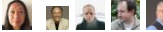


Tomado de

<https://docs.microsoft.com/en-us/microsoftteams/qos-in-teams>

## Implement Quality of Service (QoS) in Microsoft Teams

- 12/17/2018
- 12 minutes to read  +13
- Applies to: Microsoft Teams

This article will help you prepare your organization's network for Quality of Service (QoS) in Microsoft Teams. If you are supporting a large group of users and they are experiencing any of the problems mentioned below, you probably need to implement QoS. A small business with few users may not need QoS, but even there it should be helpful.

QoS is a way to allow real-time network traffic (like voice or video streams) that is sensitive to network delays to "cut in line" in front of traffic that is less sensitive (like downloading a new app, where an extra second to download isn't a big deal). QoS identifies and marks all packets in real-time streams (using Windows Group Policy Objects and a routing feature called Port-based Access Control Lists, more about those is below) which then helps your network to give voice, video, and screen share streams a dedicated portion of network bandwidth.

Without some form of QoS, you might see the following quality issues in voice and video:

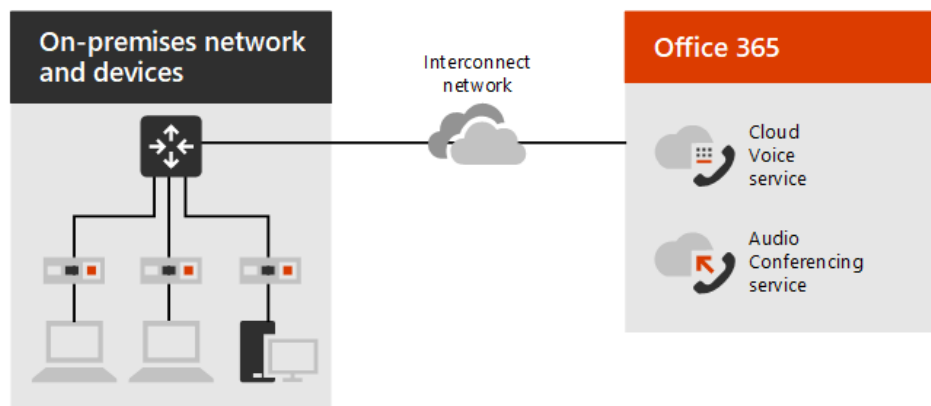
- Jitter – media packets arriving at different rates, which can result in missing words or syllables in calls.
- Packet loss – packets dropped, which can also result in lower voice quality and hard to understand speech.
- Delayed round trip time (RTT) – media packets taking a long time to reach their destinations, which results in noticeable delays between two parties in a conversation, causing people to talk over each other.

The least complex way to address these issues is to increase the size of the data connections, both internally and out to the internet. Since that is often cost-

prohibitive, QoS provides a way to more effectively manage the resources you have instead of adding new resources. To fully address quality issues you would use QoS across the implementation, then add connectivity only where absolutely necessary.

For QoS to be effective, you will have have consistent QoS settings applied end to end in your organization, because any part of the path that fails to support your QoS priorities can degrade the quality of calls, video, and screen shares. This includes applying settings to all user PCs or devices, network switches, routers to the internet, and the Teams online service.

Figure 1. The relationship between an organization's networks and Office 365 services



In most cases, the network connecting your enterprise to the cloud will be an unmanaged network where you won't be able to reliably set QoS options. One choice available to address end-to-end QoS is [Azure ExpressRoute](#), but we still recommend that you implement QoS on your on-premises network for both inbound and outbound traffic. This will increase the quality of real-time communication workloads throughout your deployment and alleviate chokepoints.

## Verify your network is ready

If you are considering a QoS implementation, you should already have determined your bandwidth requirements and other [network requirements](#).

Traffic congestion across a network will greatly impact media quality. A lack of bandwidth leads to performance degradation and a poor user experience. As Teams adoption and usage grows, use reporting, [Call Analytics, and Call Quality Dashboard](#) to identify problems and then make adjustments using QoS and selective bandwidth additions.

