(/)

Broadband Information

En Español (https://www.att.com/es-us/sdabout/sites/broadband/network)

Network Practices

How does AT&T manage congestion with respect to its mass market broadband internet access services?

AT&T strives to provide a high-quality internet experience for all of our customers. Because the internet consists of multiple interconnected networks and most internet end points (e.g., websites and other content providers) are not directly connected to the AT&T network, AT&T must connect to and exchange traffic with other networks to provide its subscribers the capability of uploading data to or downloading data from internet end points that are connected to those networks. To that end, AT&T has entered into commercially negotiated agreements to exchange traffic with those networks (and the networks with which those networks are connected) on mutually agreeable terms. The links AT&T and other networks use to exchange such traffic may become congested at times. Consistent with its agreements with those other networks and its long-standing practice, AT&T may establish or expand the connections between its network and other networks, but only on mutually agreeable terms. If AT&T is unable to reach agreement on terms of interconnection or network expansion with these other networks, it could affect customers' ability to upload or download data to internet endpoints connected to those networks. AT&T does not guarantee that it will 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.

In addition, like the other networks that make up the internet, the AT&T network is a shared network, which means that the transmission links and other network resources used to provide broadband services are shared among AT&T's subscribers, as well as among the various services offered by AT&T. Temporary congestion may occur when a large number of customers

in a concentrated area access the network at the same time or when some customers consume a very large amount of network capacity during busy periods, such as at stadium events, during peak usage times, or during planned network maintenance.

AT&T invests billions of dollars annually to address potential congestion in its broadband networks. As is common in the industry, we use network management practices and other tools to manage network resources for the benefit of all of our broadband customers, especially during periods when network demand exceeds available network resources (also known as “congestion”). As you would expect, our network management practices and our service offerings have evolved over time to benefit our customers and take advantage of the billions we have spent to expand and augment our networks.

Congestion-based Data Management. One network management practice we use to manage our wireless network resources may affect customers with most AT&T post-paid and AT&T PREPAID[SM] unlimited mobile data plans (“AT&T Unlimited Data Plans”). During periods of congestion, these customers may experience reduced data speeds and increased latency as compared to other customers using the same cell site (“Congestion-based Data Management”). Depending on the customer’s AT&T Unlimited Data Plan, they will either always experience Congestion-based Data Management or experience it only after they have used a set amount of data in a billing period as outlined in their AT&T Unlimited Data Plan (for example, 22GB or 50GB of data in a billing period). As always, even when subject to this congestion management practice, these customers have the comfort of knowing that, no matter how much data they use in a billing cycle, they will never be subject to overage charges and will pay a single monthly flat rate. That is our essential promise with the AT&T Unlimited Data Plans. Reduced speeds and increased latency may cause web sites to load more slowly or affect the performance of data-heavy activities such as video streaming or interactive gaming. Customers subject to Congestion-based Data Management will experience reduced speeds and increased latency only when they use data at a cell site experiencing network congestion at the same moment. As soon as the congestion at the cell site abates, or if the customer’s session migrates to an uncongested cell site, speeds and latency are not affected. In addition, this network management practice adjusts dynamically to address the amount of congestion, which can start and stop over a very short time period (often measured in fractions of a second), further minimizing any customer impact. Because the amount of congestion at a cell site can vary significantly, the performance impact for affected AT&T Unlimited Data Plan customers may also vary significantly, but such impact will last only as long as the site is congested.

For customers on plans subject to a data usage threshold for triggering the foregoing congestion management practice, we will notify them during each billing cycle when their usage reaches 75% of their threshold (so, for example, 16.5GB for plans with a 22GB threshold and 37.5GB for plans with a 50GB threshold) so they can adjust their usage to avoid network management practices that may result in slower data speeds.

Buffer Tuning. With the ever-increasing growth in smart phone and tablet usage on our wireless networks, and the growing prevalence of video downloads, AT&T has deployed a reasonable network management video optimization technique in our mobile data network. That technique delivers recorded video to the user's device in a "just in time" fashion (“Buffer Tuning”). Buffer Tuning only applies to internet browser traffic (HTTP, port 80) for recorded video downloads, regardless of the source (including AT&T branded or 3rd party content) and does not affect real-time streaming video. Without Buffer Tuning, video content may be completely delivered to the device and charged against the user's data plan regardless of whether it is viewed. With Buffer Tuning, a sufficient amount of video is delivered to the device so that the user can start viewing the video, and the remainder of the video is delivered just in time to the device as needed for uninterrupted viewing. This optimizes the user's data plan consumption. Additionally, this frees up network resources for all users. Buffer Tuning does not alter video content and should not directly introduce any adverse impact to the viewing experience.

