Network Management Policy

Congestion Management Policy

The provider monitors and proactively reinforces the network with additional capacity in areas where growth trends identify a need. If network congestion occurs, the provider employs various techniques to ensure a positive customer experience and fair distribution of network resources.

Currently, based on experience, if customers encounter any congestion, it is typically during the hours of peak usage — between 7 p.m. and 11 p.m. local time. During peak hours, the majority of our residential customers are using the Internet simultaneously, giving rise to a greater potential for congestion. Peak usage will vary due to extraordinary conditions such as pandemics, weather events and/or national emergencies.

When network congestion is identified, the provider uses various techniques to create a good customer experience. The network management techniques include preventing virus/spam delivery to email accounts. They also reinforce the network with additional capacity in areas where congestion is identified or as part of standard network engineering design plans. In some cases, they may limit the number of customers that can be served on a particular network node or in very rare cases they may need to downgrade the service available to existing customers until additional capacity can be added.

The links the provider and other networks use to exchange traffic may also become congested at times. The provider devotes considerable resources to maintaining adequate traffic exchange arrangements with these other networks and has entered into commercially negotiated agreements to exchange traffic with them on mutually agreeable terms wherever possible. Consistent with its agreements with those other networks and its long-standing practices, the provider will work to establish or expand the connections between its network and other networks on mutually agreeable terms when needed. But, sometimes this is not possible due to circumstances beyond the provider's control. For example, in some instances, other networks refuse to make adequate arrangements. In other instances where adequate arrangements are in place, some edge providers or their intermediaries (other networks) choose to route traffic in ways that result in congestion when there are other choices. If the provider is unable to reach agreement on the terms of its interconnection or network expansion with these other networks, or if some of these other circumstances occur, it could affect a customer's ability to upload or download data via Internet endpoints connected to those networks. The provider cannot guarantee that it will be able to establish or expand the connections between its network and other networks, or that subscribers will be able to upload data to or download data from Internet end points connected to other networks at any particular speed.

Excessive Use Policy

The Excessive Use Policy (EUP) uses a 1.0 terabyte (TB) monthly data usage limit. This limit applies to all uploaded and downloaded data for all residential High Speed Internet (HSI) customers except for those excluded below. Of all of our HSI customers, a very small fraction exceed the data usage limit provided with their monthly HSI plan.

NT&T is committed to providing an optimal Internet experience for every customer we serve. It is for this reason that NT&T places data usage limits on residential plans. The data usage limit applies to residential HSI. It does not apply to business HSI.

NT&T does not currently charge customers a fee for excessive data usage. The provider will weigh variables such as network health, congestion, and the availability of customer usage data as factors when enforcing this policy. Customers who have exceeded their monthly data usage limit and are subject to EUP enforcement will be notified.

Customers who are subject to EUP enforcement are given options to reduce their usage, subscribe to a higher-speed residential HSI plan, or migrate to an alternate HSI service that is exempt from usage limits. Our EUP is application neutral; it only considers the total usage (bytes transferred) over a defined period of time independent of protocols, applications, or the content that is generating the excessive usage.

Application-Specific and/or User-Specific Policy

NT&T High-Speed Internet customers receive full access to all the lawful content, services, and applications that the Internet has to offer.

As described more fully below, the provider deploys Type of Service (ToS) and Differentiated Service (DiffServe) capabilities at the customer modem and in limited network equipment deployed across the provider's High-Speed Internet network. The network equipment enabled with this capability will honor ToS and DiffServe settings of any third-party network consistent with the National Standards recommendations described in the Internet Engineering Task Force (IETF) RFC 1349 and RFC 2474.

The provider does not otherwise block, prioritize, or degrade any Internet sourced or destined traffic based on application, source, destination, protocol, or port unless it does so in connection with a security practice described in the security policy section below.

The provider also deploys certain user-specific policies (i.e. practices that are applied to traffic associated with a particular user or user group). Currently, these are limited to practices described above and the security practices described in the security policy section below.

Device Attachment Policy

NT&T will provide the customer with an approved modem to use.
NT&T customers may attach devices of their choice to the modem. Any attached devices must be used in a manner consistent with our Acceptable Use Policy.

