4 Steps to Ensure Network Performance for Remote Workers

Keep employees connected and productive
The new normal when remote work surges unexpectedly

There has been an ongoing trend of virtual workers over recent years. OWL Labs reports that 62 percent of the respondents to their 2019 survey work from home at least occasionally. However, a sudden shift from an in-office work environment to remote work impacts both the way people work and interact, and the resulting demands placed on digital services, IT systems, and the supporting infrastructure. This is especially true for the enterprise network.

Whether the move to remote workers is planned or a response to an unexpected event, there are several considerations for IT to ensure remote workers have the experience they need to successfully conduct business.

Remote workers use the network for a variety of different work, placing different capacity demands on the company’s network. Typical workloads include online meetings, audio-only, audio and presentations or audio and video, across a variety of locations and with a varying number of participants.

As you make the transition to work-from-home, it’s crucial to make sure that your network bandwidth can support the staff and workloads at all times. But how do you go about this? It’s entirely possible that you’ll need to add bandwidth—but how much? Which metrics should you be looking at, and how will you analyze them? If users are experiencing slowdowns, how can you be sure it’s a matter of network capacity and not a network server problem?

In this ebook, we’ll look at a four-step process for modeling network capacity to ensure that you have the network bandwidth needed to support your remote workers.
Ensuring adequate bandwidth for remote workers

The process to evaluate the network capacity for supporting remote workers is relatively straightforward:

1. **Model your current network** bandwidth to understand utilization

2. **Analyze your bandwidth** use in a remote work scenario to see whether expansion is needed

3. **Model business continuity scenarios**, including the impact of a potential network failure, how the load could be distributed, and what this would do to the remaining networks

4. **Correlate end user response** times for applications to determine whether a slowdown results from a network issue or a compute issue

To perform these steps, you first need to gather metrics data from across your network, including:

- Number of VPN active sessions
- Internet utilization
- Bandwidth of network interface
- Link usage per connection
- Input bit rate by network interface
- Output bit rate by network interface
- Response times
- CPU utilization

Depending on your environment, your data sources might include network monitoring tools such as Entuity, HP NNMI, Solarwinds, and CSV files; as well as end user response data from application performance monitors like Dynatrace, Splunk, AppDynamics, and BMC Helix AppVisibility.

In the following steps, BMC Helix Capacity Optimization was used to do the network capacity modeling.
Step 1 – Model your current bandwidth

The first step for supporting your remote workforce is understanding the “normal” use of your network. The Quick Analysis, Analysis, and Network views in BMC Helix Capacity Optimization can help you visualize total current active VPN sessions as well as VPN sessions per location, as in the example to the right.

Keep in mind that bandwidth utilization will be different per access point. Historical views will help you understand seasonal factors that might come into play in your new remote work scenario as well. As the shift to remote work begins, continue to analyze and visualize active VPN sessions over time to look for trends or potential anomalies.

This view helps you understand current bandwidth utilization on network interface devices and predict projected bandwidth utilization over time. With this insight, you can anticipate spikes in usage to prevent slowdowns and saturation.
Step 2 – Analyze the impact of remote work on your network

The next step is to make sure that your network devices and servers do not become performance bottlenecks. In the example below, you can see a spike in AnyConnect device CPU utilization as an increase in work-from-home begins, but the real question is whether this will push levels beyond the threshold your environment can handle.

In this example, we see a 100 percent workload increase on two different servers following the increase of remote workers, but server capacity utilization remains in the range of 20 – 40 percent. Performance will not be affected at this point, but it’s important to continue to analyze these devices as more remote users are added.
You’ll also want to look at the correlation between active sessions and output bit rate by network interface to determine when a given circuit will saturate. This can vary significantly based on the specific devices and workloads involved. For example: An audio-only conference will use fewer bits than a video conference. Dependency on AWS cloud services will cause higher network usage. Laptop backups by remote workers will consume the capacity of both network servers and network bandwidth. As a result of factors like these, you might find that the 500 Mbps link at one site can handle 400 – 500 sessions, while another site with similar number of sessions will saturate a 1 Gbps link.
Step 3 – Model business continuity scenarios to understand the impact of a failure

If you have multiple network servers supporting your distributed organization, you’ll need to understand the workloads and corresponding capacity requirements at each location. This is especially important for ensuring consistent performance in the event that one of these servers fails. In this situation, you’ll need to be able to redistribute its workload across your remaining networks without exceeding their individual capacity thresholds.

The modeling you did in Step 1 will provide the information you need for your business continuity plan. Analysis and What-If event models will help you see how various scenarios might play out. In this example, we’ve stacked the utilization graphs for two regions—Amsterdam and Tel Aviv—and assigned the combined utilization to each region. We can see that while Tel Aviv would be able to step up and handle the load from a failure in Amsterdam, the reverse isn’t true—the Amsterdam link would be saturated by the addition of the load from Tel Aviv.

In this case, you’d need to adjust your plan accordingly, either by adding available capacity in Amsterdam to ensure business continuity, or by finding a different way to distribute the load from a failure in Amsterdam.
**Step 4 – Model end user response time for an application**

Remote workers need the same high-quality experience at home that they’d get in the office. To make sure networks are performing as expected, you can model the end user response time across your enterprise. You’ll also be able to determine whether a potential slowdown results from a network issue or a server issue.

First, collect end user response times for internal and customer-applications from your application performance monitor. You can then correlate this data with network response and server response times to see whether or when a performance problem arises. BMC Helix Capacity Optimization Analysis, Forecast Model, and Extrapolation Analysis will help with this step.

Next, correlate response times with the number of concurrent users on your VPN. By extrapolating this relationship, you can predict the number of concurrent users you can support without breaching your response time thresholds. In the example to the right, we learn that we can add up to 400 users and still maintain current response times. You should rerun this model at least once each week to make sure the correlation remains accurate over time, referring to a “golden model” of your company response time standard for comparison.

Because some applications are more sensitive to network issues than others, review response times by different applications across geographies and numbers of concurrent users. If a given application is performing uniformly across networks, the issue is likely with the application itself; variations by region can point to a problem with an individual network or server.
About BMC Helix Capacity Optimization

BMC Helix Capacity Optimization helps organizations align IT resources with business service demands, optimizing resource usage and reducing costs. The solution provides visibility into the entire IT infrastructure—physical, virtual, containers, and cloud—so IT can easily add, remove, or adjust compute, storage, network, and other IT infrastructure resources to meet changing application and service demands. Service views, forecasting, modeling, and simulated migration capabilities provide the insight for future resource needs and the ability to control the timing and cost of new capital and operating expenditures. Self-service dashboards and reports keep project owners, business owners and other stakeholders informed.

To learn more about BMC Helix Capacity Optimization, please visit https://www.bmc.com/it-solutions/capacity-optimization.html

About BMC
From core to cloud to edge, BMC delivers the software and services that enable over 10,000 global customers, including 84% of the Forbes Global 100, to thrive in their ongoing evolution to an Autonomous Digital Enterprise.

BMC—Run and Reinvent

www.bmc.com