

CHAPTER 3

Organization Readiness for Microsoft Teams

In the era of modern collaboration, Microsoft Teams has emerged as a powerful platform offering a multitude of features for seamless communication and collaboration. With its advanced audio and video calling capabilities, real-time conversations, and content sharing, Teams has revolutionized the way organizations work together. Microsoft's meticulous approach in building Teams from the ground up, incorporating the latest codec and media stack support, ensures optimal call quality for users. However, to fully leverage the potential of Teams, organizations must ensure their network infrastructure is prepared to handle the signaling and media traffic generated by Teams. Sufficient bandwidth for audio and video media traffic is crucial for delivering a smooth user experience. Without a properly provisioned and ready infrastructure, Teams may not perform as expected, leading to user frustrations and diminished productivity.

In this chapter, we delve into the critical aspects that organizations need to consider to ensure their readiness for Teams. We explore the network infrastructure requirements, including signaling and media traffic considerations, and we provide insights into provisioning the right bandwidth to support Teams' audio and video communication. We discuss the significance of preparing the network infrastructure to enable optimal call quality and seamless collaboration.

By addressing the organization's readiness for Teams, organizations can proactively eliminate potential roadblocks and ensure a smooth deployment and adoption of the platform. We explore best practices, recommendations, and practical steps to assess and optimize network infrastructure, enabling organizations to unlock the full potential of Microsoft Teams and empower their teams to collaborate effectively, regardless of geographical boundaries. This chapter serves as a comprehensive guide for organizations seeking to maximize the benefits of Microsoft Teams. By focusing

on organization readiness, IT professionals and decision-makers can ensure a robust and reliable environment for Teams, elevating collaboration, productivity, and user satisfaction within their organization.

Microsoft Teams offers a wide array of features, including audio and video calls, meetings, content sharing, and real-time conversations. Microsoft has invested significant effort in building Teams from the ground up, incorporating the latest codec and media stack support. As a result, Teams delivers commendable call quality. However, to ensure an optimal Teams experience, it is essential to have a network infrastructure that seamlessly handles Teams signaling and media traffic while providing sufficient bandwidth for audio and video transmissions. While Teams is designed to deliver optimal call quality, it heavily relies on a well-provisioned infrastructure. If your infrastructure is not correctly set up or prepared for Teams, the platform may not perform as intended, leading to a subpar experience for end users.

To avoid such issues, it is crucial to prioritize infrastructure readiness for Teams deployment. This involves evaluating and optimizing the network infrastructure, ensuring adequate bandwidth allocation, and configuring proper quality of service (QoS) settings. By proactively addressing these considerations, organizations can create an environment that supports the full functionality and performance of Microsoft Teams, enhancing collaboration and minimizing user frustrations. Ultimately, a properly provisioned and ready infrastructure for Teams is key to unlocking its potential and enabling seamless communication and collaboration among team members. By acknowledging the importance of infrastructure readiness, organizations can ensure a positive user experience, drive productivity, and maximize the benefits of Microsoft Teams within their workforce.

Preparing the infrastructure is, therefore, essential. Before starting Teams deployment, you as a Teams admin must ensure that all Teams network requirements are completed, including infrastructure and network readiness. You can then plan for starting the actual deployment. Microsoft did a better job of consolidating all the Teams (Office 365) IP subnets and port and protocol requirements in one document (<https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide#skype-for-business-online-and-microsoft-teams>), which you can refer to in completing these requirements.

So far, you have learned about Teams fundamentals, team and channel architecture, live events, identity, and Teams management tools. This chapter covers detailed information on network assessment and bandwidth planning for Teams, how to deploy

and manage QoS, and how to deploy a virtual private network (VPN) split tunnel for Microsoft Teams media traffic. Before the deployment of Microsoft Teams in a production environment, you, as an admin, need to determine whether the existing network meets the networking requirements of Microsoft Teams. Make sure you have the required bandwidth, access to all required IP addresses, and correct ports opened. You also need to ensure you meet the performance requirements for Teams real-time media traffic, such as audio, video, and application sharing.

Network Assessment and Bandwidth Planning for Teams

Assessing the network and planning the bandwidth for Microsoft Teams are crucial steps in ensuring a smooth and reliable communication experience within the platform. These processes involve evaluating the organization's network infrastructure, identifying potential bottlenecks or limitations, and determining the required bandwidth to support Teams' audio and video traffic.

Network assessment is the evaluation of the organization's existing network infrastructure to assess its readiness for supporting Microsoft Teams. It involves analyzing various factors that impact network performance, such as network capacity, latency, jitter, packet loss, and overall network health. The purpose of the assessment is to identify any network issues that may hinder Teams' performance and to implement appropriate measures to address them.

Bandwidth planning is the process of determining the amount of network bandwidth required to support the audio and video traffic generated by Microsoft Teams. It involves estimating the bandwidth needs based on factors such as the number of concurrent users, their usage patterns, and the types of activities they engage in (e.g., audio calls, video calls, screen sharing). Bandwidth planning ensures that the network can handle the anticipated traffic volume without degradation in call quality or performance.

To conduct a network assessment and bandwidth planning for Microsoft Teams, the following requirements should be considered:

- **Network monitoring tools:** Implement network monitoring tools to gather data on network performance metrics such as latency, jitter, and packet loss. These tools help identify areas of concern and provide insights into the network's capabilities.

- **Testing scenarios:** Simulate various usage scenarios within Microsoft Teams, including audio and video calls, screen sharing, and file transfers. These tests help assess the network's ability to handle different types of traffic and identify any bottlenecks or performance issues.
- **Quality of service (QoS) configuration:** Configure QoS settings to prioritize Teams' traffic over other network traffic. This ensures that audio and video calls receive the necessary bandwidth and are not impacted by competing network activities.
- **Network capacity planning:** Evaluate the organization's current network capacity and determine if any upgrades or optimizations are required to accommodate Teams' traffic. Consider factors such as the number of users, their geographical distribution, and potential growth projections.
- **Collaboration with network administrators:** Collaborate with network administrators to gather insights into the network infrastructure, understand its limitations, and work together to address any identified issues.

Network assessment and bandwidth planning are essential for a successful deployment of Microsoft Teams. They help organizations identify and mitigate potential network-related challenges that could impact call quality, user experience, and overall performance. By ensuring a robust and well-prepared network infrastructure, organizations can provide their users with a reliable and seamless communication and collaboration platform, optimizing productivity and enhancing the value of Microsoft Teams within their organization.

Before doing a network assessment and bandwidth planning for Microsoft Teams, you must know what different types of traffic Teams generates. At a high level, Teams produces and supports two types of traffic: Teams signaling traffic, also known as *gesturing*, and Teams media traffic, known as *real-time media traffic*. Teams is a purely cloud-hosted service that allows it to operate in three types of network traffic directions.

- **Teams signaling traffic:** Teams data traffic between the Teams service (Office 365 Online environment) and the Teams client for signaling, presence, chat, file upload and download, and OneNote synchronization).

- **Teams media traffic:**
 - Teams one-to-one real-time communications media traffic for audio, video, and application (desktop) sharing.
 - Teams conferencing real-time media communications traffic for audio, video, and application (desktop) sharing.

If any of the Teams network traffic directions are affected, then it will affect Teams communication. Teams traffic flows between the Teams clients directly in one-to-one call situations or between the Office 365 environment and the Teams clients for meetings.

To ensure the optimal traffic flow for both one-to-one and conference scenarios in Microsoft Teams, it is crucial for administrators to enable seamless communication between the organization's internal network segments. This includes establishing an uninterrupted traffic flow between different sites over a wide-area network (WAN) and between the network sites and the Office 365 environment. For instance, let's consider the example of the Bloguc organization. They have central offices located in Tracy, California, and Denver, Colorado, with branch offices in India. To facilitate effective communication, traffic between the central and branch offices is allowed to flow freely over the WAN without any restrictions. Additionally, these offices have direct connectivity to the Teams services in Office 365 via the Internet.

To ensure smooth traffic flow, the organization has taken measures to allow all necessary Teams IP subnets, ports/protocols, fully qualified domain names (FQDNs), and URLs. By permitting these essential communication elements, the organization ensures that there are no interruptions or interference in the flow of Teams-related traffic. By implementing these configurations, the Bloguc organization enables their users to seamlessly connect and collaborate within Microsoft Teams, irrespective of their geographical locations. This unrestricted traffic flow allows for efficient communication, smooth meeting experiences, and optimal utilization of Teams' features and capabilities.

Overall, by allowing seamless traffic flow and ensuring compatibility between network segments and the Office 365 environment, organizations can create an enhanced user experience and maximize the benefits of Microsoft Teams for their workforce.

Note Actively blocking specific ports or not opening the correct ports will lead to a degraded Teams experience.

Carrying Out a Network Assessment Before Teams Deployment

You have learned what type of traffic Teams generates, the traffic directions, and how it potentially affects the user experience. A network assessment is essential before Teams deployment because it will evaluate the existing network infrastructure and pinpoint the network impairments that could cause poor call quality. Also, the assessment will identify the performance-linked problems that can be introduced into the environment through latency and packet loss. Issues such as these will result in a negative experience in Teams audio and video scenarios, where real-time streams are essential.

Network assessment has several different aspects.

- It assesses the existing network configuration that might affect Teams traffic, while evaluating the existing network environment for hard limitations such as blocked IP addresses, faulty name resolution through DNS, and blocked ports. These problems are easy to spot because specific Teams features will simply not work at all when IP addresses or ports are blocked.
- Point-in-time problems, like bandwidth, latency, or packet-loss issues, are more complicated, because they might appear only under special conditions; for example, the Bloguc organization HQ office might have a high number of users who are using audio and video communication at the same time. Thus, when planning the network requirements for a Teams deployment, you must calculate the maximum number of concurrent users, including a sufficient buffer and bandwidth.

There are several best practices for preparing your environment for Microsoft Teams.

- You must allow seamless connectivity from your corporate network where the user resides to the Microsoft Teams service, which is in Office 365. Also, make sure that all required DNS names are resolved correctly, and Teams service IP addresses must be reachable.
- Make sure the network connection quality of an established connection is optimal through measuring in values, such as latency, jitter, and packet-loss rates. Also, the existing networking hardware must provide a stable connection with minimum network hops by keeping as few active networking devices between a Teams client and Office 365 as possible. Each active networking device adds additional latency and raises the chance of connectivity quality issues. So, optimizing the network path by eliminating the unnecessary network devices or hops will expedite packet flow and untimely improve call quality.
- Make sure to keep enough bandwidth available for Teams communication to Office 365 services. Remember, the required bandwidth of Teams depends on the required functionalities and number of Teams clients in an organization location. You must analyze the maximum number of concurrent participants and then multiply this number with the provided utilized Teams functionalities. For example, Bloguc has 100 users in the HQ office, and the available bandwidth is 100 MB. At any point in time 30 users will be on calls, so the available bandwidth must be sufficient for 30 users' calls.
- The Teams client can be connected over any network, either wired or wireless. Teams clients connected over a wireless connection, such as corporate Wi-Fi networks and hotspots, are more vulnerable for high latency and possibly higher packet loss because wireless networks usually are not necessarily designed or configured to support real-time media or not prepared for real-time services, such as Teams audio and video communication. For the wireless network, implementing QoS or Wi-Fi Multimedia (WMM) will ensure that media traffic is getting prioritized appropriately over the Wi-Fi

networks. You can work with your organization network engineer to plan and optimize the Wi-Fi bands and access point placement. Implement band steering, and ensure the access points that are next to each other are on channels that do not overlap. Furthermore, the network coverage must provide enough bandwidth even between wireless access points and on the edges.