Security Policy

The provider engineers are dedicated to managing the network to ensure that all customers receive the most secure online experience. They use industry-leading security practices to manage the network, provide services to our customers, and ensure compliance with our Acceptable Use Policy. These tools and practices may change from time to time to keep up with the new and innovative ways that customers use the network and to keep up with changing network technologies.

When malicious behavior is identified, the provider engineers employ various techniques to help provide a positive customer experience. The security management techniques include ensuring that customer systems are not propagating viruses, distributing spam email, or engaging in other malicious behavior. For example, they use industry best practices to prevent virus/spam delivery to customer email accounts. They also automatically detect and mitigate DoS (Denial of Service) attacks for our High-Speed Internet customers. They block malicious sites and phishing sites to

prevent fraud against our customers and to prevent our customers from getting infected via DNS (Domain Name Service) blackholing and Internet Protocol (IP) address blackholing.

They reserve the right at any time to take action to protect the integrity and normal operation of their networks and to safeguard customers from Internet threats, including fraud and other forms of abuse. Such actions may include, but are not limited to, blocking, redirecting, or rate-limiting traffic using specific protocols, delivered over specific protocol ports, or destined for particular domain names or IP addresses associated with known malicious activity.

Specific security practices deployed by the provider may include but are not limited to:

IP Spoofing Prevention

The basic protocol for sending data over the Internet network and many other computer networks is Internet Protocol (IP). The header of each IP packet contains, among other things, the numerical source and destination address of the packet. The source address is normally the address that the packet was sent from. By forging the header so it contains a different address, an attacker can make it appear that the packet was sent by a different machine. The machine that receives spoofed packets will send a response back to the forged source address, which means that this technique is mainly used when the attacker does not care about the response or the attacker has some way of guessing the response.

The provider applies security measures to prevent an attacker within the network from launching IP spoofing attacks against these machines and flooding the network with unwanted data that can cause congestion.

DoS/Distributed DoS Monitoring and Mitigation

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person, or multiple people, to prevent an internet site or service from functioning efficiently or at all, temporarily or indefinitely.

The provider applies various security measures to prevent someone within the network from launching DoS or DDoS attacks to ensure that customers can access the Internet when needed.

The provider may block or rate-limit connections on other ports that are commonly used to exploit other customers or non-customer computers.

The provider may block sites that are used in a malicious manner to infect customers, perform fraud against them and otherwise as needed to protect our network and our customers.

Port 25 Blocking

The provider filters port 25 to reduce the spread of email viruses and spam (unsolicited email). Email viruses allow malicious software to control infected computers. These viruses direct the infected machines to send email viruses and spam through port 25. Port 25 filtering is a recognized Internet industry best practice for service providers to filter e-mail traffic. The Messaging Anti-Abuse Working Group (MAAWG), a global organization focused on preserving electronic messaging from online exploits and abuse with the goal of enhancing user trust and confidence, recommends that "providers block incoming traffic to your network from port 25."

UDP Port 1900 Blocking

The provider may filter User Datagram Protocol (UDP) port 1900 to prevent DoS attacks across the network. SSDP (Simple Service Discovery Protocol) runs on UDP port 1900 and is part of the Universal Plug and Play (uPnP) protocol that allows discovery and configuration of devices on a local network. Normal use of the protocol is limited to a local network, but the protocol is used by attackers in reflective DoS across the backbone.

Performance Characteristics

Expected Performance

When you order NT&T High-Speed Internet access service, the service we quote you is based on an advertised "up to" connection speed. The provider continually upgrades its network, but our quoted speed is based on the characteristics of the relevant network facilities at the time you order.

The actual throughput you experience may vary. During most periods, based on evaluation, most customers that subscribed to the up to 940Mbps service as explained below, can generally expect average speeds at or above 95% of the advertised "up to" speed and many can generally expect speeds above that level. Less than 20 percent of customers can expect average speeds below 80% of the advertised "up to" speed. In rare cases, average speed may be significantly less than this level.

The service speed is established between a provider network device (such as a DSLAM) and the in-premises modem. The service speed established between these devices may be less than the speed you ordered due to physical condition of the line and other factors. It may also vary from time to time.