Stream Saver. Another reasonable network management practice we use to more efficiently manage our wireless network resources is Stream Saver, which is a feature we offer on some of our wireless plans that include data. Stream Saver allows customers to watch more video over our wireless network while using less data by streaming content recognized as video content at Standard Definition quality, similar to DVD (about 480p). Stream Saver applies only to recognized video content delivered over AT&T’s wireless network. Once activated by AT&T on a customer’s account for plans that include Stream Saver, the customer can turn it off and back on at any time via the customer’s online account or by calling AT&T. Content providers can opt out of Stream Saver, in which case Stream Saver does not impact delivery of their video content. More information is available **here (https://www.att.com/offers/streamsaver.html)**.

Does AT&T limit data usage? Does AT&T provide any tools to help customers monitor and control their data usage?

We have developed speed tiers for our wired and data plans for our mobile broadband internet access services so that our customers can choose from a variety of speed tiers or rate plans that best reflect their own usage levels, and the manner in which they intend to use their service. For example, some AT&T data plans designated for use only with a basic phone or smart phone may not be used with a LaptopConnect card, tablet, or stand-alone mobile hotspot device. However, customers wishing to use their service in such a manner, such as with a mobile hotspot device, may purchase other plans that permit such use. AT&T provides usage calculators, alerts, and other tools for our wired and mobile broadband internet access services to assist customers in estimating their anticipated usage levels. For more information, please click here (**wired (https://www.att.com/support/internet/usage.html)**) and here (**mobile (https://www.att.com/support/wireless/data-usage.html)**). In addition, we send notices to customers of applicable usage thresholds for our tiered wired and mobile services. Many of AT&T’s Internet, Broadband, or Fiber plans for businesses have no data caps or data usage plans.

We have some post-paid mobile plans (for example, our Mobile Share Plus plans) that provide customers allotments of high speed data they may share among different devices on the plan, and some of our AT&T PREPAID[SM] plans (not including AT&T Wireless Internet, formerly known as Wireless Home Phone & Internet, or Mobile Hotspot) provide an allotment of high speed data to the specific line. Once customers on these plans exceed their allotments of high speed data -- which includes the plan data, any available Rollover Data, or other data allotments customers may have -- during a billing period, they may continue to consume data at no extra charge, but at significantly lower speeds when connected to the cellular network. Specifically, after one of these customers uses all available data allotments in a billing cycle, the customer's service over the cellular network will transmit data at a maximum of 128Kbps for the remainder of the billing cycle, unless the customer upgrades to a rate plan with a higher allotment of high speed data access before the end of the billing cycle. Once speeds are limited like this, the customer's connection over the cellular network should still allow viewing static web pages or checking email, but bandwidth-intensive activities such as audio and video streaming, picture and video messaging, and apps/services that use large amounts of data will be impacted and may not be fully functional. But, when the next billing cycle begins, the customer will once again have high speed data access. We will notify customers during each billing cycle when their data usage reaches either 75% or 90% of their monthly high-speed allotment (or at both intervals), and when they reach 100% of their monthly high speed data allotment so that they are aware of their amount of data usage and can make adjustments to avoid slower speeds. When connected to a Wi-Fi network, the customer's speed will not be impacted. For information regarding these types of post-paid Mobility plans and Rollover Data, click **here (https://www.att.com/shop/wireless/rollover-data.html)**, and for AT&T PREPAID[SM] plans, click **here (https://www.att.com/shop/wireless/gophone-plans.html#tab2)**.

We also have a sponsored data program that enables third parties to pay for the data usage for specific content on behalf of eligible AT&T wireless customers. With AT&T Sponsored Data, eligible customers can sample, browse, stream and enjoy applications, content and services provided by data sponsors without using up their monthly data allotments. Sponsored data thus effectively extends a customer's data usage allotment, and enables providers of online content, applications and services to encourage users to sample their services. For information about AT&T's sponsored data program, AT&T wireless customers should click **here (https://att.com/sponsoreddata)** and providers of online content, applications, and services should click **here (http://developer.att.com/sponsored-data)**.