- One of the significant network impairments is the intrusion detection system (IDS) and intrusion prevention system (IPS) feature on the firewalls that can analyze the payload of data packages for the attack signatures. If any organization network environment uses IDS and IPS solutions, then make sure all network traffic between your organization and the Teams services (Office 365) is whitelisted and excluded from any kind of scanning.
- Another best practice for Network Address Translation (NAT) pool size provides access to multiple internal systems by using a single public IP address. When multiple users and devices access Office 365 using NAT or Port Address Translation (PAT), you, as a Teams admin, must ensure that the devices hidden behind each publicly routable IP address do not exceed the supported number. You might need to check with your network engineer, who can help you to understand NAT configuration.
- Most of the time, the organization uses VPN that offers an encryption tunnel between endpoints, like remote users and the corporate network. Generally, VPNs are not designed to support real-time media traffic and introduce an extra layer of encryption on top of media traffic that is already encrypted. This adds overhead. Additionally, connectivity to the Teams service (Office 365) might not be efficient because of hair-pinning traffic through a VPN device. For VPNs, the suggestion is to provide an alternate path that bypasses the VPN tunnel for Teams traffic. This is generally known as split-tunnel VPN. We will cover the VPN split tunnel in detail in this chapter.
- Finally, verifying overall network health is equally critical, so identify the network health and quality baseline before Teams deployment in your organization. After planning on the Teams implementation

in your organization using the existing network, you should ensure there is sufficient bandwidth, accessibility to all required IP addresses, correct configuration of ports, and that the performance requirements for Teams real-time media are met.

Network Bandwidth Requirements for Microsoft Teams Calling Scenarios

Network bandwidth requirements for Microsoft Teams meetings and calls depend on various factors, including the type of communication (audio or video), the number of participants, and the activities involved, such as desktop sharing or content sharing. While these requirements can vary, the following are general guidelines for network bandwidth needed for different Teams communication scenarios:

Teams audio call:

- Recommended minimum bandwidth: 30 to 50 kilobits per second (Kbps) per user.
- This is the typical bandwidth requirement for a standard audio call between two participants. It may increase slightly depending on the quality of audio and any additional audio features in use (e.g., background noise suppression).

Teams video call:

- Recommended minimum bandwidth:
 - **For one-to-one video calls:** 300 to 500 Kbps per user for standard definition (SD) video.
 - **For group video calls:** 1.2 megabits per second (Mbps) for 720p HD video and 1.5 Mbps for 1080p Full HD video.
- These bandwidth recommendations apply to each participant in the video call. For example, in a four-person video call, the total bandwidth requirement will be four times the recommended minimum per user.

Teams desktop sharing:

- Recommended minimum bandwidth: 50 to 150 Kbps per user.
- Desktop sharing involves transmitting the screen contents to participants, including any applications or documents being shared. The bandwidth requirement can vary based on the complexity of the shared content and the frequency of screen updates.

It's important to note that these bandwidth requirements are for smooth and optimal performance. Actual bandwidth usage may vary based on factors such as network congestion, device capabilities, and other network activities running simultaneously.

To ensure a high-quality experience, it is recommended to have a reliable Internet connection with sufficient bandwidth. Additionally, implementing QoS settings on the network can help prioritize Teams traffic over other network activities, ensuring a smooth communication experience. Organizations with larger deployments or higher user densities may need to consider additional network capacity and scaling requirements to accommodate multiple concurrent meetings and calls.

Regularly monitoring and assessing your network's performance and bandwidth utilization can help identify any bottlenecks or issues and make necessary adjustments to ensure a seamless Microsoft Teams experience for all users.

So far, you have learned about network assessment and network best practices. Next, you need to understand the importance of network quality between your organization's network and Microsoft Teams cloud service and the required bandwidth for each Teams calling scenario. When assessing the existing network environment, first complete the Teams IP address, port/protocol, URLs, and faulty name resolution through DNS requirements, because specific Teams features will not work at all when Teams service IP addresses or ports are blocked. Additionally, finding the bandwidth, latency, or packet-loss issues is more complicated because they might appear only under particular circumstances. Refer to Table 3-1, which shows the recommended network capabilities and accepted latency, burst packet loss, packet loss, jitter, and packet reordering. For example, Teams call quality will be best when you have less than 50 ms latency between your organization network and Microsoft Edge router along with packet loss and jitter values under the limit.

Table 3-1. *Accepted Limits for Network Values*

Network (Value)	Teams client to Microsoft Edge N/W (without SfB Hybrid)	Customer Edge N/W to Microsoft Edge (with SfB Hybrid)
Latency (one way)	< 50ms	< 30ms
Latency (RTT or Round-trip Time)	< 100ms	< 60ms
Burst packet loss	<10% during any 200ms interval	<1% during any 200ms interval
Packet loss	<1% during any 15s interval	<0.1% during any 15s interval
Packet inter-arrival Jitter	<30ms during any 15s interval	<15ms during any 15s interval
Packet reorder	<0.05% out-of-order packets	<0.01% out-of-order packets

Because Microsoft Teams supports multiple features, each feature has different bandwidth requirements; for example, Teams one-to-one audio calling requires 30 Kb bandwidth for upstream and downstream. Table 3-2 shows call scenarios and required network bandwidth for your Teams clients to optimally use Teams features.

Table 3-2. *Teams Call Scenarios with Required Bandwidth*

Teams call/ conference scenarios	Required Bandwidth (up/down)
One-to-one audio calling	30 kbps
One-to-one audio calling and screen sharing	130 kbps
One-to-one video calling with resolution 360p at 30fps	500 kbps
One-to-one High Definition (HD) quality video calling with resolution of HD 720p at 30fps	1.2 Mbps
One-to-one HD quality video calling with resolution of HD 1080p at 30fps	1.5 Mbps
Group (more than 2 participant) Video calling	500kbps/1Mbps
HD Group video calling (540p videos on 1080p screen)	1Mbps/2Mbps

For network assessment, you can use the Network Planner and Network Testing Companion tools.

Network Planner

In the context of Microsoft Teams, the Network Planner is a tool designed to help organizations assess their network readiness and plan for optimal network performance when using Teams. It focuses on network quality perspectives and provides insights into network requirements for a smooth Teams experience.

The Network Planner helps organizations understand and address potential network challenges that may impact the audio, video, and screen sharing quality in Teams meetings. It provides guidance on network capacity, latency, and network paths to ensure that Teams can function optimally.

Here are some key aspects of the Network Planner in Microsoft Teams:

- **Network assessment:** The Network Planner conducts a network assessment to evaluate the suitability of your network infrastructure for Teams usage. It measures key network parameters such as available bandwidth, network latency, and network paths to determine whether they meet the recommended requirements for Teams.
- **Bandwidth planning:** The Network Planner helps organizations estimate the bandwidth requirements for different Teams activities, such as audio calls, video calls, and screen sharing. It provides insights into the expected bandwidth usage, allowing organizations to allocate sufficient network resources for a seamless Teams experience.
- **Latency analysis:** Latency refers to the delay in data transmission across a network. The Network Planner assesses network latency and helps identify any potential latency issues that could impact real-time communication in Teams meetings. It provides recommendations to reduce latency and improve call quality.
- **Network path analysis:** The Network Planner examines the network paths between users and the Teams services to identify potential bottlenecks or areas of concern. It helps organizations understand the network paths used by Teams traffic and suggests optimizations to ensure smooth connectivity and minimize disruptions.
- **Reports and recommendations:** Based on the assessment results, the Network Planner generates reports and recommendations to help organizations address network quality issues. It provides actionable insights and guidance on network configuration changes, network optimizations, and network infrastructure upgrades to enhance the overall Teams experience.

By leveraging the Network Planner, organizations can proactively assess and plan their network infrastructure to meet the specific requirements of Microsoft Teams. It enables IT administrators to identify and address network quality issues, ensuring that users can have reliable and high-quality audio and video communication in Teams meetings. Using Network Planner, an admin can create representations of an organization using sites and Microsoft-recommended personas (office workers, remote workers, and Teams room system devices) and then generate reports and calculate bandwidth requirements for Teams usage. To use the Network Planner, you must have global administrator, Teams admin, or Teams communication administrator role permissions.

Adding a Plan

You can access the Network Planner tool, shown in Figure 3-1, by going to the Microsoft Teams admin center and navigating to Planning. Select “Network planner.”

Network planner

Network planner helps you to determine and organize network requirements for connecting people that use Teams across your organization in a few steps. By providing your networking details and Teams usage, you get calculations and the network requirements you need when deploying Teams and cloud voice across organizational physical locations. [Learn more](#)

Network plans summary

1 Network plans 3 Personas

Network plans Personas

+ Add Delete

✓	Network plan name	Description	Network sites	Network users
	Cyclotron's BW Planning 2023	This is Cyclotron, Inc...		

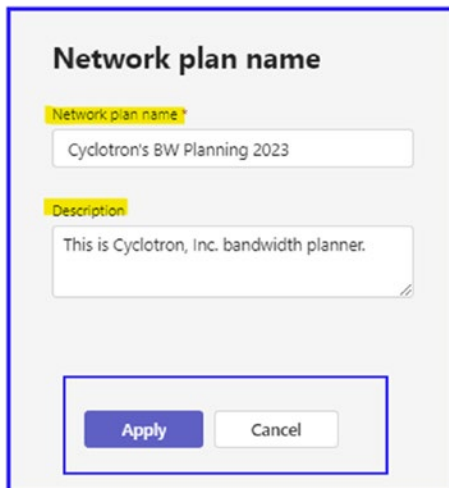
Figure 3-1. Network planner

When you click Add, it will allow you to create a Network Planner name. By default, there will be three user personas; you can add custom personas on the “Network planner” page by clicking the Users tab. On the Add Persona page, provide the persona name and description. In the Permissions section, select from the following services: Audio, Video, Screen Sharing, File Sharing, Conference Audio, Conference Video, Conference Screen Sharing, and PSTN.

Developing a Network Planner Plan

The Network Planner helps you to determine and organize network requirements for connecting people who use Teams across your organization in a few steps. To build your network plan, follow these steps:

1. Log in to the Microsoft Teams admin center and then navigate to Planning. Select “Network planner.”
2. On the “Network planner” page, under Network Plans, click Add.
3. On the “Network plan name” page, enter the name for the network plan (in the example shown in Figure 3-2, Cyclotron’s BW Planning 2023) and an optional description. Click Apply.



The screenshot shows a form titled "Network plan name". It contains two text input fields. The first field is labeled "Network plan name" and contains the text "Cyclotron's BW Planning 2023". The second field is labeled "Description" and contains the text "This is Cyclotron, Inc. bandwidth planner.". At the bottom of the form, there are two buttons: "Apply" and "Cancel".