The actual throughput achieved will vary due to a wide variety of factors such as the congestion issues on our network described above, as well as other factors outside of the provider control such as customer location, the quality of the inside wiring within the home, the websites and other Internet resources accessed, usage and performance of the networks any data must traverse, and the customer's equipment within the home or premises.

Latency (the time it takes for a data packet to travel from one point to another in a network) is also highly variable depending on the network path, other providers in the path, as well as the actual distance to the destination and performance of the end destination servers. It generally increases with distance of the route between the source and destination and with any congestion on the route and decreases as actual speed increases. The provider measures latency by measuring the round-trip time from the consumer's home to the closest measurement server and back. NT&T High-Speed Internet customers generally should expect roundtrip latency to most Internet sites in the range from 3-65 milliseconds.

Packet loss (the percentage of packets that are sent by the source but not received by the destination) is also highly variable. The most common reason that a packet is not received is that it encountered congestion along the route. A small amount of packet loss is expected, and indeed some Internet protocols use the packet loss to understand Internet congestion and to adjust the sending rate accordingly. The provider denotes a packet as lost if the latency exceeds 3 seconds or if the packet is never received. The Federal Communications Commission’s 11th Measuring Broadband America (MBA) – Fixed Broadband Report provides the average peak-period packet loss for each participating ISP, for that ISP’s speed tiers covered by MBA testing. That document - available at:

https://www.fcc.gov/general/measuring-broadband-america - reports that NT&T High-Speed Internet customers should generally expect to experience packet loss at a rate significantly below 1% for the NT&T speed tiers covered by the report, at levels unlikely to significantly affect customer experience.

Gateway / in-home networking configuration:

Use of the NT&T provided gateway. We recommend not attaching any additional gateway/router devices not sold/approved by NT&T behind the gateway.

Connected device minimum requirements

Device Type	Processor	Memory	Network Interface Card	Operating System	Browser
Personal Computer/Windows	Intel® Core™ i5-3320M CPU @ 2.60GHz (4 CPUs)	16+ GB of RAM	1Gbps enabled Ethernet port	Windows 10 (64 bit) and above	• Internet Explorer 11 • Microsoft Edge • Firefox 55 and above • Google Chrome 70.0.3538.77 and above
MAC	Quad-Core Intel Core i7 (or faster) processor	16+ GB of RAM	1Gbps enabled Ethernet port	OS X 10.13.6 and above	Safari 11.1.2 and above

Wired configuration:

- Connect via the Ethernet port on the gateway

- Use 1Gbps network interface card on computer / connected hardware (Intel or Broadcom based interface cards preferred)

- Use Cat5e or Cat6 cabling between the gateway and customer equipment. Ensure eight wires are connected from the cable to the RJ45 connector on each end of the cable. The wires can be visible through the transparent connector on each end of the cable.

Wireless configuration:

- Wireless speeds will vary due to many factors such as WiFi radio enabled on the gateway, WiFi radio on the receiving device, environmental conditions, type of hardware device connecting to the service, the operating system of the device and distance between the WiFi radio and the device receiving the bandwidth.

To optimize wireless throughput, we recommend the following:

- Place WiFi-enabled gateway in a centralized location to maximize coverage, away from any devices that generate signal frequencies (microwaves, etc.)

- Ensure the gateway has an unobstructed path to where most of the wireless devices will be operating

- Minimize the number of wireless devices connecting to the gateway, turn off devices if not in use

- Use 802.11ac or WiFi6 radios with the 5GHz channel enabled

Wireless factors impacting high-speed internet throughput

Wireless throughput in the home will vary due to many factors, including WiFi radio used, environmental conditions, the number of devices connected via the wireless signal, and distance between the WiFi radio and the receiving device (e.g., laptop, computer, tablet, mobile phone, etc.). The device receiving the throughput can also impact the throughput by the configuration of hardware (e.g., operating system, processor, memory, etc.). Additional details regarding some of the more prevalent factors impacting wireless throughput are listed below:

- Environmental limitations: walls (brick, normal drywall construction, etc.), metal cabinets, windows and HVAC duct work are a few of the many construction materials that degrade WiFi signals. Each building has unique properties that may degrade the wireless throughput.

- Distance from the gateway: the atmosphere (air) between the gateway and the receiving wireless device degrades the wireless signal. In general, the greater the distance from the gateway to the receiving device, the slower the speed.

