

FRANKFORT PLANT BOARD CABLE MODEM INTERNET

BROADBAND INTERNET SERVICE DISCLOSURES

Consistent with FCC¹ regulations, Frankfort Plant Board (FPB) provides this information about our broadband Internet access services. We welcome questions or comments about this information. You may contact us in person at 151 Flynn Avenue, Frankfort, KY 40601, or by phone at 502-352-4372.

NETWORK PRACTICES

General description: We continually monitor our network and traffic patterns and make changes we deem necessary to manage and improve overall network performance. FPB uses reasonable, nondiscriminatory, network management practices to improve overall network performance to ensure a high-quality online experience for all users. Our network management practices do not target any specific content, application, service, or device. As network management issues arise and as technology develops, we may employ additional or new network management practices. We will update these disclosures as necessary.

Related documents and disclosures: Use of our broadband service is also governed by the following:

- FPB Product Definition, available at <https://fpb.cc/s/SectionX2020.pdf>

These documents contain important information regarding FPB's broadband service and its use. We encourage you to read them.

Congestion Management:

We describe in this section network management practices used to address congestion on our network.

Congestion Management Practices Used

Real-time "fair share" traffic management: FPB utilizes monitoring and application/protocol agnostic means of maximizing performance for as many customers as possible by ensuring that each user has access to a fair share of the available bandwidth.

Network monitoring: We monitor our network for utilization trends, changes in network traffic, and congestion on a daily basis. We use this information to plan increases in bandwidth available, port additions, or additional connectivity to the Internet.

Types of traffic affected: Our congestion management practices do not target any specific content, application, service, or device. As such, any network traffic is potentially affected as congestion can occur anywhere at any time on FPB's network.

¹ 47 CFR 8.3 and *In re: Preserving the Open Internet, Broadband Industry Practices, Report and Order*, 22 FCC Rcd 17905 (2010).

Purposes of congestion management practices: Our network is a shared network. This means that our customers share upstream and downstream bandwidth. The goal of our congestion management practices is to enable better network availability and speeds for all users. Our congestion management practices serve to help us adapt and upgrade our network to maintain or improve network performance as demand increases. These management practices also help us adapt and upgrade our network to maintain or improve network performance as demand for higher bandwidth applications increases. Some examples of higher bandwidth applications are gaming, streaming movies, and streaming high definition video.

Congestion Management Criteria

Network monitoring: Our network monitoring provides data to help us plan upgrades to our network, equipment, technology, and connectivity to the Internet. As demand for service increases and as demand for higher bandwidth applications increases, we monitor the effects on network performance and plan upgrades as we deem necessary. We have not established specific criteria to govern our upgrade decisions.

Effects on end user experience: Because our broadband Internet network is a shared network, periods of high network demand may result in Internet traffic congestion. End users may experience reduced bandwidth or speed during these times.

Typical frequency of congestion: Network congestion occurs on portions of our network on an irregular basis. When congestion occurs, it is during periods of peak demand for higher bandwidth applications. These high bandwidth applications tend to see their highest usage between 6pm and 11pm local time. As a result, this is usually the time frame that a congestion event is most likely to occur.

Application-Specific Practices:

This section discloses any application-specific practices we use, if any.

Management of specific protocols or protocol ports: All ports and protocols are subject to our management practices. As described below, to ensure network and end user security, we also may employ practices that affect specific protocols or ports.

Modification of protocol fields: FPB does not modify protocol fields.

Applications or classes of applications inhibited or favored: Our congestion management practices are application and protocol agnostic.

Device Attachment Rules:

This section addresses any limitations on attaching lawful devices to our network.

General restrictions on types of devices to connect to network: We place no restrictions on lawful devices that a customer may connect our network, so long as the device is: (i) compatible with our network; and (ii) does not harm our network or other users. Our service works with most types of PCs and laptops including Macs, and other Internet compatible devices like game systems and Internet enabled TVs. If a wireless router is connected, wireless Internet compatible devices including computers, tablets, smartphones and other devices can connect to our network.

Cable Modems: FPB requires a cable modem to connect to our network. You can obtain a cable modem from us or you may purchase one from most retail electronics sellers. Only devices that have been fully certified by CableLabs as compliant with the DOCSIS 2.0 or DOCSIS 3.0 specifications may be used. FPB does not maintain a list of supported DOCSIS 2.0 devices. The current list of supported DOCSIS 3.0 modems is as follows (list is subject to frequent change): Motorola SURFboard models: SB6120, SB6121, SB6141, SB6180

Once operational on FPB's network, we will manage and update the firmware on the customer-owned devices as needed.

Network and end-user security:

This section provides a general description of the practices we use to maintain security on our systems.

Practices Used to Ensure End-User Security (including triggering conditions)

Hostile port blocking: We block known hostile ports to reduce attacks on customers.

SMTP traffic (mail clients): Email traffic (SMTP) directly from customers using residential service package is allowed only through FPB's email platform. This reduces the occurrence of unsolicited bulk email originating from exploited computers. While customers may receive email into a client (i.e. Outlook Express) via POP3, they may not send outbound mail through another server directly using SMTP (alternatives are ports 587 or 465).

Infected messages: FPB employs industry standard virus scanning and prevention techniques on its email platform for mail inbound from the public network. Infected incoming messages for our email service are quarantined and the customer is notified via email. Should an outbound email message be found to contain a virus or other harmful content, the message will be deleted without notification given to either the sender or the intended recipient(s).