Figure 3-2. Adding a network plan name

4. The newly created network plan will appear in the Network Plans section. Select the plan you created. On the plan page, in the Network Sites section, click Add A Network Site. On the Add A Network Site page, shown in Figure 3-3, enter the following information:
 - Name of the network site
 - Network site address
 - Network settings: IP address subnet and network range
 - Express route or WAN connection
 - Internet egress
 - Internet link capacity
 - PSTN egress (VoIP only or local)
 - An optional description

5. Once you enter all the details, click Save to commit the changes.

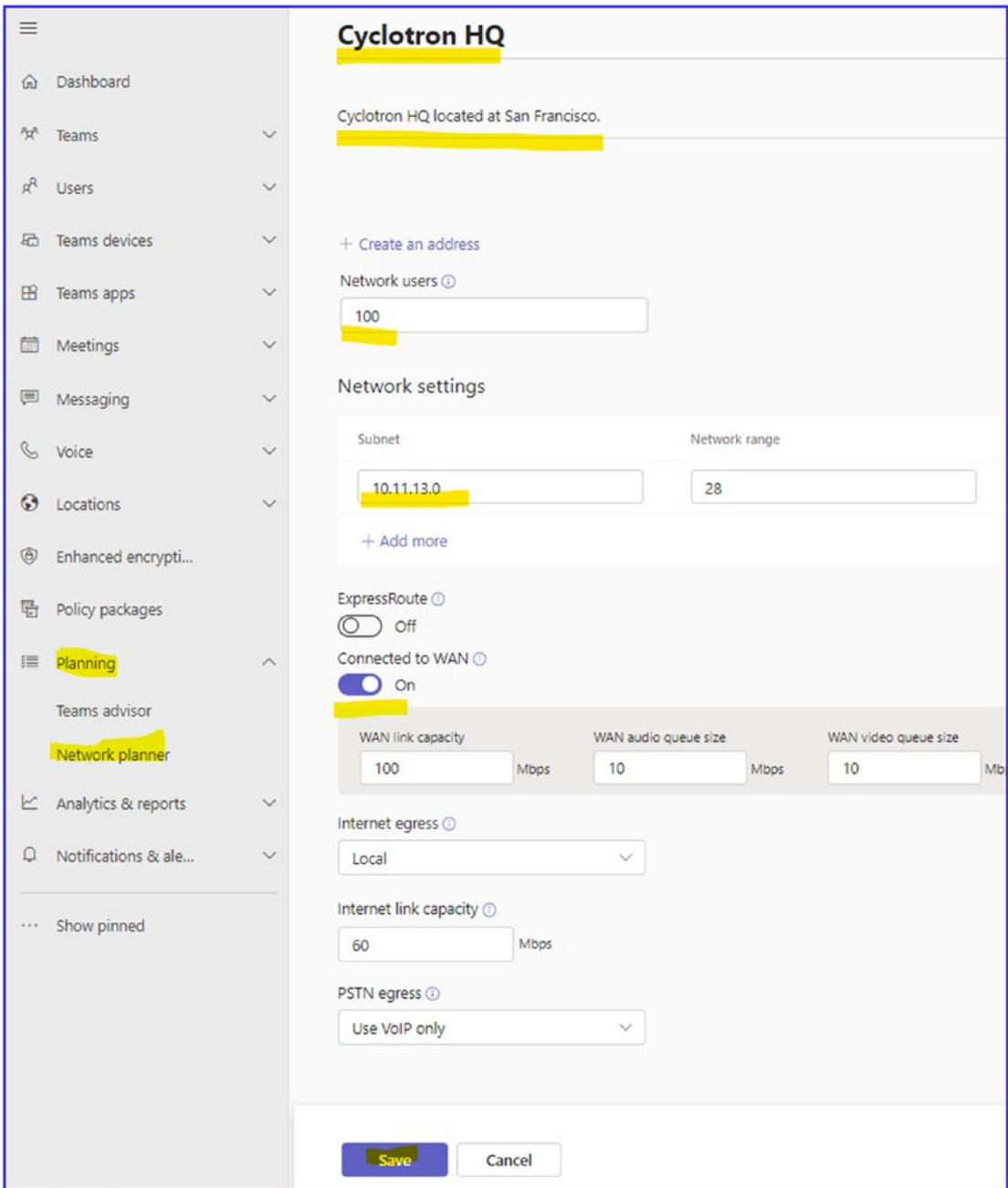


Figure 3-3. Adding a network site and subnet

After creating a plan, the next thing you have to do is create a report based on your network plan and view the projected impact of Teams media traffic such as audio, video, meetings, and PSTN calls. To do so, log in to the Teams admin center, navigate to Planning, and then select Network Planner. On the Network Planner page, in the Network Plans section, select your network plan (given a meaningful name). On the plan page, select Report, and then click Add Report.

On the Add Report page, enter the report name (Cyclotron's BW Report in our example), and in the Calculation section, select the type of persona, such as Office Worker or Remote Worker and the number of each persona type, and then click Generate Report. On the report page, review the report including type of service and required bandwidth for different services, such as audio, video, desktop sharing, Office 365 server traffic, and PSTN.

Microsoft Teams Network Assessment Tool

The Microsoft Teams Network Assessment Tool is a utility designed to help assess network connectivity and performance for Microsoft 365 services, including Microsoft Teams. It allows you to simulate network traffic and measure the quality of the network connection between your client devices and Microsoft's datacenters.

The Microsoft Teams Network Assessment Tool is used to test the quality of your network connection to the Teams service. It's crucial to ensure that your network meets the minimum requirements for a good user experience with Teams.

This tool checks the following:

- Network connectivity to the Teams service
- UDP port connectivity
- Network performance statistics such as jitter, latency, packet loss, and round-trip time

The information it provides can be valuable for troubleshooting network problems that might be affecting Teams audio and video quality.

Microsoft Teams Network Assessment Tool Capabilities

Let's look at the tool's capabilities.

Network Connectivity Checker

The Microsoft Teams Network Assessment Tool also possesses the capability to confirm whether the network connectivity between the user's location and the Microsoft Network is properly set up for additional services necessary for Microsoft Teams calls. These essential services encompass the following, along with their associated protocols:

- Call Controller (HTTP and UDP)
- Conversation Service (HTTP)
- Chat Service (HTTP)
- Trouter Service (HTTP)
- Broker Service (HTTP)

The specific addresses and ports for these services can be found at https://support.office.com/en-us/article/Office-365-URLs-and-IP-address-ranges-8548a211-3fe7-47cb-abb1-355ea5aa88a2#bkmk_teams.

Network Quality Checker

The Microsoft Network Assessment Tool allows users to conduct a basic network performance test to evaluate the network's compatibility for a Microsoft Teams call. This tool examines the connection to a Microsoft relay server by broadcasting a series of RTP media packets to the server and back for a duration defined by the user. In this process, the client attempts to allocate with the relay load-balancer (VIP). Similar to a Teams call, priority is given to UDP relay connections over TCP/HTTPS relay connections. To ensure this, the checker initiates UDP relay allocations slightly ahead of TCP/HTTPS allocations. If the relay allocations are successful, the tool proceeds to transmit media packets to the forwarded relay instance (DIP). The tool then periodically (approximately every five seconds) reports the following:

- Timestamp
- Packet loss rate
- Round-trip latency
- Jitter

- Media Path local IP/port
- Media path reflexive (NAT translated) IP/port
- Media path remote IP/port
- Status of proxy usage for media flow (applicable only to TCP/HTTPS relay connection)

As with the relay connectivity check, a default relay load-balancer relay (VIP) FQDN for Worldwide Office 365 Endpoints is used by default, but users have the option to enter a custom FQDN in the configuration file. The checker performs DNS resolution to acquire a relay load-balancer IP address, although users can specify connectivity checks to a particular load-balancer relay IP address in the configuration file. If a relay IP address is input, the relay FQDN (either default or custom) is ignored. Users can also designate the source port range on their client machine for relay connection. Unlike the connectivity checker, users can opt to disable either UDP or TCP connections to the relay, but not both. Users can also alter the UDP/TCP relay instance (DIP) ports for media packet transmission. The quality checker can be halted at any moment by pressing Ctrl+C; this will conclude the checker after the next set of metrics is displayed on the console.

Prerequisites for the Teams Network Assessment Tool

There are some prerequisites for this tool. Your operating system must be Windows 8 or later, and most importantly, you must have a local administrator account permission to install the Network Assessment Tool.

Installing the Teams Network Assessment Tool

Installation is very straightforward; however, to install this tool, a user must have administrator rights to the computer. You can download the tool at <https://www.microsoft.com/en-us/download/confirmation.aspx?id=103017>. After downloading, run the downloaded executable to install. The install location is %ProgramFiles(x86)%\Microsoft Teams Network Assessment Tool, and the tool itself is NetworkAssessmentTool.exe. Follow the prompts and install the tool; after a successful install, your screen will look like Figure 3-4.

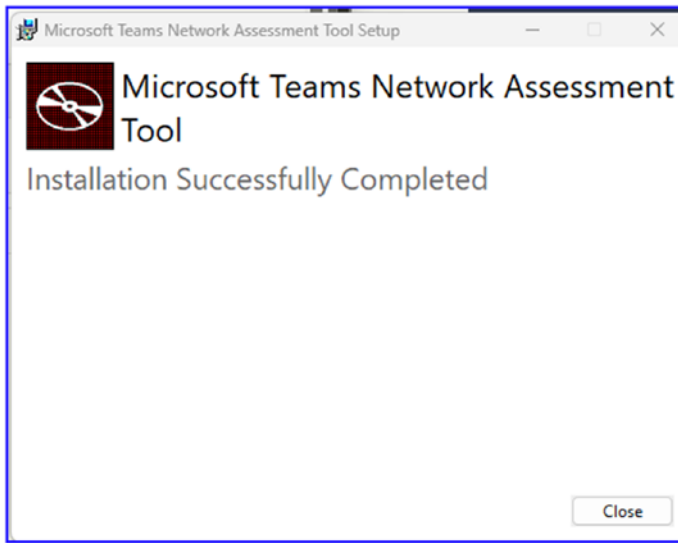


Figure 3-4. *Installing the Teams Network Assessment Tool*

After installation, to start the Teams Network Assessment Tool, open the command prompt with administrative privileges and then go to the path where the tool installed, which is `%ProgramFiles(x86)%\Microsoft Teams Network Assessment Tool`.

Using the Teams Network Assessment Tool

This tool is self-explanatory. After you install this tool, you can simply open the command prompt with administrative privileges and then browse to the tool installer directory, which is `%ProgramFiles(x86)%\Microsoft Teams Network Assessment Tool`. Then from a command prompt, view the options in the tool by running `NetworkAssessmentTool.exe /?` or `NetworkAssessmentTool.exe /usage`. Figure 3-5 shows the usage options.

```

Administrator: Command Prompt

C:\>cd C:\Program Files (x86)\Microsoft Teams Network Assessment Tool

C:\Program Files (x86)\Microsoft Teams Network Assessment Tool>NetworkAssessmentTool.exe /?
Microsoft Teams - Network Assessment Tool

Usage:
NetworkAssessmentTool.exe [options]
[options]:
<no option>                Perform connectivity checks.
/qualitycheck               Perform quality checks with relay.
/infraconnectivitytest     Perform HTTP stack infra tests.
/interfaces                 Dumps the list of the interfaces found.
/location                  Perform lldp and geolocation checks.
/usage or /?               Print usage text.

C:\Program Files (x86)\Microsoft Teams Network Assessment Tool>

```

Figure 3-5. Teams Network Assessment Tool

For a Teams connectivity check, from a command prompt, execute the tool by simply running `NetworkAssessmentTool.exe`.

