

CALIFORNIA

Assessment of Student Performance and Progress

Technical Specifications and Configuration Guide for CAASPP Online Testing

◆ System Requirements ◆

Network Configuration ◆ System Configuration ◆

Secure Browser Configuration ◆

Summative and Interim Assessments

Test Administrator Sites

Student Practice Tests

Test Operations Management System

Online Reporting System

Interim Assessment Hand Scoring System



California Assessment of
Student Performance and Progress



This page is left blank intentionally.

Chapter 2. Network Configuration

Network Configuration and Testing

Your network's configuration has a significant impact on the test delivery system's (TDS's) performance. An improperly configured network can slow a TDS's responsiveness and possibly impact students' scores or an assessment's integrity. The following subsections provide guidance on properly configuring your network and lists popular tools for diagnosing network bottlenecks.

Finally, the network configuration must support a secure online testing environment, which is a state in which a device is restricted from accessing prohibited computer applications (local or Internet-based), or copying and/or sharing test data. The purpose of this environment is to maintain test security and provide a stable testing experience for students across multiple platforms.

Network Configuration

This subsection provides guidance or requirements pertaining to networking configurations for online testing.

Guidance for Determining Required Bandwidth

Bandwidth is the measure of a network's capacity or utilization, usually measured in terms of bits per second. Your network should have enough bandwidth to support online testing at the required performance level. For example, if a testing program requires that Web browsers display test items within 10 seconds after sending a request, then the network must have enough bandwidth to support that requirement.

In an online testing environment, the following factors contribute to determining the required bandwidth:

- **Number of Students Simultaneously Testing**—As the number of students testing at one time increases, the required bandwidth also increases.
- **Size of the Test Content**—The size of a test's content is determined by two factors:
 1. the number of items on the test; and
 2. the average size of each item.

The more items a test contains and the larger the average test item, the higher the bandwidth requirement for a given test. For example, some writing tests have a few questions to which the student composes a response, and these tests are small. In contrast, tests with animations or simulations are large.

- **Hubs or Switches**—Local area network performance can be hindered when hubs are used instead of switches. A hub broadcasts signals from various network devices to propagate across the network, potentially saturating the network and causing traffic competition or data collisions. If you use hubs, ensure they have enough bandwidth to handle the propagation.
- **Internet service provider (ISP) Router**—For Internet networks, the most common bottleneck is the ISP's router connection, which typically operates at speeds of between 1.5M bits per second and 100M bits per second. Network administrators should spend

time prior to test administration determining if their Internet infrastructure has the capacity to accommodate online testing at the required performance level.

- **Encryption**—Encryption at wireless access points (WAPs) may contribute to bandwidth usage. If you use encryption, ensure the WAPs have enough bandwidth to prevent degradation of performance.
- **Required Response Time**—When a network’s bandwidth cannot service the amount of data requested by clients, latency starts to accumulate and the students experience delays. Ensure your network’s bandwidth is high enough to support the required response times between the browsers and the servers.

Table 10 displays the estimated average bandwidth used by the secure browser for testing. When designing your network for online testing, ensure that the available bandwidth can support these values.

Table 10. Average Bandwidth Used by Secure Browser for Testing

Number of Students Testing Concurrently in School or Building	Average Estimated Bandwidth Consumed During Subsequent Startup of Secure Browser ^a	Average Estimated Bandwidth Consumed During Testing ^b
1	8K bits/second	5–15K bits/second
50	400K bits/second	250–750K bits/second (0.25–0.75M bits/second)
100	800K bits/second	500–1500K bits/second (0.5–1.5M bits/second)

^a Bandwidth consumed when opening the secure browser and accessing an assessment for the first time is significantly more than when opening the secure browser and accessing an assessment subsequently. This is because the initial launch of the secure browser downloads nonsecure cacheable content (not test content) that can be immediately accessed upon opening the secure browser later.

^b The values in this column are based on averages from tests in a variety of subjects.

Required Ports and Protocols

Table 11 lists the ports and protocols used by the TDS. Ensure that all content filters, firewalls, and proxy servers are open accordingly.

Table 11. Ports and Protocols for the TDS

Port/Protocol	Purpose
80/Transfer Control Protocol (TCP)	HTTP (initial connection only)
443/TCP	HTTPS (secure connection)

Configuration for Domain Name Resolution

[Appendix B, URLs for Testing Systems](#), lists the domain names for California Assessment of Student Performance and Progress testing and nontesting applications. Ensure the testing devices have access to a server that can resolve those names.

Configuring Session Timeouts

Session timeouts on proxy servers and other devices should be set to values greater than the average time it takes a student to participate in a test session or to complete a given test. For example, if your school determines that students will test in 60-minute sessions, then consider setting the session timeout to 65 or 70 minutes.

Data Caching

Data caching is a technique by which an intermediate server checks if it can serve the client's requests instead of a downstream server. While data caching is a good strategy in some situations, its overhead is detrimental in the online testing environment. Ensure all intermediate network elements, such as proxy servers, do not cache data.

Configuring Quality of Service and Traffic Shaping

If your testing network includes devices that perform traffic shaping, packet prioritization, or Quality of Service, ensure the URLs in [Appendix B, URLs for Testing Systems](#), have high priority.