## VPN considerations

QoS only works as expected when implemented on all links between callers. If you use QoS on an internal network and a user signs in from a remote location, you can only prioritize within your internal, managed network. Although remote locations can receive a managed connection by implementing a virtual private network (VPN), a VPN inherently adds packet overhead and creates delays in real-time traffic. We recommend that you avoid running real-time communications traffic over a VPN.

In a global organization with managed links that span continents, we strongly recommend QoS because bandwidth for those links is limited in comparison to the LAN.

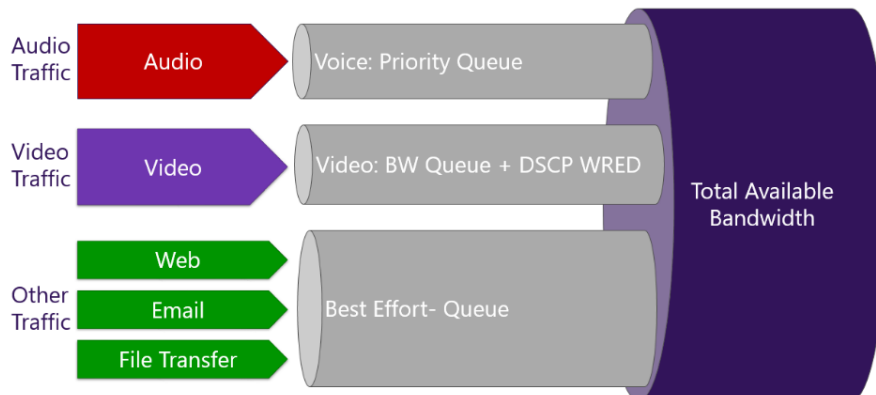
## Introduction to QoS queues

To provide QoS, network devices must have a way to classify traffic and must be able to distinguish voice or video from other network traffic.

When network traffic enters a router, the traffic is placed into a queue. If a QoS policy isn't configured, there is only one queue, and all data is treated as first-in, first-out with the same priority. That means voice traffic (which is very sensitive to delays) might get stuck behind traffic where a delay of a few extra milliseconds wouldn't be a problem.

When you implement QoS, you define multiple queues using one of several congestion management features (such as Cisco's priority queuing and Class-Based Weighted Fair Queueing [CBWFQ](#)) and congestion avoidance features (such as weighted random early detection [WRED](#)).

*Figure 2. Examples of QoS queues*



A simple analogy is that QoS creates virtual “carpool lanes” in your data network so some types of data never or rarely encounter a delay. Once you create those lanes, you can adjust their relative size and much more effectively manage the connection bandwidth you have, while still delivering business-grade experiences for your organization's users.

## Select a QoS implementation method

You could implement QoS via port-based tagging, using Access Control Lists (ACLs) on your network's routers. Port-based tagging is the most reliable method because it works in mixed Windows and Mac environments and is the easiest to implement. Mobile clients don't provide a mechanism to mark traffic by using DSCP values, so they will require this method.

Using this method, your network's router examines an incoming packet, and if the packet arrived using a certain port or range of ports, it identifies it as a certain media type and puts it in the queue for that type, adding a predetermined [DSCP](#) mark to the IP Packet header so other devices can recognize its traffic type and give it priority in their queue.

Although this works across platforms, it only marks traffic at the WAN edge (not all the way to the client machine) and creates management overhead. You should refer to the documentation provided by the router manufacturer for instructions on implementing this method.

You could also implement QoS implemented by using a Group Policy Object (GPO) to direct client devices to insert a DSCP marker in IP packet headers identifying it as particular type of traffic(for example, voice). Routers and other network devices can be configured to recognize this and put the traffic in a separate, higher-priority queue.

Although this scenario is entirely valid, it will only work for domain-joined Windows clients. Any device that isn't a domain-joined Windows client won't be enabled for DSCP tagging. Clients such as Mac OS have hard-coded tags and will always tag traffic.

On the plus side, controlling the DSCP marking via GPO ensures that all domain-joined computers receive the same settings and that only an administrator can manage them. Clients that can use GPO will be tagged on the originating device, and then configured network devices can recognize the real-time stream by the DSCP code and give it an appropriate priority.

We recommend a combination of DSCP markings at the endpoint and port-based ACLs on routers, if possible. Using a Group Policy object to catch the majority of clients, and also using port-based DSCP tagging will ensure that mobile, Mac, and other clients will still get QoS treatment (at least partially).