Here is the exact command:

```
C:\Program Files (x86)\Microsoft Teams Network Assessment Tool>Network
AssessmentTool.exe
```

You will get detailed reports about the connectivity check test, as shown in Figure 3-6.

```

C:\Program Files (x86)\Microsoft Teams Network Assessment Tool>NetworkAssessmentTool.exe
Microsoft Teams - Network Assessment Tool

Starting Relay Connectivity Check:
UDP, PseudoTLS, FullTLS, HTTPS connectivity will be checked to this relay (VIP) FQDN: worldaz.tr.teams.microsoft.com
If user wants to check connectivity to a particular relay (VIP) IP, please specify in NetworkAssessment.exe.config.

Connectivity check source port range: 50000 - 50019

Relay : 52.115.63.231 is the relay load balancer (VIP)
Relay : 52.115.63.231 is reachable using Protocol UDP and Port 3478
Relay : 52.115.63.231 is QoS (Media Priority) enabled
Relay : 52.115.63.231 is the relay load balancer (VIP)
Relay : 52.115.63.231 is reachable using Protocol PseudoTLS and Port 443
Relay : 52.115.63.231 is the relay load balancer (VIP)

Starting Service Connectivity Check:
Relay : 52.115.63.231 is reachable using Protocol FullTLS and Port 443
Relay : 52.115.63.231 is the relay load balancer (VIP)
Relay : 52.115.63.231 is reachable using Protocol HTTPS and Port 443
Relay : 52.115.63.242 is the actual relay instance (DIP)
Relay : 52.115.63.242 is reachable using Protocol UDP and Port 3478
Relay : 52.115.63.242 is the actual relay instance (DIP)
Relay : 52.115.63.242 is reachable using Protocol UDP and Port 3479
Relay : 52.115.63.242 is the actual relay instance (DIP)
Relay : 52.115.63.242 is reachable using Protocol UDP and Port 3480
Relay : 52.115.63.242 is the actual relay instance (DIP)
Relay : 52.115.63.242 is reachable using Protocol UDP and Port 3481

Relay connectivity and Qos (Media Priority) check is successful for all relays.

```

Figure 3-6. Network connectivity and quality test

For network quality checker usage, from a command prompt, execute the tool by running `NetworkAssessmentTool.exe /qualitycheck`.

Here is the command:

```
C:\Program Files (x86)\Microsoft Teams Network Assessment Tool>NetworkAssessmentTool.exe /qualitycheck
```

This command initiates the media flow by starting the Teams call and then waiting for the call to end after 300 seconds, displaying call quality metrics every five seconds or so. Figure 3-7 shows the call quality metrics.

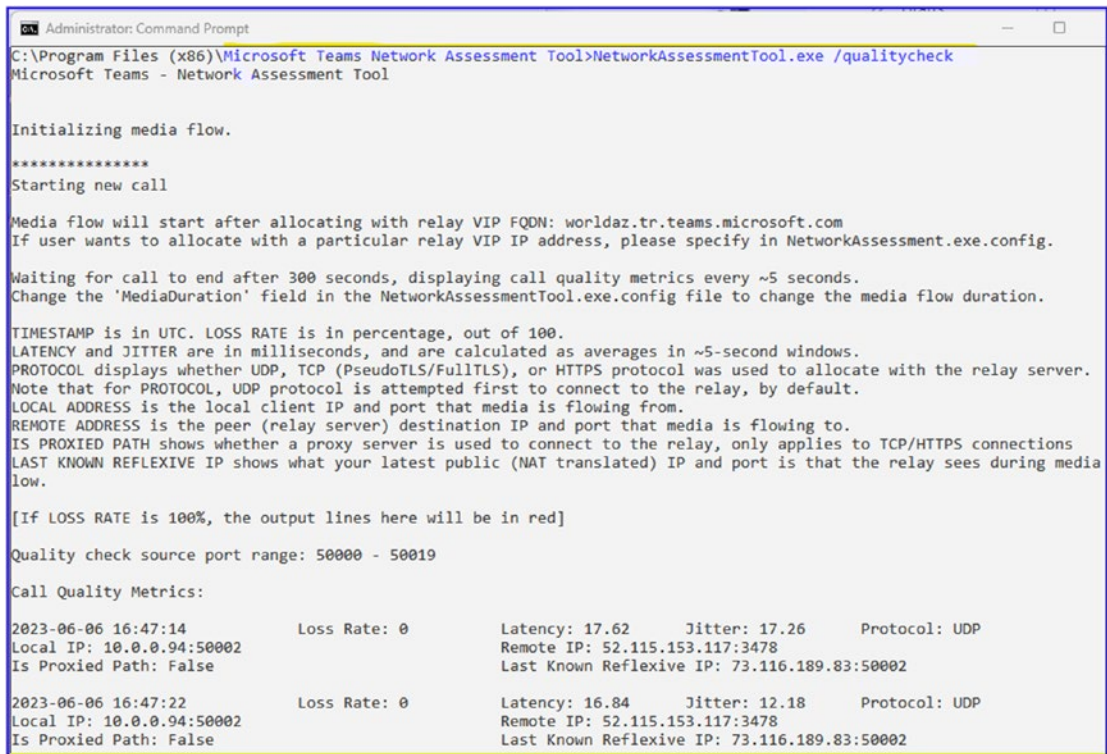


Figure 3-7. Media quality checks

The next thing you can test is the infrastructure connectivity; the test `infraconnectivitytest` performs HTTPS stack infra tests. Here is the command:

```
C:\Program Files (x86)\Microsoft Teams Network Assessment Tool>NetworkAssessmentTool.exe/infraconnectivitytest
```

This command checks multiple HTTP stack infra connectivity tests such as the following:

- Checking connectivity to <https://go.trouter.teams.microsoft.com/>
- Checking connectivity to <https://config.teams.microsoft.com/config/>
- Checking connectivity to <https://ic3.events.data.microsoft.com/Collector/3.0/>
- Checking connectivity to <https://api.flightproxy.teams.microsoft.com/api/v1/health>

The report, shown in Figure 3-8, summarizes the HTTP connectivity checks, results, and status.

```
Administrator: Command Prompt
C:\Program Files (x86)\Microsoft Teams Network Assessment Tool>NetworkAssessmentTool.exe /infraconnectivitytest
Microsoft Teams - Network Assessment Tool

2023-06-06 14:01:36.325 [#71c822d5-S] T#80416 [DEBUG2] [auf.log_config] Log console updated, adding log console
2023-06-06 14:01:36.325 [#40548b1b-S] T#80416 [DEBUG4] [auf.log_config] Not persisting log config, disabled
2023-06-06 14:01:36.325 [#13504ed8-S] T#80416 [ERROR] [auf.log_config] Text file logging not allowed in public clients
2023-06-06 14:01:36.325 [#6d7ac071-S] T#80416 [DEBUG2] [auf] Rotating log file: ....log
2023-06-06 14:01:36.325 [#8b56a8d8-S] T#80416 [DEBUG1] [auf] Opening log file ....log
2023-06-06 14:01:36.325 [#46925e77-S] T#80416 [DEBUG1] [auf] Current time: Local=2023-06-06T14:01:36.328 ; Utc=2023-06-06T21:01:36.328 ; tzBias=-25200s
2023-06-06 14:01:36.325 [#46925e77-S] T#80416 [DEBUG1] [auf] Current time: Local=2023-06-06T14:01:36.329 ; Utc=2023-06-06T21:01:36.329 ; tzBias=-25200s
2023-06-06 14:01:36.325 [#46925e77-S] T#80416 [DEBUG2] [auf.log_config] Log file updated, adding log file MaxSize=104857600 MaxRotations=10 Encryption=1 File=c....log
2023-06-06 14:01:36.361 [#46925e77-S] T#80416 [DEBUG1] [auf] Current time: Local=2023-06-06T14:01:36.361 ; Utc=2023-06-06T21:01:36.361 ; tzBias=-25200s
2023-06-06 14:01:36.361 [#40548b1b-S] T#80416 [DEBUG4] [auf.log_config] Not persisting log config, disabled

====
Checking connectivity to https://go.trouter.teams.microsoft.com/
2023-06-06 14:01:36.368 [#8420e817-S] T#80416 [DEBUG4] [httpstack.Init] Init
2023-06-06 14:01:36.368 [#d0cc8b0a-S] T#80416 [DEBUG4] [auf] auf::init() from C:\a_work\1\s\RootTools\roottools\auf\include\auf\auf_init.hpp:Tue Feb 21 16:53:06 2023 g_aufUp=1
2023-06-06 14:01:36.371 [#56a7ec71-S] T#80416 [DEBUG4] [spl.EcsConfig] Pushed keys: {}
2023-06-06 14:01:36.371 [#4d0fb7a0-S] T#80416 [DEBUG4] [auf] Spawning new worker (concurrency 0, cur count 0)
2023-06-06 14:01:36.371 [#af4d0c25-S] T#19100 [DEBUG4] [auf] New worker is created
2023-06-06 14:01:36.372 [#518a18f3-S] T#34888 [DEBUG4] [spl] Created thread 34888.
2023-06-06 14:01:36.372 [#c15bb53a-S] T#34888 [DEBUG4] [spl] threadWinEntry: Thread is at Win32 priority 0.
2023-06-06 14:01:36.373 [#4be6c0a9-S] T#80416 [DEBUG2] [httpstack] Configured backend RT, will use RT
2023-06-06 14:01:36.373 [#f576d4a0-S] T#80416 [DEBUG3] [httpstack.rt.Backend] @00dd7478: Created version 2023.09.00.20
2023-06-06 14:01:36.373 [#6e93c25d-S] T#80416 [DEBUG4] [httpstack] @00dfc248: Created
2023-06-06 14:01:36.373 [#e0ae1e2a-S] T#80416 [DEBUG2] [httpstack.Request] @0782e060: RQ1: Open GET "https://go.trouter.teams.microsoft.com/..."
```

Figure 3-8. *Infra connectivity test*

Figure 3-8 also shows the different HTTP stack infra tests and their results and status information.

Deploying and Managing Quality of Service

Microsoft Teams provides real-time communication, including persistent chat, audio and video calls (VoIP), conferences, desktop sharing, PSTN calls, content sharing, and so on. These capabilities, however, will increase the traffic on your existing network. It is increasingly important for you as a Teams admin to balance network performance with QoS. All of these modalities include signaling and media traffic, and this real-time traffic is latency sensitive. Microsoft Teams is a latency-sensitive application; to provide an optimal user experience using Teams audio, video, and application sharing, you must prioritize the Teams real-time media traffic against lower-priority traffic.

Quality of service (QoS) is a networking technology feature that can manage data traffic to reduce packet loss, latency, and jitter on the network. This can be crucial for applications such as Microsoft Teams, where network performance can greatly impact the user experience. Teams uses different sets of ports for signaling, audio, video, and desktop sharing, and these can be configured with different QoS values.