Configuring for Certificate Revocations

Testing servers present certificates to the clients. The following subsections discuss the methods used to check those certificates for revocation.

Certificate Revocation List

To use a certificate revocation list, ensure your firewalls allow the URL <http://crl.verisign.com/>.

Online Certificate Status Protocol

To use the Online Certificate Status Protocol (OCSP), ensure your firewalls allow the domain names listed in Table 12. The values in the *Patterned* column are preferred because they are more robust.

Table 12. Domain Names for OCSP

Patterned	Fully Qualified
*.thawte.com	ocsp.thawte.com
*.geotrust.com	ocsp.geotrust.com
*.ws.symantec.com	ocsp.ws.symantec.com

If your firewall is configured to check only Internet protocol (IP) addresses, do the following:

1. Get the current list of OCSP IP addresses from Symantec. The list is available at https://forms.symantec.com/websurveys/servlet/ActionMultiplexer?Action_ID=ACT2000&WSD_surveyInfoID=2177.
2. Add the retrieved IP addresses to your firewall's whitelist. Do not replace any existing IP addresses.

Network Diagnostic Tools

You should conduct a performance analysis of your networking infrastructure to identify any bottlenecks that may impact test performance. The choice of diagnostic tool depends on the operating system running the tool, the network administrator's technical knowledge, and the desired level of network analysis. A number of network diagnostic tools are available, as described in the following subsections.

American Institutes for Research's (AIR's) Network/Bandwidth Diagnostic Tool

AIR provides a diagnostic tool that can be directly accessed from the student practice test logon page or in the "Additional Resources" box on most [caaspp.org](http://www.caaspp.org) Web pages.

1. On the practice test logon page (accessed by selecting the [**Student Interface Practice and Training Tests**] button on the Online Practice and Training Tests Web page at <http://www.caaspp.org/practice-and-training/>), select the [Run Diagnostics] link in the lower-left corner of the sign-in page (Figure 1) to open the Diagnostic Screen Web page.

Please Sign In

Guest User

State-SSID:
(ex: CA-999999123)

First Name:

Guest Session

Session ID: - -

For Students:

1. Uncheck the Guest User and Guest Session checkboxes.
2. Enter your first name into the First Name box.
3. Enter your two-digit state code and your SSID into the State-SSID box.
4. Enter the Session ID that your TA gave you.
5. Click [Sign In].

Guest Users:

To log in to the Practice and Training Tests, simply select [Sign In], then navigate through the login screens.

[Run Diagnostics](#)

Browser: IE v11

Figure 1. Sign In Web page for the training test

2. In the "Network Diagnostics" section, select a test.
3. Select the approximate number of students who may take that test *at one time*.
4. Select [**Run Network Diagnostics Tests**].

To determine your bandwidth, select a test from the drop-down list and enter the maximum number of students likely to test at one time, then click [Run Network Diagnostics Tests].

The [Text-to-Speech Check] is for schools who will be administering the test, and requires the use of the secure browser. The secure browser is available from www.caaspp.org.

Your Operating System: **Windows 7**

Your Browser Version: **IE v11**

Secure Browser: **false**

Network Diagnostics:

Select Test: **2**

Enter the total number of students you would like to test at one time: **3**

4

Figure 2. Run the diagnostics test

The tool displays your current upload and download speed as well as a general idea of whether you can reliably test the number of students you entered in step 3. You may want to run this test several times throughout the day to verify that your upload and download speeds remain relatively consistent.

Windows-Specific Tools

PRTG Traffic Grapher

PRTG (<https://www.paessler.com/prtg>) monitors bandwidth usage and other network parameters via Simple Network Management Protocol. It also contains a built-in packet sniffer. A freeware version is available.

NTttcp

NTttcp (<https://gallery.technet.microsoft.com/NTttcp-Version-528-Now-f8b12769>) is a multithreaded, asynchronous application that sends and receives data between two or more endpoints and reports the network performance for the duration of the transfer.

Pathping

Pathping is a network utility included in Windows. It combines the functionality of the `ping` and `tracert` commands by providing details of the path between two hosts and ping-like statistics for each node in the path based on samples taken over a time period.

OS X-Specific Tools

Network Utility.app

This tool is built into OS X.

Multiplatform Tools

Wireshark

Wireshark (<http://www.wireshark.org/>) is a network protocol analyzer. It has a large feature set and runs on most platforms including Windows, OS X, and Linux.

TCPDump

TCPDump (<https://sourceforge.net/projects/tcpdump/>) is a common packet sniffer that runs from the command line on Linux and OS X. It can intercept and display data packets being transmitted or received over a network. A Windows version, WinDump, is also available (<http://www.winpcap.org/windump/>).

Ping, NSLookup, Netstat, Traceroute

Ping, NSLookup, Netstat, and Traceroute comprise a set of standard UNIX network utilities. Versions of these utilities are included in Linux, Windows, and OS X.

Iperf

Iperf (<https://github.com/esnet/iperf>) measures maximum TCP bandwidth, allowing the tuning of various parameters and User Datagram Protocol characteristics. Iperf reports bandwidth, delay jitter, and datagram loss.

This page is left blank intentionally.
