ROGERS NETWORK MANAGEMENT POLICY

Wireline

Rogers relies on network investments as the primary tool to manage Internet traffic and address potential congestion. We monitor the utilization of the wireline Internet network to maintain the service experience and plan for additional capacity to ensure that our customers continue to receive the broadband speeds they have purchased.

Rogers has mechanisms in place to protect our wireline Internet network from malicious traffic and security threats, such as Denial of Service (DOS) attacks, malware, spam, and fraudulent activity (e.g., modem cloning). We take standard, necessary and reasonable steps to prevent service outages and to ensure that bandwidth usage is optimized efficiently amongst our customers who share the same service node.

In times of emergencies and extreme circumstances, Rogers may also apply the following technical Internet traffic management practice (ITMP) to our wireline Internet service:

1. What is the ITMP and when will it occur:

- Rogers' traffic management policy for our retail wireline Internet service comes into effect in the event of significant network congestion as the result of an emergency or extreme circumstance.
- During such instances, Rogers may deploy a traffic management measure to a customer's upload traffic (i.e. from the customer to the Internet) on wireline Internet service plans with a maximum upload speed of 10 Mbps or higher.
- Should a customer engage in a volume of upload activity over a sustained period of time such that this usage negatively impacts, or is likely to negatively impact, the Internet experience for other customers, that customer's maximum upload speed may be temporarily reduced.

2. Why the ITMP is applied:

- Rogers deploys this traffic management measure so that all Rogers Internet customers receive fair access to the Internet. During periods of significant network congestion resulting from emergency or extreme circumstances, this helps to ensure that all of our customers can enjoy a consistent and reliable online experience and preserves the integrity of our network.
- This objective is especially important in times of public emergency that result in greater demands on our network. During such periods, keeping our customers connected to their families, friends and co-workers – and to critical information and services – is essential.

3. What type of Internet traffic (e.g. application, class of application, protocol) is subject to the ITMP:

- No specific application or protocol is specifically targeted through this traffic management policy.
- Only data upload activity described under #1 above may be subject to traffic management. Download traffic is not managed.
- Rogers' traffic management policy is designed to reduce the impact of extreme, data-intensive activity by individuals during a congested period in order to leave resources open for more customers engaging in real-time interactive activities.

4. How the ITMP will affect a user's Internet experience, including the specific impact on speeds:

- If a customer's maximum upload speed is temporarily reduced as a result of this ITMP, it may take longer to upload larger volumes of data.
- Under the ITMP, maximum upload speeds will be maintained at levels that will continue to support real-time interactive activities, such as online banking, web-browsing, social networking, audio/video conferencing, online gaming and VoIP services.
- For the vast majority of our customers, their Internet experience is unaffected by our traffic management policy.

Wireless

Rogers relies on network and spectrum investments as the primary tool to manage mobile Internet traffic and address potential congestion. We have mechanisms in place to protect the Rogers wireless network and our customers from malicious traffic and other security threats, as well as standard network management processes to enable the normal operation of our mobile network.

Rogers First Priority Service provides priority access to first responders, public safety officials, and critical infrastructure personnel. In the rare event that demand for network resources exceeds expected peak capacity, such as during natural disasters or threats to public safety, data connections from these users are prioritized by the mobile network.

As a result, during these rare events, non-Rogers First Priority Service users connecting to sites in the same area may experience slightly slower speeds and delayed response times when using data services, such as browsing and uploading or watching videos (all applications treated equally). In extremely rare cases, data connections could need to be re-initiated. 9-1-1 service is never impacted.

Specific plans may have Internet traffic management practices applied as outlined in their data management policies (as listed below). However, all traffic is treated equally, including all applications and classes of service.

Rogers Infinite Plans Data Policy