To set up QoS for Microsoft Teams, you need to perform the following steps:

1. **Define the QoS policy:** You first need to define the QoS policies in your network infrastructure (routers, switches, etc.). This usually involves defining differentiated services code point (DSCP) values for each type of traffic. For Microsoft Teams, you may use the following recommended values:
 - **Audio:** DSCP 46, port range 50000 to 50019
 - **Video:** DSCP 34, port range 50020 to 50039
 - **Desktop sharing:** DSCP 18, port range 50040 to 50059
 - **Signaling:** DSCP 26, port range 50000 to 50059
2. **Configure QoS on Windows:** You will need to configure the Group Policy settings in Windows to enforce these QoS policies. The policy settings are located under Computer Configuration ► Windows Settings ► Policy-based QoS.

You need to create a new policy for each type of traffic (audio, video, desktop sharing, signaling) with the corresponding DSCP and port range values. In the application name field, specify `Teams.exe` to apply these policies to Microsoft Teams.

3. **Configure QoS on macOS:** macOS does not have built-in support for DSCP marking. Therefore, you'll need to use third-party tools or a network device to perform DSCP marking for macOS devices. One approach is to use the network router or switch to classify the traffic based on its source port and apply the appropriate DSCP values.

There are different ways to prioritize network traffic, but the most common way is by using Differentiated Services Code Point (DSCP) markings. DSCP values can be applied or tagged based on port ranges and via Group Policy objects (GPOs). Because Microsoft Teams is available across the platform, including Windows, macOS, iOS, Android, and so on, applying port ranges via GPO will not work for non-Windows devices. It is a best practice that you use DSCP tagging based on port ranges on the network layer because it will work for all devices, including macOS, iOS, and Android devices. In fact, a combination of GPOs for Windows and DSCP tagging at the network layer will work better.

QoS is more beneficial when you configure it from end to end, meaning from the user computer to network switches to routers to the cloud (Office 365 Service), because any part of the path that fails to support QoS can degrade the quality of the entire call.

Microsoft Teams is a cloud-only service, so you don't have end-to-end control over the network. When network traffic leaves your management network, you will be dependent on the Internet, where you don't have much control. Basically, the interconnect network will be an unmanaged network Internet connection, illustrated in Figure 3-9. One option available to address end-to-end QoS is Microsoft Azure ExpressRoute, which requires an additional investment.

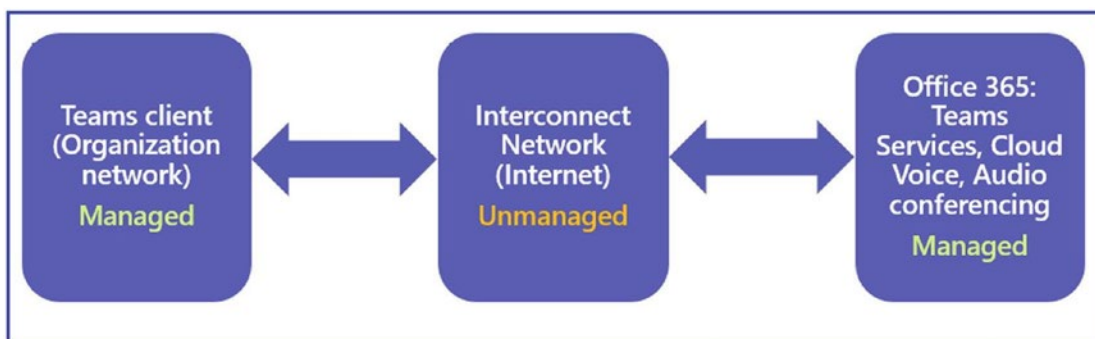


Figure 3-9. *Managed and unmanaged networks*

Even though you will not have end-to-end control on the network, it is highly recommended that you implement QoS on the portion of the network that you have control over, which is your on-premises network. This will increase the quality of real-time communication workloads throughout your deployment and improve chokepoints in your existing deployment.

Deploying Quality of Service for Microsoft Teams

For Teams traffic, you should use GPOs and DSCP marking using port ranges to accommodate Windows and non-Windows devices. This chapter covers only the QoS configuration at the endpoint level as well as the network layer. It is a best practice to use a GPO to grab the majority of clients and to use port-based DSCP tagging to ensure that mobile, Mac, and other clients will still get QoS treatment (at least partially).

Table 3-3 shows the DSCP values and client source port ranges that are recommended for Microsoft Teams media traffic.

Table 3-3. *Teams Media Category with Client Source Port Ranges*

Client Source Port Range	Protocol	Media Category	DSCP Value	DSCP Class
50,000–50,019	TCP/UDP	Audio	46	Expedited Forwarding (EF)
50,020–50,039	TCP/UDP	Video	34	Assured Forwarding (AF41)
50,040–50,059	TCP/UDP	Application/ Desktop Sharing	18	Assured Forwarding (AF21)

Applying DSCP Marking at Network Layer

To implement DSCP marking on network devices, you as a Teams admin need to work with network engineers to configure port-based DSCP tagging by using access control lists (ACLs) on network devices (switches and routers); basically, the network engineer will configure devices to mark the Teams audio, video, and application sharing traffic at the ingress/egress routers typically located on the WAN based on the client source port ranges defined for each modality. Although this works across platforms, it marks traffic only at the WAN edge, not all the way to the client computer; therefore, this incurs management overhead.

To set this up, you can discuss and share Teams client source port ranges with DSCP classes and values with your network engineer.

DSCP Marking at Endpoint Level Using Policy-Based QoS

QoS policies are applied to a user login session or a computer as part of a GPO that you have linked to an Active Directory container, such as a domain, site, or organizational unit (OU). QoS traffic management occurs below the application layer, which means your existing applications do not need to be modified to benefit from the advantages that are provided by QoS policies.

For Microsoft Teams, we need to set up QoS policies for computer configuration so that whoever logs in to a computer and uses the Teams client will have the policy applied.

The following is the GPO path: Default Domain Policy ► Computer Configuration ► Policies ► Windows Settings ► Policy-Based QoS.

Follow these steps to implement policy-based QoS for Teams.

1. First, define the Teams client source port ranges on the Teams admin center. Log in to the Teams admin center, then go to a meeting, and finally go to the meeting settings under Network (<https://admin.teams.microsoft.com/meetings/settings>).
 - a. Turn on “Insert Quality of Service (QoS) markers for real-time media traffic,” as shown in Figure 3-10.
 - b. Select “Select a port range for each type of real-time media traffic,” as shown in Figure 3-10.
 - c. Update starting and ending port ranges with media traffic type. Figure 3-10 shows the media port ranges.

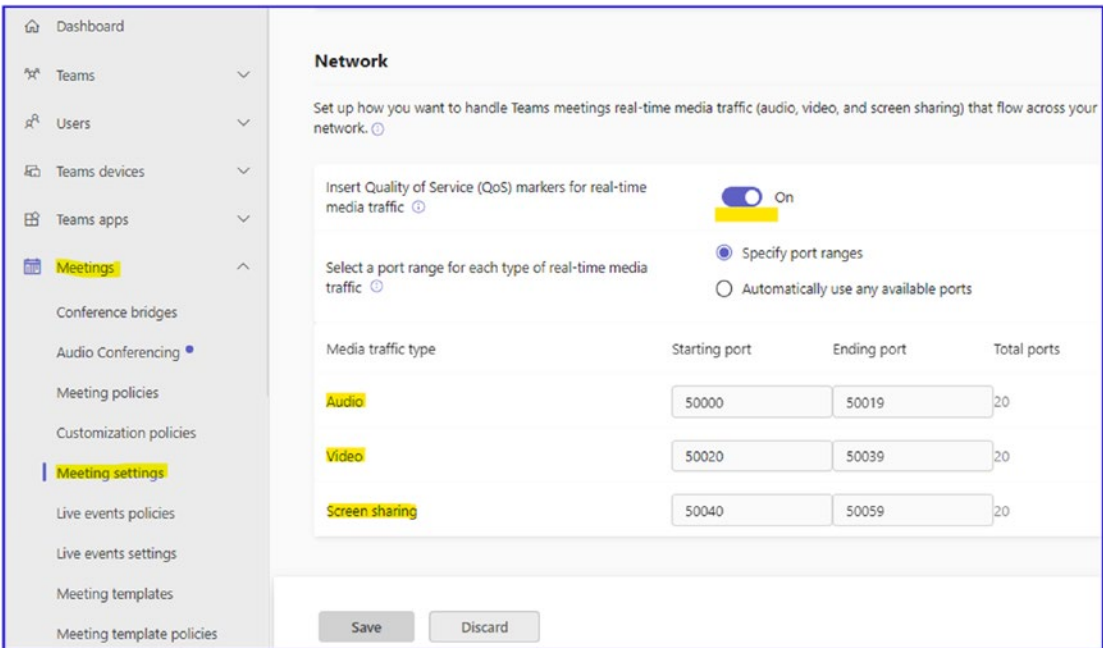


Figure 3-10. Configuring media port ranges

You can set up a port range using PowerShell as well.

2. Configure a separate GPO for each modality.

After defining the port ranges in the Teams admin center, you must create QoS policies that specify the DSCP values to be associated with each port range. Basically, restricting a set of ports to a specific type of traffic does not result in packets traveling through those ports being marked with the appropriate DSCP value. In addition to defining port ranges, you must also create QoS policies that specify the DSCP value to be associated with each port range. This DSCP value's association with a port range can be achieved via GPO, which is called *policy-based QoS*. With QoS policy, you can configure and enforce QoS policies that cannot be configured on routers and switches. A QoS policy provides the following advantages:

- QoS policies are easier to configure by using a user-level QoS policy on a domain controller and propagating the policy to the user's computer.

- QoS policies are flexible. Regardless of where or how a computer connects to the network, QoS policy is applied. The computer can connect using Wi-Fi or Ethernet from any location.
- Some QoS functions, such as throttling, are better performed when they are closer to the source. QoS policy moves such QoS functions closest to the source.

If you already have all the port ranges and DSCP values with media category type, then proceed to the next step. If not, then decide on port ranges and follow step 2 for configuring port ranges. Microsoft outlines the complete steps and port ranges at <https://docs.microsoft.com/en-us/microsoftteams/qos-in-teams>.

- a. You must have consolidated all your computer objects to a single OU. For example, the Bloguc organization consolidated all computers under the PC OU to apply the GPO correctly. You can apply a single GPO to multiple OUs; however, for better management, consolidate objects into one OU and then apply the policy.
- b. Log in to the domain controller or computer that has Group Policy Management installed.
- c. Open the Group Policy Management tool (Run ► `gpmc.msc`) and then right-click the OU (Computer). Click Create A GPO In This Domain And Link It Here to create a new GPO such as TeamsClient-QoS. You must have the required permission (domain admin or the like) to create and link the policy object permission.
- d. Select the newly created GPO and right-click it. Select Edit to Open Group Policy Management Editor. Expand Computer Configuration ► Policies ► Windows Settings. Right-click Policy-based QoS, then select Create New Policy, as shown in Figure 3-11.