- Type of WiFi radio: There are several types of WiFi radios readily available in the marketplace. The most prevalent in the marketplace are versions 802.11b, g, n, ac and ax. The higher the letter/letter combination at the end of the 802.11 version, the higher the speed. Both the sending and receiving devices must be enabled with the same radios to achieve maximum throughput expected for any specific radio type. When two different radio types are being used between sending and receiving devices, the lower speed version will determine maximum throughput. To maximize wireless throughput, the provider recommends using 802.11ax-enabled devices to achieve the greatest expected throughput range for the high-speed internet service. See the table below regarding maximum theoretical and generally expected throughput by WiFi radio version. "Generally Expected Throughput" is a guideline, but wireless service performance will vary based on each customer's unique environment.

WiFi Radio Version	Theoretical Maximum Throughput*	Generally Expected Throughput
802.11b	11 Mbps	<11 Mbps
802.11g	54 Mbps	12 – 20 Mbps
802.11n	600 Mbps	40 - 60 Mbps
802.11ac	1.7 Gbps	400 – 600 Mbps

***** Maximum theoretical throughput is defined through the IEEE 802.11 standard. The industry standard is created and maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802)

- Number of devices connected wirelessly: In general, the more wireless devices connected to the service, the slower the wireless connection will be. Wireless radios generally see a reduced throughput as more devices are connected to a gateway but is dependent upon each manufacturer's design. This is due to processor and antenna resource allocation within the WiFi radio. As more devices get connected, the radio's resource allocation to any one device generally is decreased.

- The use of WiFi extenders / mesh devices to improve coverage: the use of WiFi extenders or mesh devices are used to increase the WiFi signal coverage. However, each extender / mesh device may impact overall wireless throughput depending on the specific solution used. To optimize the WiFi network throughput using WiFi extenders or mesh devices, confirm WiFi radio type is consistent with the Gateway. Then consult the respective WiFi extender or mesh user manual(s) to validate throughput capabilities, ensure proper configuration and adherence to equipment placement recommendations.

- Number of other WiFi networks in close proximity: multiple WiFi networks working in close proximity can cause signal interference and throughput issues.

Actual network performance metrics

The tables below set forth peak period (7-11 pm local time, or in some cases 24 hour measures) medians for download, upload, and latency performance for the provider's High Speed Internet access services — by the download and upload speed portion of your tier, respectively. It is updated on a periodic basis.

The speed data represent medians of network speeds and are derived from either actual network measurements test data throughput rates during peak period, network train rate calculations modified by statistical modeling to replicate the likely congestion experience or internal lab speed tests that the provider has conducted regarding its services. The latency data is derived from actual network measured latency rates during peak period.

Speed Tier **(Advertised "Up-to" Download Speed)**	**Download Speed (Mbps)** **Peak-Period Median Unless Noted**	**Latency (ms)** **Peak-Period Median**
256 kbps	0.25 Mbps	60.6 ms
500 kbps	0.83 Mbps	49.3 ms
512 Kbps	0.51 Mbps	60.2 ms
640 Kbps	0.87 Mbps	50.3 ms
768 Kbps	0.78 Mbps	50.2 ms
1.5 Mbps	1.6 Mbps	47.4 ms
3 Mbps	3.5 Mbps	42.0 ms
4 Mbps	4.0 Mbps	47.3 ms
5 Mbps	6.2 Mbps	35.0 ms

6 Mbps	6.3 Mbps	40.8 ms
7 Mbps	7.5 Mbps	27.2 ms
8 Mbps	8.3 Mbps	31.9 ms
10 Mbps	10.5 Mbps	30.1 ms
12 Mbps	13.4 Mbps	22.2 ms
15 Mbps	15.9 Mbps	26.0 ms
20 Mbps	21.0 Mbps	21.3 ms
25 Mbps	25.8 Mbps	21.1 ms
30 Mbps	31.5 Mbps	21.1 ms
40 Mbps	40.3 Mbps	19.3 ms
60 Mbps	60.0 Mbps	18.0 ms
80 Mbps	80.0 Mbps	15.3 ms
100 Mbps	100.0 Mbps	7.1 ms
120 Mbps	117.0 Mbps	7.3 ms
140 Mbps	139.9 Mbps	3.0 ms
200 Mbps	216.1 Mbps	2.9 ms
500 Mbps	527.6 Mbps	5.2 Mbps
750 Mbps	790.1 Mbps	3.6 ms
940 Mbps	944.5 Mbps	3.0 ms

