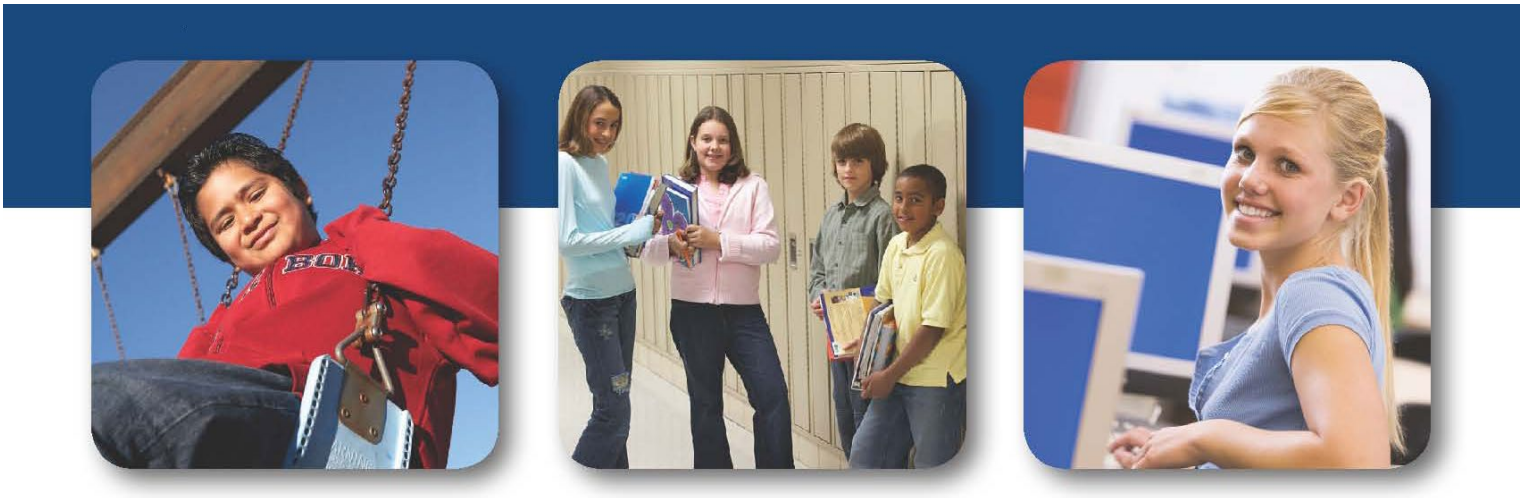
Network Evaluation and Troubleshooting



Version 2.1.1

July 2020

DATA RECOGNITION
DRC
CORPORATION

TECHNOLOGY – NETWORK CONFIGURATION

- ☐ Complete a wireless site survey to assess the wireless coverage in testing areas and review the following:
  - ☐ **Device Density**
    Review the number of devices connecting to a single access point. Devices connecting to the access point might not be in the same room where the testing occurs. If the site has an open network or available guest network, account for devices that students, proctors, and teachers have connected (e.g., smartphones, laptops, and tablets).
  - ☐ **Radio Frequency Interference**
    Review whether other devices might cause interference. Wireless networks share the same frequency as many technologies and any of these devices operating at the same frequency as an access point can cause interference. In addition, wireless access points sharing the same channel may interfere with each other.
  - ☐ **Connection Consistency**
    Consider things that may interrupt the connection between the testing device and the access point. Review whether there are objects obstructing the line of sight between testing devices and access points that could interrupt the connection. Also, multiple access points can lead to momentary interruptions as a testing device moves from one point to another.
  - ☐ **2.4 GHz vs. 5 GHz Bands**
    Assess whether the site's wireless network is using either the 2.4 GHz or 5 GHz bands appropriately. Wireless networks operate in either 2.4 GHz or 5 GHz band. The 5 GHz connection can transmit higher amounts of data with better speeds. The 2.4 GHz connection is better for transmitting data over longer ranges and through walls and other solid objects.
- ☐ Review the district and school network capacity (LAN, WAN, and ISP) to administer online testing. Verify that there is available capacity for the number of students taking the test at the same time. Take into account competing Internet bandwidth and other traffic in the building at the time of testing.