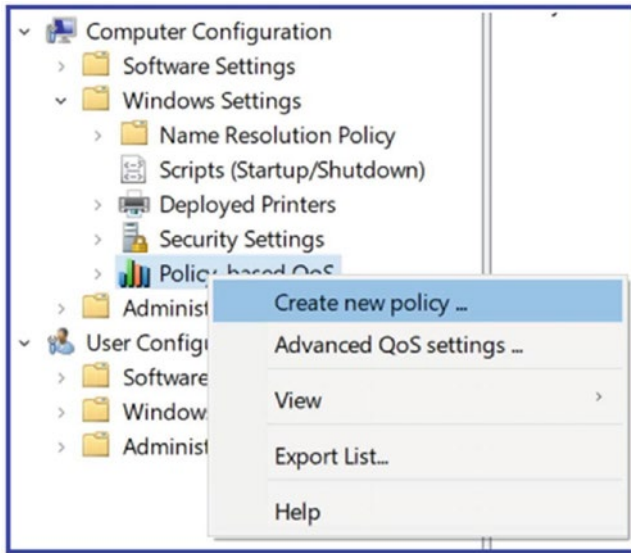


Figure 3-11. Policy-based QoS

- e. On the Policy-based QoS page, shown in Figure 3-12, give the policy a name, such as Teams Audio. Select the Specify DSCP Value check box and enter the value **46**. Click Next.

Policy-based QoS

Create a QoS policy

A QoS policy applies a Differentiated Services Code Point (DSCP) value, throttle rate, or both to outbound TCP, UDP, or HTTP response traffic.

Policy name:
Teams Audio

Specify DSCP Value:
46

Specify Outbound Throttle Rate:
1 KBps

[Learn more about QoS Policies](#)

< Back Next > Cancel

Figure 3-12. Specifying the policy name and DSCP values

- f. On the next page, shown in Figure 3-13, select the Only Applications With This Executable Name option, and enter **Teams.exe**. Click Next.

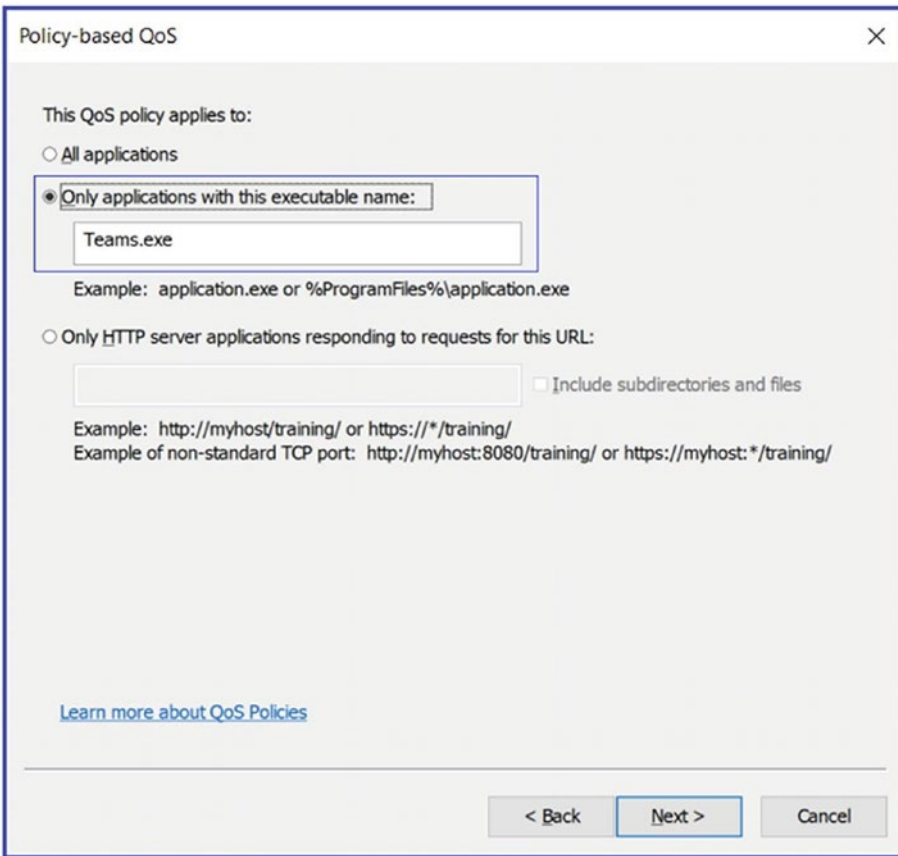


Figure 3-13. Application name

Note This simply ensures that the Teams .exe application will match packets from the specified port range with the specified DSCP code.

- g. On the next page, make sure that both the Any Source IP Address and Any Destination IP Address options are selected, as shown in Figure 3-14. Click Next.
-

Note These two settings ensure that packets will be managed regardless of which computer (IP address) sent those packets and which computer (IP address) will receive those packets.

Figure 3-14. Selecting the IP addresses that the QoS policy applies to

- h. On the next page, for the Select the Protocol This QoS Policy Applies To setting, select TCP and UDP. Select From This Source Port Number Or Range. Also, enter a port range reserved for audio transmissions (50000–50019) and select To Any Destination Port. Figure 3-15 shows protocol and port range configuration information.

Note Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are the two networking protocols most commonly used by the Microsoft Teams service and its client applications.

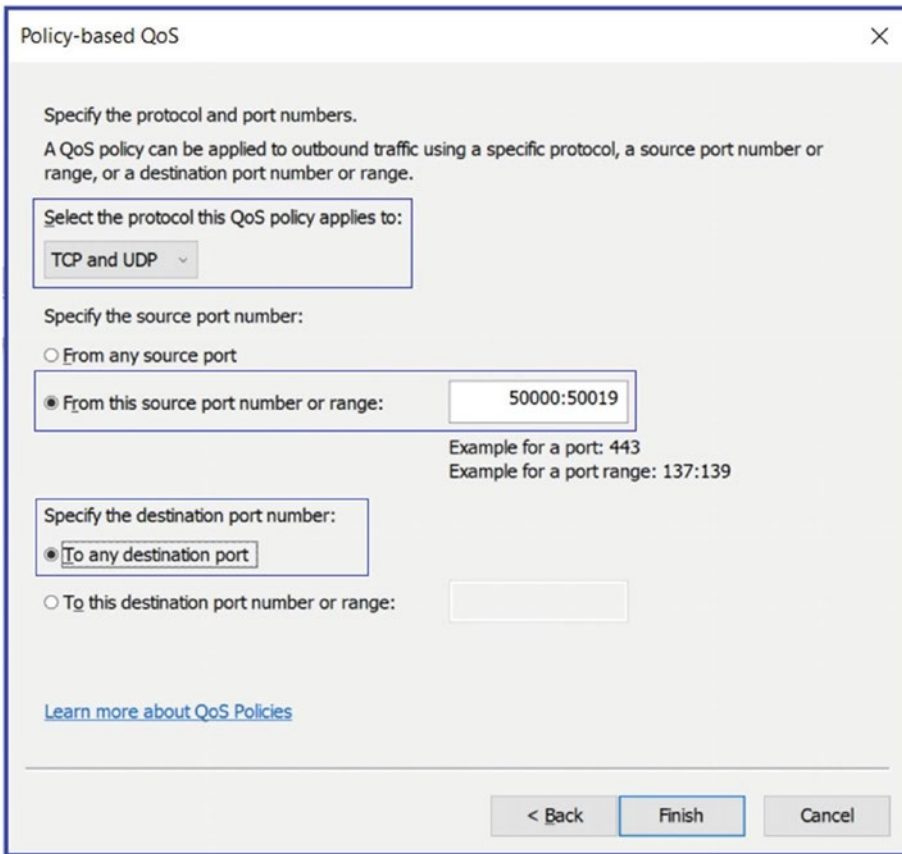


Figure 3-15. *Defining the source port number or range*

- i. Follow steps e to h and create new policy objects as Teams Video and Teams Sharing with the given port ranges and DSCP values.
- ii. After you are finished configuring all policy objects, it will look like Figure 3-16.

Policy Name	Application	Name o...	Protocol	Source Port	Destination ...	Source IP / P...	Destination ...	DSCP Value
Teams Audio	Teams.exe		TCP and UDP	50000:50019	*	*	*	46
Teams Video	Teams.exe		TCP and UDP	50020:50039	*	*	*	34
Teams Sharing	Teams.exe		TCP and UDP	50040:50059	*	*	*	18

Figure 3-16. *All policies*

3. Finally, test the QoS. As a best practice, you must validate QoS configuration and DSCP tagging on a quarterly basis.

Verifying QoS Policies Are Applied

After QoS policy configuration, you must verify all QoS settings. There are multiple ways to verify the QoS.

- **Using Registry on the Windows local computer:** Once the GPO pushed and applied to the computer, you can force the GPO to the local computer by running the command `gpupdate.exe /force`. Then visit the Registry path `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\QoS\Teams Audio` to verify that QoS policies have been applied. Figure 3-17 shows Teams Audio, Teams Video, and Teams Sharing policies with port ranges and DSCP values.

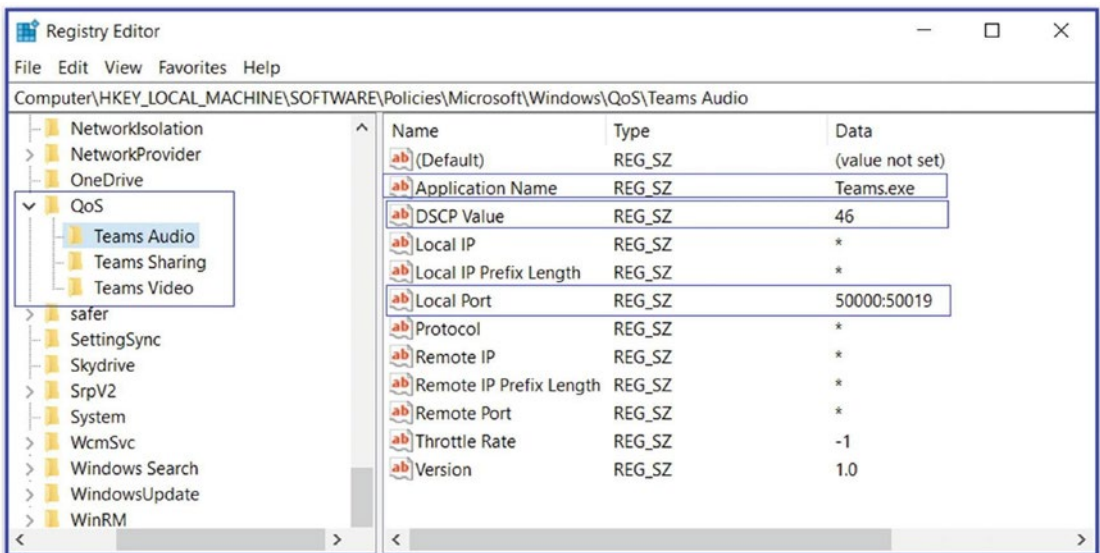


Figure 3-17. Verifying QoS using local computer registry

- **Validate QoS tagging using packet capture:** You need Wireshark as a network packet capturing tool. Start a Teams audio/video meeting and capture the network traffic via the Wireshark tool (it is a freeware tool that you can download and install on your computer).

Figure 3-18 shows Teams audio traffic (the source is 10.0.0.207 and destination is 104.42.192.49) protocol UDP with the port number 50018. This packet shows DSCP marked as EF (expedite forwarding as DSCP 46). Verify the two-way traffic to get QoS benefits.