DSCP markings can be likened to postage stamps that indicate to postal workers how urgent the delivery is and how best to sort it for speedy delivery. Once you've configured your network to give priority to real-time media streams, lost packets and late packets should diminish greatly.

Once all devices in the network are using the same classifications, markings, and priorities, it's possible to reduce or eliminate delays, dropped packets, and jitter by changing the size of the port ranges assigned to the queues used for each traffic type. From the Teams perspective, the most important configuration step is the classification and marking of packets, but for end-to-end QoS to be successful you also need to carefully align the application's configuration with the underlying network configuration. Once QoS is fully implemented, ongoing management is a question of adjusting the port ranges assigned to each traffic type based on your organization's needs and actual usage.

## Choose initial port ranges for each media type

The DSCP value tells a correspondingly configured network what priority to give a packet or stream, whether the DSCP mark is assigned by clients or the network itself based on ACL settings. Each media workload gets its own unique DSCP value (other services might allow workloads to share a DSCP marking, Teams does not) and a defined and separate port range used for each media type. Other environments might have an existing QoS strategy in place, which will help you determine the priority of network workloads.

The relative size of the port ranges for different real-time streaming workloads sets the proportion of the total available bandwidth dedicated to that workload. To return to our earlier postal analogy: a letter with an "Air Mail" stamp might get taken within an hour to the nearest airport, while a small package marked "Bulk Mail" mark can wait for a day before traveling over land on a series of trucks.

The following table shows the required DSCP markings and the suggested corresponding media port ranges used by both Teams and ExpressRoute. These ranges might serve as a good starting point for customers who are unsure what to use in their own environments. To learn more, read [ExpressRoute QoS requirements](#).

### *Recommended initial port ranges*

Media traffic type	Client source port range	Protocol	DSCP value	DSCP class
Audio	50,000–50,019	TCP/UDP	46	Expedited Forwarding (EF)
Video	50,020–50,039	TCP/UDP	34	Assured Forwarding (AF41)
Application/Screen Sharing	50,040–50,059	TCP/UDP	18	Assured Forwarding (AF21)

Be aware of the following when you use these settings:

- If you plan to implement ExpressRoute in the future and haven't yet implemented QoS, we recommend that you follow the guidance so that DSCP values are the same from sender to receiver.
- All clients, including mobile clients and Teams devices, will use these port ranges and will be affected by any DSCP policy you implement that uses these source port ranges. The only clients that will continue to use dynamic

ports are the browser-based clients (that is, those clients that let participants join meetings by using their browsers).

- Although the Mac client uses the same port ranges, it also uses hard-coded values for audio (EF) and video (AF41). These values are not configurable.
- If you later need to adjust the port ranges to improve user experience, the port ranges can not overlap and should be adjacent to each other.

## Migrate QoS to Teams

If you've previously deployed Skype for Business Online, including QoS tagging and port ranges, and are now deploying Teams, Teams will respect the existing configuration and will use the same port ranges and tagging as the Skype for Business client. In most cases, no additional configuration will be needed.

### Note

If you're using Application Name QoS tagging via Group Policy, you must add Teams.exe as the application name.

## QoS implementation steps

At a very high level, implementing QoS requires these steps:

1. [Verify your network is ready](#)
2. [Select a QoS implementation method](#)
3. [Choose initial port ranges for each media type](#)
4. Implement QoS settings:
  - a. On Clients using a GPO to [set client device port ranges and markings](#)
  - b. On routers (see the manufacturer documentation) or other network devices. This may include port-based ACLs or simply defining the QoS queues and DSCP markings, or all of these.

### Important

We recommend implementing these QoS policies using the client source ports and a source and destination IP address of "any." This will catch both incoming and outgoing media traffic on the internal network.

- c. On [Teams Admin Center](#)
5. [Validate the QoS implementation](#) by analyzing Teams traffic on the network.