Another way we help wireless customers manage their data usage is through Stream Saver feature summarized **above.**

For those geographic areas that are not served by AT&T's owned and operated mobile networks, we try to provide customers with data services through agreements with other carriers. The use of customers' devices to access data over another carrier's networks – both domestic and international – is called "off-net" or "roaming" usage. Our ability to make off-net or

roaming services available to customers is based on a variety of dynamic factors, including business considerations, the terms of the agreements we have at any given time with other wireless carriers, and the network technology, frequency(ies) and functionality of those networks. We do not guarantee the availability, quality of coverage or speed for data services that are accessed using other carrier networks and we may reduce speeds to 2G speeds or suspend the data service available on these networks at any time without notice. We update our coverage maps regularly to show where we provide domestic off-net and international roaming services. To obtain the most recent coverage updates you may access the maps **here (http://www.att.com/coverageviewer)**.

How does AT&T handle alleged copyright infringement by subscribers to its broadband internet access services?

The AT&T Copyright Alert Program was established to respond to alleged copyright infringement activities using peer-to-peer file sharing and attempts to educate customers about the importance of protecting copyright and lawful use of content available over the internet. Under the program, content owners may notify AT&T of alleged copyright infringement based on the IP address of a user. AT&T then will attempt to identify a subscriber account based on that IP address and forward a copyright alert to the subscriber account, advising the account holder of the allegation and providing information about online copyright infringement. If a subscriber receives additional alerts, we may temporarily redirect the account holder's broadband internet access service to a webpage where the account holder must review material on the importance of copyright and the lawful use of content available over the internet. Upon completion of this review, such redirection will be discontinued and the subscriber's service will be restored to normal. After this stage, if a subscriber continues to receive additional alerts, then AT&T may take action consistent with Section 512(i) of the Digital Millennium Copyright Act, which may result in termination of the subscriber/accountholder's broadband internet access service. Account holders' personally identifiable information is protected throughout this process — AT&T will not provide such information to content owners unless required to do so by court order. For more information about AT&T's Copyright Alert Program, please go to: **https://copyright.att.net/home (https://copyright.att.net/home)**.

Does AT&T favor certain websites or internet applications by blocking, throttling, or modifying particular protocols on its broadband internet access service?

No, AT&T does not favor certain websites or internet applications by blocking or throttling lawful internet traffic on the basis of content, application, service, user, or use of nonharmful devices on its broadband internet access services. Nor do we modify particular protocols, protocol ports, or protocol fields in ways not prescribed by the protocol standards. However, in response to a specific security threat against our network or our customers, AT&T may occasionally need to

limit the flow of traffic from certain locations or take other appropriate actions. In addition, we prevent the use of certain ports on our wired and Wi-Fi broadband internet access services to help protect our customers and network against malicious activity, as discussed below.

Our mobile broadband internet access service data plans may include different speeds, video streaming quality, and other options consumers can choose among so as to find the best fit for the manner in which they intend to use their service. For example, the AT&T Unlimited &More Premium plan allows users to stream video in High-Definition (up to 1080p), where available (streaming video services may transmit only lower quality video content) and when Stream Saver is turned off, while the AT&T Unlimited &More plan allows for streaming Standard Definition (480p/DVD quality) video. Customers watching streaming video on a Smartphone or other small hand-held device likely will not notice a significant difference between High-Definition and Standard Definition video quality, while those watching streaming video on a tablet or other larger device may prefer High-Definition video quality. For more information about our mobile broadband internet access service data plans, please go to: **https://www.att.com/plans/wireless.html (https://www.att.com/plans/wireless.html)**

Does AT&T directly or indirectly favor some traffic over other traffic (such as through prioritization, resource reservation, or traffic shaping) in its provision of broadband Internet access service either (1) in exchange for consideration (monetary or otherwise) from a third party, or (2) to benefit an affiliate?