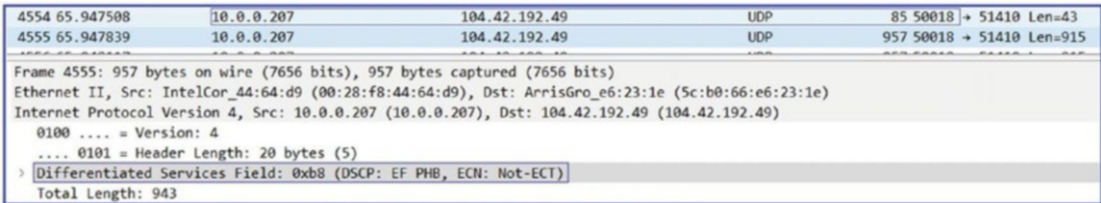


Figure 3-18. Validating QoS tagging

Deploying VPN Split Tunnel for Microsoft Teams Media Traffic

A virtual private network (VPN) provides a secure, encrypted connection between a user’s device and a private network. Traditionally, all traffic from a user’s device is sent over the VPN, which can ensure security but also lead to bandwidth issues, particularly when dealing with heavy traffic such as video calls and meetings.

It’s common for an organization to use remote access or a VPN solution that offers an encryption tunnel between endpoints, like remote users and the corporate network. Usually, VPNs are not designed to support real-time media traffic and introduce an extra layer of encryption on top of Teams media traffic that is already encrypted. This means it adds overhead to Teams media packets. Additionally, connectivity to the Teams service (Microsoft 365) might not be efficient due to hair-pinning traffic through a VPN device. For VPNs, the suggestion is to provide an alternate path that bypasses the VPN tunnel for Teams traffic. This is generally known as *split-tunnel VPN*.

Understanding Split-Tunnel VPN for Teams Media Traffic

With split tunneling, only traffic destined for the private network is sent over the VPN. Other traffic goes directly over the public Internet. This has several benefits for Microsoft Teams:

- **Bandwidth optimization:** Since only necessary traffic is sent over the VPN, it reduces the overall bandwidth consumption on the VPN connection. This means less congestion and better performance for Teams calls and meetings.
- **Better performance:** Teams is a latency-sensitive application, meaning it performs better with lower network delays. By sending Teams traffic directly over the Internet, it can take a more direct and faster route to Microsoft's servers, reducing latency.
- **Scalability:** Since less traffic is sent over the VPN, it can support more users without needing to upgrade the VPN infrastructure.
- **Reduced load on VPN gateways:** Offloading Teams traffic from the VPN connection reduces the load on the VPN gateways, increasing their longevity and decreasing maintenance costs.

Because there are multiple VPN solutions available in the market and every solution vendor might have a different process to implement split-tunnel VPN, this topic covers general recommendations as to what should be configured on the VPN solutions. There are multiple rationales for which you, as a Teams admin, must implement split-tunnel VPN.

- For Microsoft Teams conversation and collaboration features, VPN or remote access connections are usually acceptable because the network qualities are frequently not visible to the end user. If a chat message arrives a second or two later, there would be only a minor impact. The same is not applicable for keeping a bidirectional conversation in real time, like a Teams audio call.
- Microsoft Teams uses a number of codecs, and they have different packetization times. However, VPN solutions add another layer of encryption and decryption, which greatly increases network latency on these packets getting to their destination in a timely manner. When these Teams media packets are delayed or received out of order, jitter increases, and the receiving endpoint will attempt to fill in and stretch the audio to fill in the gaps, which usually results in undesired audio effects such as robotic noise, voice speed up, and so on.

- A VPN solution contributes to intermittent difficulties such as random network disconnections, which will cause the Microsoft Teams session to disconnect (disruption of the signaling path) or media quality issues. This would generally indicate a need for increased capacity on the VPN solution. However, when the VPN solution was designed, this likely wasn't factored in, and the media usage is degrading the overall VPN experience for other applications as well.
- Clients who have configured their VPN solution to exclude Microsoft Teams traffic or implement split-tunnel VPN have seen great returns in user satisfaction not specific to the Teams audio and video experience. For this purpose, we strongly recommend leveraging the steps that follow to complete a split-tunnel VPN for Teams media traffic over VPN solutions.

Some Recommendations Before Implementing VPN Split Tunnelling

Before implementing split tunneling, it's important to understand your organization's security requirements, as it can increase exposure to Internet-based threats. For example, at Cyclotron, Inc., we have implemented VPN split tunnelling, which has improved our Teams call quality drastically over VPN connections.

Here are some recommendations:

- **Security assessment:** Conduct a risk assessment before implementing split tunneling to ensure it aligns with your organization's security policy.
- **Traffic monitoring:** Regularly monitor network traffic to detect any abnormal behavior or potential security threats.
- **Selective split tunneling:** Rather than implementing split tunneling for all traffic, consider only implementing it for Teams media traffic to balance performance with security.
- **VPN choice:** Choose a VPN solution that fits your organization's needs, both in terms of features and scalability.

- **Network optimization:** Regularly review and optimize your network to ensure it continues to support the needs of your organization as they evolve.
- **Microsoft recommendations:** Follow Microsoft's guidance for implementing VPN split tunneling with Teams. They provide documentation and support that can be invaluable during the process.

Remember that while split tunneling can improve performance, it may not be suitable for all organizations, particularly those with strict security requirements. Always weigh the benefits against the potential risks before implementing.

Split-Tunnel VPN Architecture

A VPN split tunnel architecture for Microsoft Teams media traffic would involve both your private network (with the VPN server) and the public internet. Here's a basic layout:

- **User device:** This is the starting point of the network traffic. It could be a laptop, desktop, or mobile device running the Microsoft Teams client.
- **VPN client:** Installed on the user device, the VPN client handles creating the secure connection to the VPN server and managing the split tunnel.
- **VPN server:** This server resides within your organization's private network and manages the incoming VPN connections. The VPN server also applies the split tunnel rules.
- **Private network:** This is your organization's internal network, where private resources (such as file servers, intranet websites, etc.) reside. Traffic to these resources goes over the VPN.
- **Public Internet:** Traffic not destined for the private network, such as Microsoft Teams media traffic, goes directly over the public internet.

When a Microsoft Teams call or meeting is started, the following happens:

- Signaling traffic (used to initiate the call or meeting) is sent from the Teams client on the user device to the Teams service over the Internet, bypassing the VPN.
- Once the call or meeting is established, the media traffic (audio, video, and screen sharing) also goes directly from the Teams client to the Teams service over the internet, bypassing the VPN.
- Other traffic, such as access to file servers or other private resources, is sent over the VPN to the private network.

This setup ensures that Teams media traffic takes the most direct path to the Teams service, reducing latency and improving call quality. It also reduces the load on the VPN server, freeing up bandwidth for other traffic.

In this scenario, the VPN client and VPN server are configured to allow Microsoft Teams traffic (based on specific ports and/or IPs) to bypass the VPN while sending other traffic over the VPN. This is often done through firewall rules or specific VPN configuration settings.

For this setup to work, both the VPN solution and the network infrastructure must support split tunneling, and the VPN client must be correctly configured on the user devices. It's also important to note that while this architecture can improve Teams performance, it can potentially expose Teams traffic to Internet-based threats, so appropriate security measures should be taken.

The VPN split tunneling solution for Microsoft Teams provides optimal call quality to the end user who uses Teams over VPN. In a split-tunnel VPN configuration, all IP addresses that are used by the Microsoft Teams services (Office 365) environment are excluded so that traffic to and from those IP addresses is not included in the VPN tunnel. This means the split-tunnel VPN must work exactly the same way as the external Teams client should. Most VPN solution providers support split-tunnel VPN; you must check the configuration for your VPN solution by checking the vendor documentation. Figure 3-19 shows how split-tunnel VPN works.

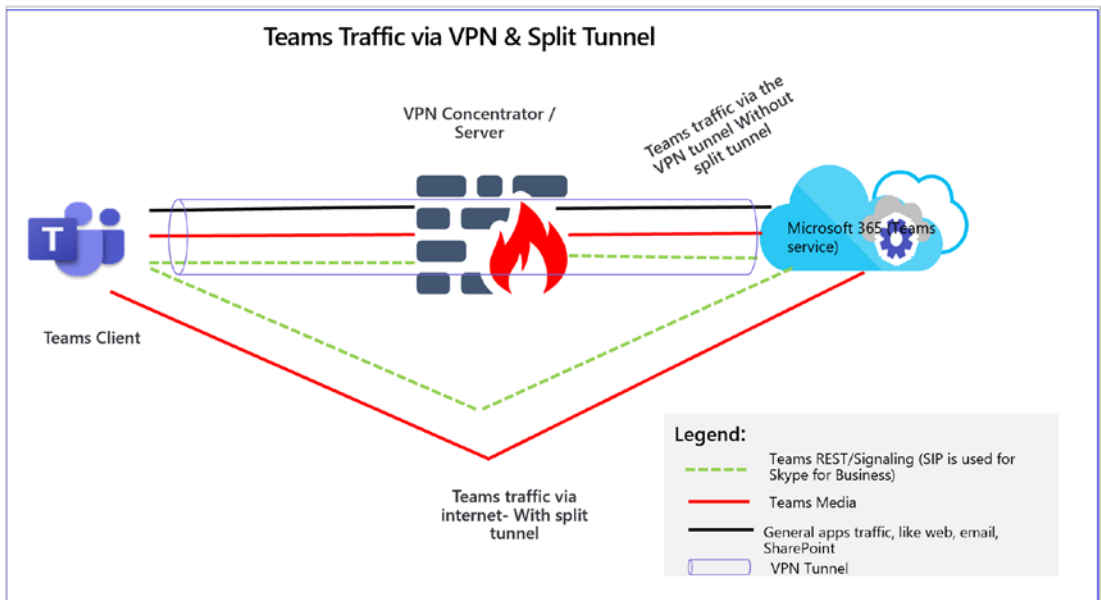


Figure 3-19. Split-tunnel VPN traffic flow

All Microsoft Teams signaling and media traffic split from the VPN secure tunnel, as shown in Figure 3-19, and go through Microsoft Teams service (Office 365). To redirect users away from the VPN solution for Teams, it must first be configured to support a split tunnel, which is a popular feature of today's VPN appliances. Split-tunnel VPN allows Teams traffic without going through the VPN tunnel. For example, the external web traffic from the Teams site (`teams.microsoft.com`) does not traverse over the VPN solution. Without split tunnel, the default VPN configuration will force all the Teams traffic through the VPN tunnel.

Implementing Split-Tunnel VPN

There might be different way to achieve a VPN split tunnel for Teams media and signaling traffic, such as using a firewall or third-party VPN solution. I have mentioned here one of the ways that is commonly used to configure VPN split tunneling using a third-party VPN.

Using a Third-Party VPN Solution

In this topic, we cover split-tunnel VPN configuration based on the Pulse secure VPN solution as an example. I strongly recommend contacting your VPN vendor for split-tunnel configuration documentation. There are different approaches and solutions to implement split-tunnel VPN, and I present here a combined solution to use a VPN concentrator and your corporate firewall.

We are creating a policy on a VPN concentrator to exclude Microsoft Teams service IP addresses (Office 365) traffic from the VPN tunnel. This means denying signaling and media traffic via the VPN tunnel for Teams service IP addresses (Office 365). Then, using your corporate firewall, create a deny rule to deny traffic sourced from the VPN user subnet to Teams service IP addresses (Office 365) and from Teams service IP addresses (Office 365) to VPN user subnets both ways.

The split-tunnel solution is a combined solution using a VPN concentrator and your firewall.

