunks. Also, list media types and the distance between devices if possible.
- **Layer 2 – Link Control and Segmentation:** List the link speeds and duplex setting, VLAN membership, and point-to-point connections. This will help with identifying possible congestion points.
- **Layer 3 – IP Addressing:** list all the subnets, routes, tunnels, VPNs, or anything that would direct traffic to another subnet and/or networks.

2) Manufacturer documentation

Use manufacturer configuration guides and spec sheets to verify feature set and configuration strategies for your QoS implementation.

3) Baseline your network

Create a baseline of your network by analyzing traffic patterns and bandwidth utilization before and after your implementation. You may be revisiting your device configurations more than once in order to get the optimal tuning of your network correct.

QoS Implementations

Once you have all this information gathered, you will need to coordinate the QoS implementation. Be sure to give yourself enough time to analyze traffic and test your configurations. Best practice methods recommend starting from the outer edges of your network and working your way towards the distribution and core switches.

Conclusion

Industrialized networking really has come a long way over the years. The introduction of advanced switching technologies into once separated, closed off digital networks has opened the doors to a new generation of communications. This new generation of industrialized protocols, gigabit switch ports, and wireless data transmission has given industrial industries the ability to increase production in a safer, more efficient manner.

However, these new abilities come with a cost. New application and I/O devices rely heavily on bandwidth for synchronized and time-sensitive communications. In modern-day industrialized networks, guaranteed bandwidth for data streams is a premium and must be treated and allocated as such. One of the tools being used by engineers and administrators to manage and provide guaranteed bandwidth is Quality of Service.

QoS, with its advanced mechanisms, can provide the bandwidth allocation needed during the time of network congestion. By provisioning network switches to prioritize specific types of traffic, data transmissions for uninterruptible services can be guaranteed.

Implementing QoS for efficient packet delivery is by no means a small task. It's an involved process that takes time and effort to coordinate and configure. However, the tradeoff of knowing you have an efficient, well-refined, documented network, that has been customized to meet your specific needs, is worth the investment. QoS is worth it.

If you have any questions regarding QoS, feel free to email Antaira with your questions at PM@antaira.com.



Antaira Technologies is a leading developer and manufacturer that provides high-quality industrial networking and communication product solutions. Since 2005, Antaira has offered a full spectrum of product lines that feature reliable Ethernet infrastructures, extended temperature tolerance, and rugged enclosure designs. Our product lines range from industrial Ethernet switches, industrial wireless devices, Ethernet media converters, and serial communication devices. Our vast professional experience allows us to deploy a wide array of products worldwide in mission-critical applications across various markets, such as, automation, transportation, security, oil/ gas, power/utility, and medical.

www.antaira.com

714-671-9000

 **antaira**[®]
making connectivity simple...