  Estimate the available bandwidth for transferring test content from the student testing devices to the location of the test content (test content could be on a local COS Service Device at the site, on a central COS Service Device at another site, or at DRC if there is no COS Service Device for content hosting)**:**

  - Up to 25 Concurrent Testers: 50 Mbps
  - 26–150 Concurrent Testers: 100 Mbps
  - 151–500 Concurrent Testers: 200 Mbps
  - 501–900 Concurrent Testers: 400 Mbps
  - 901–1000 Concurrent Testers: 800 Mbps
  - >1000 Concurrent Testers: >1 Gbps

  Use the **Testing Site Capacity Estimator** to help determine bandwidth requirements.
- ☐ Review the connection from the test content source to the testing device, verifying that it is strong and consistent.

  For most tests, after the test has started, the bandwidth requirements are reduced significantly. However, for tests with audio content, the network requirements from the test content source to the device remains high throughout the test. For these tests, content, including the audio file, is delivered as students receive each item and averages 2MB per item. This results in the need for a more reliable connection throughout the test.
- ☐ Verify connection speed from a device in the testing rooms, ideally when the devices in the room are using the Internet. Run a Speed Test using www.speedtest.net to a server in Minnesota. Results showing less than 3 Mbps download and 3 Mbps upload speeds indicate there may be insufficient available bandwidth.
- ☐ Ensure that all firewalls and filters on the computer network are configured with the necessary URLs allowed. The URLs are listed in the Network Requirements for Testing Computers section of the DRC INSIGHT Technology User Guide Volume I: Introduction to Online Testing.

- ☐ Some firewalls and content filters can be configured to perform deep packet inspection. This may negatively impact the performance of online testing. Review the configuration and consider disabling deep packet inspection during the testing window if the site is experiencing connectivity issues.
- ☐ Distributed gateway platforms can be configured to use Reverse DNS Lookup. This feature is used to verify the domain name associated with an IP address. DRC INSIGHT uses a content distribution network where the DNS will direct the request to your nearest IP address. Doing a Reverse DNS Lookup on that IP address may not resolve back to our URL, which may result in a site being blocked from testing. If the site is experiencing connectivity issues, consider configuring the gateway to not use Reverse DNS Lookup during the testing window.
- ☐ If available, use traffic shaping to give DRC INSIGHT testing traffic priority over other network traffic.
- ☐ Limit other use of the network during testing, especially high-bandwidth activities such as downloading and watching videos.
- ☐ Verify that the wireless access point is fully operational.
- ☐ Some access points interpret testing traffic between the COS Service Device and the DRC INSIGHT testing device as Peer-to-Peer Networking. Review Layer 7 filtering to ensure that testing traffic is not blocked.
- ☐ Access points may limit the bandwidth a testing device can consume, typically to around 5 Mb per device. Review the access points and if this setting is in place, temporarily remove the limit during the test window.
- ☐ Require anyone sharing the testing room's wireless access point, to turn off wireless devices that are not used for testing. **Note:** Devices using the access point may be outside of the testing room.

ADDITIONAL TECHNOLOGY – NETWORK CONFIGURATION FOR CHROMEBOOKS

- ☐ Chromebooks launch very quickly. Have students wait for the Chromebook to successful connect to an access point before launching the DRC INSIGHT testing device. If DRC INSIGHT is launched before the device connects to the network, the student will receive an Internet Connection Error (ICE).
- ☐ DRC INSIGHT is loaded as a Kiosk Application, so a Chromebook is not logging in as a user account. In some situations, the Chromebook may act like a “Guest” in the wireless network. Review the wireless policy to provide “internal access” to “Guest” Chromebooks to enable access to a COS Service Device.
- ☐ Review whether non-authenticated Chromebooks are viewed as guest devices by the wireless policy until the Chromebook logs in and authenticates. Verify that Chromebooks are assigned an IP address that allows for internal traffic and the connection to the COS Service Device.
- ☐ If an access point is over-saturated, a Chromebook may move from the access point to another access point, at which time the Chromebook may switch wireless networks. This may cause the Chromebook to be assigned a new IP address during the test, resulting in an error. Verify that Chromebooks are assigned a preferred network to reduce the risk of this occurring during testing.
- ☐ Verify that Chromebook traffic does not have any proxy settings and does have a direct connection to the Internet.
- ☐ If the DRC INSIGHT testing device is unable to connect, temporarily turn off Content Hosting in the COS application. If the DRC INSIGHT testing device is now able to connect and successfully deliver an online test, it indicates that traffic through the Internet is working and that local access to the COS Service Device is an issue.