As you prepare to implement QoS, keep the following guidelines in mind:

- The shortest path to Office 365 is best.
- Closing ports will only lead to quality degradation.
- Any obstacles in-between, such as proxies, are not recommended.
- Limit the number of hops:
  - Client to network edge – 3 to 5 hops.
  - ISP to Microsoft network edge – 3 hops
  - Microsoft network edge to final destination – irrelevant

For information about configuring firewall ports, go to [Office 365 URLs and IP ranges](#).

## Managing source ports in the Teams admin center

In Teams, QoS source ports used by the different workloads should be actively managed, and adjusted as necessary. Referring to the table in [Choose initial port ranges for each media type](#), the port ranges are adjustable, but the DSCP markings are not configurable. Once you have implemented these settings, you may find that more or fewer ports are needed for a given media type. [Call Analytics and Call Quality Dashboard](#) should be used in making a decision to adjust port ranges after Teams has been implemented, and periodically as needs change.

### Note

If you've already configured QoS based on source port ranges and DSCP markings for Skype for Business Online, the same configuration will apply to Teams and no further client or network changes to the mapping will be required, though you may have to [set the ranges used in Teams Admin Center](#) to match what was configured for Skype for Business Online.



If you've previously deployed Skype for Business Server on-premises, you may need to re-examine your QoS policies and adjust them as needed to match port range settings you've verified provide a quality user experience for Teams.

## Validate the QoS implementation

For QoS to be effective, the DSCP value set by the Group Policy object needs to be present at both ends of a call. By analyzing the traffic generated by the Teams client, you can verify that the DSCP value isn't changed or stripped out when the Teams workload traffic traverses moves through the network.

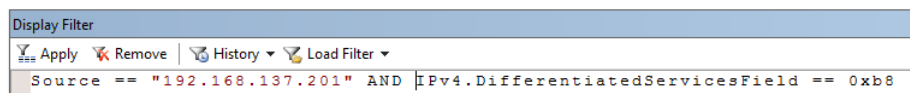
Preferably, you capture traffic at the network egress point. You can use port mirroring on a switch or router to help with this.

### Use Network Monitor to verify DSCP values

Network Monitor is a tool you can [download from Microsoft](#) to analyze network traffic.

1. On the PC running Network Monitor, connect to the port that has been configured for port mirroring and start capturing packets.
2. Make a call by using the Teams client. Make sure media has been established before hanging up the call.
3. Stop the capture.
4. In the **Display Filter** field, use the source IP address of the PC that made the call, and refine the filter by defining DSCP value 46 (hex 0x2E) as search criteria, as shown in the following example:

```
Source == "192.168.137.201" AND IPv4.DifferentiatedServicesField == 0x2E
```



5. Select **Apply** to activate the filter.
6. In the **Frame Summary** window, select the first UDP packet.
7. In the **Frame Details** window, expand the IPv4 list item and note the value at the end of the line that begins with **DSCP**.

```
Frame Details
  Frame: Number = 85, Captured Frame Length = 196, MediaType
  WiFi: [Unencrypted Data] .T....., (I)
  LLC: Unnumbered(U) Frame, Command Frame, SSAP = SNAP(Sub-Ne
  Snap: EtherType = Internet IP (IPv4), OrgCode = XEROX CORPC
  IPv4: Src = 192.168.137.201, Dest = 194.69.127.18, Next Prc
  Versions: IPv4, Internet Protocol; Header Length = 20
  DifferentiatedServicesField: DSCP: 46, ECN: 0
  DSCP: (101110..) Differentiated services codepoint 46
  ECT: (.....0) ECN-Capable Transport not set
  CE: (.....0) ECN-CE not set
  TotalLength: 132 (0x84)
  Identification: 31886 (0x7C8E)
  FragmentFlags: 0 (0x0)
  TimeToLive: 128 (0x80)
  NextProtocol: UDP, 17 (0x11)
  Checksum: 12633 (0x3159)
  SourceAddress: 192.168.137.201
  DestinationAddress: 194.69.127.18
  Udp: SrcPort = 50019, DstPort = 50009, Length = 112
```

In this example, the DSCP value is set to 46. This is correct, because the source port used is 50019, which indicates that this is a voice workload.

Repeat the verification for each workload that has been marked by the GPO.

## More information

[Video: Network Planning](#)

[Prepare your organization's network for Microsoft Teams](#)

[ExpressRoute QoS requirements](#)