No, in its provision of broadband internet access services, AT&T does not directly or indirectly favor some traffic over other traffic in exchange for consideration from a third party or to benefit an affiliate, except to address the needs of emergency communications, law enforcement, public safety (including FirstNet), or national security authorities, consistent with or as permitted by applicable law. Additionally, AT&T offers a wide variety of services to its customers, including but not limited to Voice over Internet Protocol (VoIP), Internet Protocol (IP)-video, unified messaging, Voice over LTE (VoLTE), and enterprise networking. These services share AT&T's network infrastructure and may rely on network practices to assign different levels of priority dynamically or statically. Use of these services may affect the availability of network resources for broadband internet access services, and thus the performance of that service. For example, your service may be interrupted, delayed, or otherwise limited in the event of a disaster or emergency, or during periods of congestion, to accommodate the needs of national security and emergency preparedness personnel.

What practices has AT&T adopted to manage network security?

AT&T takes the security of our customers and our network very seriously. We proactively monitor network activity to help guard against a wide range of security threats, including viruses, botnets, worms, distributed denial of service attacks, SPAM, and other harmful activity. We encourage customers to adopt their own security practices.

We use a variety of network tools to monitor network activity and health to maintain its stability and functionality, to protect the network against threats, and for other operational purposes. We store the information we gather through this monitoring for only as long as we have a business purpose to maintain it. The AT&T Privacy Policy describes how we collect, use and share this information. You can view AT&T's Privacy Policy at: **www.att.com/privacy (http://www.att.com/privacy)**.

If we detect a security threat, we will typically attempt to isolate the threat and minimize the impact to network service. We may use a variety of security measures to protect the network, including blocking malicious or unlawful traffic, redirecting the flow of traffic over some portions of our network, or taking other actions to address the threat. For example, as described in more detail below, we block certain ports that transfer malicious or disruptive traffic (such as Ports 25, 135, 139, 445, and 1900). We attempt to limit actions to the specific portions of our network or customer base impacted by the security threat and only for as long as necessary to mitigate the threat.

AT&T may scan or analyze network addresses that are registered through AT&T, including addresses that may have been delegated to customers, and/or routes that originate from AT&T-provided networks to detect vulnerabilities that might be used to compromise AT&T or customer assets or might be used in attacks against others. In doing so, we seek to avoid disrupting network service to customers. We may use information derived from these activities to identify and address security issues or to notify customers of issues.

As noted above, AT&T blocks certain ports that transfer malicious or disruptive traffic to protect our customers and our network. Below is more information about port blocking that is currently in place. We may block additional ports in the future based upon threat assessments.

Port	Transport	Protocol	Direction	Threats
0	TCP	Reserved	Both	Reserved Port
19	UDP	Chargen	Both	Reflective DDOS
25	TCP	SMTP	Outbound	SPAM, Malware
68	UDP	BOOTP	Outbound	DHCP server spoofing
123	UDP	NTP	Both	Reflective DDOS
135	TCP	NetBios	Both	Worms, Malware, Reflective DDoS

139	TCP	NetBios	Both	Worms, Malware
445	TCP	MS-DS SMB	Both	Worms, Malware
520	UDP	RIPv	Both	Reflective DDOS
1900	UDP	SSDP	Both	Reflective DDOS
3479	TCP	Twrpc	Both	End user device instability
7547	TCP	CWMP	Both	End user device instability
49152	TCP	Dynamic	Inbound	Unauthorized access, DoS
49955	TCP	Dynamic	Inbound	Unauthorized access, DoS
50001	TCP	Dynamic	Inbound	Unauthorized access, DoS
51001 - 51003	TCP	Dynamic	Inbound	Unauthorized access, DoS
51010 - 51011	TCP	Dynamic	Inbound	Unauthorized access, DoS
51020	TCP	Dynamic	Inbound	Unauthorized access, DoS
61001	TCP	IPDR	Both	Data exposure, end user device instability

Port 0/TCP: Port 0 is a reserved port. This port should not be used for any applications. Blocking protects our customers from potentially harmful types of network abuses.

Port 19/UDP: Port 19 Chargen is a protocol designed to generate a stream of characters for debugging and measurement. Because more recent tools have been developed for measurement and debugging purposes, blocking protects against use of this port in Reflective DDOS attacks.

Port 25/TCP: Simple Mail Transport Protocol (SMTP) is used to send email. Port 25/TCP may be blocked from customers with dynamically-assigned Internet Protocol (IP) addresses to protect systems from becoming a mail relay for SPAM. Customers can subscribe to AT&T SMTP services if they need to host an SMTP server on the internet.