1. First, get all Teams service IP addresses, including optimized required and allow required. Refer to the Microsoft documentation for Teams service IP addresses at <https://docs.microsoft.com/en-us/Office365/Enterprise/urls-and-ip-address-ranges>.
2. Create a policy on a VPN concentrator, which will exclude traffic via VPN tunnel for all Teams service IP addresses (refer to the preceding URL for Teams IP addresses). In other words, deny traffic or split tunnel to these Teams IP addresses from your VPN tunnel and assign this policy to all other policies and users.
3. Now work with your network firewall team and do this. Split Teams conferencing (media) traffic to external (not via VPN tunnel).

Remember, all-conference modality traffic is involved through a multicontrol unit (MCU) running on Teams service (Office 365). First, create the following firewall rules:

- Create a firewall rule that will block traffic going from VPN user subnets to Teams service IP addresses or subnets (Office 365). Refer to the earlier Microsoft documentation link.

- Create another firewall rule that will block traffic going from Teams service IP addresses or subnets (Office 365) to the VPN user subnet.

To implement split-tunnel VPN for Teams one-to-one call traffic, you must create more rules on your corporate firewall.

Apart from the Teams conferencing traffic, you can enable the blockage of the UDP/TCP source port for Teams audio, video, and application sharing. Basically, Microsoft Teams, by default, has a limited scope of UDP/TCP ports it will be using as the source ports for communication. If you block these source ports from entering the VPN tunnel, then the media should go via the external split from the VPN tunnel. That will ensure that even two users both connected via VPN and their Teams media traffic will not allow hair-pinning via their VPN connection but go directly from one Internet connection to the other.

The sample firewall rules look like this:

- Create a firewall rule source address from the VPN_Users subnet to the destination as Any with the application Stun and Teams (if allowed) and Service port (UDP/TCP port ranges of audio, video, and application sharing).
- Create another firewall rule source from any address to the destination VPN_Users subnet with the application Stun and Teams (if allowed) and Service port (UDP/TCP port ranges of audio, video, and application sharing).

You can get Teams audio/video and application sharing client port ranges from the Teams admin center. Log in to the Teams admin center, and go to a meeting. In Meeting Settings, under Network, select Get New Image.

DOES THIS TOPIC APPLY TO SKYPE FOR BUSINESS ONLINE?

Yes, this applies to Skype for Business Online as well, because Microsoft Teams and Skype for Business Online share the same IP subnets and ports.

Verifying VPN Split Tunneling

To verify the VPN split tunnel, you must connect using the external network (wired or wireless) and then connect the VPN, which has the split tunnel implemented.

1. Make a Teams one-to-one call and capture network traces using Wireshark or Network Monitor. Verify the Teams media (UDP) traffic going between your local IP address and other third-party local IP addresses (not via VPN IP addresses).
2. Join the Teams meeting, and capture network traces using Wireshark or Network Monitor. Verify the Teams media (UDP) traffic going between your local IP address and Teams service IP address (Office 365) transport relay and not via VPN IP addresses.

Note For the Teams service IP addresses or subnet block rule on the firewall, set the action to Reset instead of denying. That allows for a faster Teams client sign-in.

Providing optimal experience to the end-user community is our main goal, and using VPN split tunneling helps to achieve this through blocking the Teams client from connecting via VPN tunnel. The media will then always go through externally, not via VPN tunnel, which will eliminate extra hops, double encryption, and so on.

Security and Compliance Requirements for Teams Deployment

Before deploying Microsoft Teams in an organization, it is crucial to understand and meet the necessary security and compliance requirements.

- **Data security:** Teams is built on the Office 365 hyper-scale, enterprise-grade cloud, delivering the advanced security and compliance capabilities. Data in Teams resides in Exchange, SharePoint, and OneDrive for Business, so protection, detection, and response capabilities cover the security spectrum.

- **Identity and access management:** It is important to ensure only authorized individuals have access to your Teams data. This involves setting up appropriate user authentication and authorization methods such as multifactor authentication (MFA), single sign-on (SSO), and conditional access.
- **Data compliance:** Teams is Tier-C compliant including standards such as ISO 27001, ISO 27018, SSAE16 SOC 1, and SOC 2, HIPAA, and EU Model Clauses (EUMC). Data residency commitments also apply to Teams.
- **Data governance and retention:** Organizations must set up data retention policies according to their needs and the regulatory landscape of their industry. Teams allows admins to set up granular data retention policies.
- **Audit logs:** Teams provides a unified audit log in the Security & Compliance Center for events, and teams-related information is logged into the Office 365 audit log for review.
- **Privacy and transparency:** Teams follows the Office 365 Privacy and Trust Center commitments such as access control, auditing and compliance, certification and compliance, and more.

Benefits of Security and Compliance Planning

Thorough security and compliance planning before deploying Microsoft Teams provides several benefits.

- **Risk mitigation:** By understanding and addressing potential security risks up front, organizations can significantly reduce the chance of data breaches and other security incidents.
- **Regulatory compliance:** Compliance planning helps organizations meet industry-specific regulatory requirements, such as HIPAA for healthcare or the GDPR for EU data protection, avoiding potential legal issues and penalties.

- **Trust and reputation:** Having strong security and compliance measures in place helps build trust with customers, partners, and employees, thereby enhancing the organization's reputation.
- **Data protection:** Proper data governance and retention policies ensure that organizational data is properly stored, managed, and protected.
- **Operational efficiency:** A well-planned security and compliance strategy can streamline operations, making it easier to manage and monitor Teams deployment.
- **Cost savings:** By avoiding potential security incidents and regulatory fines, organizations can save significant costs in the long term.

By meeting the security and compliance requirements for Teams deployment, organizations can ensure they get the most out of the platform while minimizing potential risks and issues.

Training and Change Management for Teams Deployment

A successful transition to Microsoft Teams requires not only technical readiness but also comprehensive training and effective change management strategies.

- **Understanding Teams:** Before initiating training, ensure that everyone in the organization understands the purpose, value, and benefits of Teams. This can be done through seminars, workshops, and introductory meetings.
- **Training programs:** Develop detailed training programs for different user groups. This could include live training sessions, online courses, tutorial videos, and quick reference guides. Training should cover all aspects of Teams, from basic functionality to advanced features.

- **Change management:** Implementing a new tool like Teams can cause disruption. Effective change management strategies can help manage this transition smoothly. This could involve regular communication updates, providing ample resources for self-learning, and appointing “champions” or power users who can help others in their team.
- **Support and feedback:** After deployment, provide ongoing support to address any issues or challenges that users might face. Establish clear channels for users to provide feedback or ask questions.

Benefits of Training and Change Management

Effective training and change management during Teams deployment offer several benefits:

- **Higher adoption rates:** Proper training ensures users understand how to use Teams effectively, leading to higher adoption rates.
- **Improved productivity:** When employees understand how to use all the features of Teams, they can leverage the platform to work more efficiently and collaboratively.
- **Reduced resistance:** Change can often meet resistance in an organization. Effective change management can help ease this transition and reduce resistance to the new tool.
- **Lower support costs:** When users are well-trained, they will encounter fewer issues, resulting in lower support costs.
- **Feedback loop:** Establishing clear channels for feedback helps the organization understand the challenges users are facing and how the deployment can be improved.
- **Employee satisfaction:** When employees feel supported during the transition and understand how to use the new tool, it can lead to higher overall job satisfaction.

In conclusion, training and change management are crucial elements of successful Teams deployment. They help ensure that the organization can effectively use the platform, leading to higher productivity and collaboration.

Microsoft Teams Adoption Strategy

Creating an effective adoption strategy is critical to ensure your organization gets the most from Microsoft Teams. The adoption process involves more than just technical deployment; it's about driving a change in how people work and collaborate. The following are the key steps to creating a successful adoption strategy.

Identify Business Objectives and Use Cases

This involves the following:

1. Understand what your organization wants to achieve with Microsoft Teams. Is it to streamline communications, enhance collaboration, reduce emails, or all of the above? Next, identify specific use cases that align with these objectives. Use cases could be department-specific or project-specific. They provide concrete examples of how Teams can be used to improve processes and productivity.
2. Define success metrics. Set clear, measurable goals to track the success of your Teams deployment. These could include user engagement metrics (such as the number of active users or the frequency of use), productivity metrics (such as the reduction in email usage or faster project completion times), and satisfaction metrics gathered through user surveys.
3. Develop a champions program. Identify and recruit enthusiastic individuals from different departments to be Teams “champions.” These individuals will receive additional training and will play a crucial role in driving Teams adoption within their respective departments. They can provide peer support, share success stories, and give feedback from the ground level.

Prepare a Training Plan

Based on your use cases and user roles, prepare a comprehensive training plan. The training could be in the form of workshops, webinars, one-on-one sessions, online courses, and self-help resources. Remember that training is not a one-time event; refresher courses, tips, and tricks, and updates about new features should be provided regularly.

1. **Communicate:** Keep all users informed about the rollout plan, training schedules, and where they can get help if needed. This ongoing communication helps to manage expectations, reduce resistance to change, and increase user confidence.
2. **Pilot and iterate:** Consider running a pilot with a small group of users before a full-scale rollout. The pilot will help you identify potential issues, understand user feedback, and make necessary adjustments before deploying Teams across the organization.
3. **Launch and monitor:** After successful testing and iteration, launch Teams to the entire organization. Post-launch, monitor the success metrics you've defined and take corrective actions if needed. Keep channels for feedback open and make sure users are supported throughout their journey.
4. **Celebrate success:** Recognizing and celebrating success is an important part of the adoption strategy. It could be sharing success stories, acknowledging active users or departments, or celebrating milestones like 100 percent deployment.

Remember, a successful Teams adoption strategy is not just about deploying the technology. It's about changing habits and driving a new way of working that aligns with your organization's culture and objectives. Be patient and persistent. Change takes time, and the journey to full adoption is a marathon, not a sprint.

Summary

This chapter underscored the pivotal role of network preparedness and bandwidth planning in facilitating a smooth Microsoft Teams deployment. It elaborated on the integral steps required to assess the network's current state, the potential adjustments needed, and the planning of bandwidth in accordance with calling scenarios and meetings.

Network assessment provides a detailed examination of the existing network infrastructure, revealing its readiness to support the implementation of Microsoft Teams. Highlighting the importance of a robust and stable network, the chapter furnished insights on potential enhancements needed to ensure optimum performance.

Bandwidth planning defines how effectively Teams can operate, particularly in regard to calling scenarios and meetings. The chapter illustrated the bandwidth requirements, demonstrating the relationship between the quality of calls and meetings and the network's capacity.

In this chapter, you learned detailed information about network assessment and bandwidth planning for Teams, how to deploy and manage QoS, and how to deploy split-tunnel VPN for Microsoft Teams media traffic. Before the deployment of Microsoft Teams in a production environment, you, as an admin, need to evaluate if the existing network meets the networking requirements of Microsoft Teams. Make sure you have the required bandwidth, access to all required IP addresses, the correct ports opened, and that you are meeting the performance requirements for Teams real-time media traffic such as audio, video, and application sharing.

This detailed investigation of organizational readiness sets the stage perfectly for our next chapter. Moving from the foundation of a reliable network and effective bandwidth planning, we will now venture into the intricacies of managing Teams' audio conferencing and phone system. This will help us explore the impressive potential of Teams as a comprehensive communication and collaboration platform.