Speed Tier (Advertised "Up-to" Upload Speed)	**Upload Speed (Mbps) Peak-Period Median Unless Noted**
128 kbps	0.26 Mbps
250 kbps	0.48 Mbps
256 kbps	0.31 Mbps
384 kbps	0.43 Mbps
500 kbps	0.70 Mbps

512 kbps	0.54 Mbps
640 kbps	0.78 Mbps
768 kbps	0.81 Mbps
896 kbps	0.86 Mbps
1 Mbps	1.1 Mbps
1.5 Mbps	1.8 Mbps
2 Mbps	2.5 Mbps
3 Mbps	3.4 Mbps
5 Mbps	5.5 Mbps
10 Mbps	10.8 Mbps
20 Mbps	21.3 Mbps
50 Mbps	53.4 Mbps
100 Mbps	109.0 Mbps
200 Mbps	215.3 Mbps
500 Mbps	531.7 Mbps
750 Mbps	797.5 Mbps
940 Mbps	935.6 Mbps

Once service is installed, customers can also determine the throughput of their High-Speed Internet service via the Speed Test.

These websites will provide the throughput, latency results for service provisioned over the provider network. Third-party speed test results may be different than the data provided on the provider-provided speed test since third-party sites may include data for non-provider network facilities.

All NT&T High-Speed Internet services are provided either by fiber, DOCSIS, or digital subscriber line technology. The particular technology for your service will be based upon what is available in your geographic area.

The performance the user experiences, once they connect, may vary based on any number of factors, such as the maximum bandwidth allocated for WiFi services, the number of other users trying to use the same WiFi at the same time, the user's computer or wireless device, the WiFi receiving antenna, and the distance from the WiFi router. These WiFi routers use spectrum that the FCC has allocated for "unlicensed" use, which means that, like wireless routers used for in-home networking, the use of this spectrum is not protected from interference from other devices using the same spectrum in the same geographical area. This makes it inherently difficult to predict what kind of performance you can expect.

Non-Broadband Internet Access (or Specialized Services) Policy
NT&T does not offer non-broadband internet access services (or specialized services).

Commercial terms
NT&T offers mass market retail High-Speed Internet service to residential and business customers. Customers may purchase their NT&T High-Speed Internet service with voice services offered by NT&T. Customers may also purchase NT&T High-Speed Internet service as a stand-alone product. Availability, features, rates, terms, and conditions may vary by location.

NT&T High-Speed Internet service offers a variety of speed and features to consumers with available speeds from 500 Kbps/500 Kbps up to 940 Mbps/940 Mbps.

Customers can learn about the specific pricing and service availability where they live by visiting http://www.nttservices.com. Customers have access to NT&T standard pricing for High-Speed Internet service. Customers can also see options and pricing for modem purchase and lease options and technician installation.

Customers may also speak with a NT&T representative to learn about services in their area by calling NT&T at 1-877-537-4403.

NT&T's current High-Speed Internet service offering does not include usage-based fees.

Other charges and terms

Modem lease or purchase
NT&T offers modems to customers on a monthly lease basis or a one-time purchase basis.

One-time fees
Professional installation fees apply in connection with the purchase of your internet service. If a customer signs a 2 year service agreement with NT&T, the installation fee will be waived. If the customer cancels their service before the end date of their contract, a one-time contract termination fee of $150 will be charged to the customer.

Other monthly fee
Internet Dereg fee: This fee may be charged and is subject to change, but currently is $3.00 per month.

Government taxes, government-related fees, and NT&T fees and surcharges may apply
These charges vary by location and may change. In addition, NT&T reserves the right to pass through or institute new charges related to service.

Privacy policy
NT&T's privacy policies regarding our collection, use, and disclosure of your personal information are explained in our Privacy Policy.

Redress options policy
If you have any questions about these disclosures, cannot find what you are looking for or have any other concerns about NT&T's Internet services, please email NT&T at info@nttservices.com or call us toll-free at 1.877.537.4403.