Port 68/UDP: Port 68 is used to obtain dynamic IP address information from a dynamic host configuration protocol (DHCP) server. Port 68 may be blocked to eliminate the risk of exposure to a rogue DHCP server.

Port 123/UDP: Network Time Protocol (NTP) is used to accurately synchronize computer time of day to a reference time server. Some aspects of Port 123 may be limited to minimize malicious use. Poorly-configured NTP servers can be used for Reflective DDOS attacks, and some devices provide NTP service inadvertently, which exacerbates the port's malicious use.

Port 135/TCP: NetBIOS is a network file sharing protocol and is also known as Common Internet File System or LanManager. Blocking protects customers from exposing files unintentionally, worms, and viruses.

Port 139/TCP: NetBIOS is a network file sharing protocol and is also known as Common Internet File System or LanManager. Blocking protects customers from exposing critical system files unintentionally, which could give system access to a malicious actor.

Port 445/TCP: NetBIOS is a network file sharing protocol and is also known as Common Internet File System or LanManager. Blocking mitigates a potential threat to certain operating systems. Similar to our blocking of Ports 135 and 139, blocking Port 445 protects customers from exposing files unintentionally, worms, and viruses.

Port 520/UDP: RIPv1 - UDP port 520 is used by the Routing Information Protocol (RIP) to share network routing information. RIPv1 was designed to support route information sharing on small classful (class A, B, C, D) networks and has limited usefulness in today's classless networks. Port 520 has been used by malicious actors to generate Reflective DDOS attacks.

Port 1900/UDP: Universal Plug and Play (UPnP) is a protocol standard designed to allow device discovery over a local network. Some home routers may expose this port to the internet, which could allow attackers to defeat the security attributes of Network Address Translation (NAT) and allow attackers to use the port for Reflective DDOS attacks.

Port 3479/TCP: Twrpc is a protocol used for remote management of end user devices. Blocking this port protects customers from improper use of the port, which can cause end user device instability.

Port 7547/TCP: CPE WAN Management Protocol (CWMP) is a protocol used for remote management of end user devices. Blocking this port protects customers from improper use of the port, which can cause end user device instability.

Port 49152/TCP, 49955/TCP, 50001/TCP, 51001-51003/TCP, 51010-51011/TCP, 51020/TCP: These ports are numbered from the dynamic/private ephemeral port range. Their use varies according to implementation and may include end-user device management. Blocking these

ports protects customers from malicious activity, which may include data exposure or attacks against the end user devices.

Port 61001/TCP: Internet Protocol Detail Record (IPDR) is a specification used to collect information from end user devices including device configuration data. Blocking TCP port 61001 prevents certain types of malicious activity including data exposure and end user device attacks.

Does AT&T restrict the types of devices that customers can use with its mass market broadband internet access services?

AT&T makes available to its customers a variety of network interface equipment for use with the broadband internet access services we deliver to homes and businesses, many of which are Wi-Fi enabled. We also make available a variety of additional tools, equipment and services to assist our customers in configuring the local network access in their home or business to meet their particular needs. This allows AT&T customers to use devices of their choice (PCs, Smartphones, Tablets, Smart TVs, etc.) to connect to the broadband internet access services at their home or business via Wi-Fi, via the existing wiring at their premises or via such other compatible local networking technology as they may choose to select.

Customers of our mass market mobile services may attach 3G-, 4G-, and 5G-capable devices of their choice to our mobile broadband internet access services, so long as the devices are FCC-approved, compatible with the technology used in our mobile network, and do not harm our network or other users. AT&T has retired its 2G network and we will not activate 2G-only capable devices. Our wired and Wi-Fi networks require compatible Ethernet or Wi-Fi capable devices. AT&T generally does not support IEEE2 802.11b or earlier Wi-Fi protocols. Devices must also be used in a manner consistent with our terms of service and Acceptable Use Policy. For example, some data plans are designated for use with only a basic phone or smartphone, in which case customers may not use their device to provide an internet access connection to other equipment/devices (such as computers, netbooks, tablets, other phones, USB modems, network routers, media players, gaming consoles, or other data-capable devices) by tethering, by SIM card transfer, or any other means. However, customers wishing to use their service with a mobile hotspot/tethering device may purchase a data plan that already includes such use.