Practices Used to Ensure Network Security (including triggering conditions)

Hostile port blocking: We block known hostile ports to reduce attacks on the network.

Traffic monitoring: Viruses, worms, Trojans, and other "malware" or "spyware" pose a significant threat to our network. In an effort to minimize these threats, FPB constantly monitors the activity and traffic patterns of its network. If we reasonably determine that originating traffic from a user is a form of harmful traffic, we will take actions to interrupt the traffic from that user until we determine the harmful traffic has ceased or that the traffic is legitimate traffic.

Firewall protection: We maintain firewalls to resist hacking and other traffic intended to harm our network.

PERFORMANCE CHARACTERISTICS

General Service Description: FPB serves as a local Internet service provider (ISP). The service enables residential and commercial subscribers to access all lawful content, applications, and services of their choice available on the Internet.

Service technology: We deliver our service over our hybrid fiber-coaxial (HFC) network using the Data Over Cable Service Interface Specification (DOCSIS). Service is provided using a Cable Modem Termination System (CMTS), hardware in our cable network that acts as a gateway to the Internet for cable modems located at the customer premise. Cable modems, in turn, are used to access the FPB's High Speed Internet network. This is a shared network, which means that our customers share upstream and downstream bandwidth.

Expected and Actual Speeds and Latency

Expected performance: FPB provides customers with a variety of high speed Internet plans from which to choose. A description of these product offerings with expected throughputs is available at:

<https://fpb.cc/s/SectionX2020.pdf>

Speed: FPB provisions its customers' modems and engineers its network to ensure that its customers can enjoy the speeds to which they subscribe. However, FPB does not guarantee that a customer will actually achieve those speeds at all times. FPB advertises its speeds up to a maximum level based on the tier of service to which a customer subscribes. Accordingly, the speeds advertised for FPB broadband Internet service describe the maximum upload and download speeds that subscribers are likely to experience. A variety of factors can affect upload and download speeds, including customer equipment; network equipment; congestion in our network; congestion beyond our network; performance issues with an Internet application, content, or service; and more.

Latency: Latency is another measurement of Internet performance. Latency is the time delay in transmitting or receiving packets on a network. Latency is primarily a function of the distance between two points of transmission, but also can be affected by the quality of the network or networks used in transmission. Latency is typically measured in milliseconds, and generally has no significant impact on typical everyday Internet usage. As latency varies based on any number of factors, most importantly the distance between a customer's computer and the ultimate Internet destination (as well as the number and variety of networks your packets cross), it is not possible to provide customers with a single figure that will define latency as part of a user experience.

Actual speed and latency performance: Actual speed performance in terms of speed and latency may vary depending upon network conditions and other factors. For example, broadband performance may be affected by the capabilities and limitations of the consumer's own computer or local area network ("LAN") devices such as home Wi-Fi routers, or by the performance of content and applications providers the consumer is accessing. Actual performance of FPB Broadband Internet Service in most cases will conform to national wireline broadband Internet speed and latency levels reported by the FCC². The FCC has reported that customers of coaxial cable-based broadband Internet services receive mean download speeds that are within 93% of advertised speeds during non-peak hours, and 85.7% of advertised speeds during peak hours³. In addition, the FCC has reported that these same customers experience average latency⁴ delays of 28 milliseconds, increasing by an average of 30 milliseconds during peak hours.

Customer Speed Test: We direct interested customers to a "speed test" for testing purposes, available at <http://sprint.com/speedtest/>. Should a customer experience a problem, we will troubleshoot with the customer to determine if the problem is signal related and dispatch a service technician if necessary.

Suitability of the Service for Real-time Applications: Our FPB Internet service is suitable for typical real-time applications including messaging, voice applications, video chat applications, gaming, streaming media. If users or developers have questions about particular real-time applications, please contact us in person at 151 Flynn Avenue, Frankfort, KY 40601 or by phone at 502-352-4372.

Specialized Services

Specialized services offered to end users: FPB offers other managed services over its broadband cable network, sharing network capacity with its high speed Internet services, including voice over Internet Protocol (VoIP).

Effects of specialized services on availability and performance of broadband Internet access service. The offering of these services has no effect on the availability and performance of our broadband service.

² See FCC's Office of Engineering and Technology and Consumer Affairs Bureau, Measuring Broadband, A Report on Consumer Wireline Broadband Performance in the U.S., OET CGB DOC-308828A1, pp. 4-6 (Aug. 2, 2011) (available at: http://transition.fcc.gov/cgb/measuringbroadbandreport/Measuring_U.S._Main_Report_Full.pdf).

³ The FCC has defined peak hours measured during "busy hour" as weeknights between 7:00 pm and 11:00 pm local time.

⁴ The FCC has defined latency is the total length of time it takes a signal to travel from an origination point to the nearest server, plus the time for an acknowledgement of receipt to travel back to the origination point. The nearest server is the server providing the minimum round trip time.

COMMERCIAL TERMS

Prices: Monthly prices for our broadband service are available at: <https://fpb.cc/s/SectionX2020.pdf>

Fees for early termination: FPB does not charge early termination fees.

Fees for additional network services: FPB offers additional email addresses, public IP addresses, and static IP addresses for an extra charge. Charges for these additional network services may be found at <https://fpb.cc/s/SectionX2020.pdf>

Privacy policies: We do not disclose customer information to third parties except: (i) as necessary to provide service and to manage our network; or (ii) in response to law enforcement requests, court order, or as otherwise required or authorized by law.

Inspection of network traffic: FPB routinely monitors its network and traffic patterns.

Traffic monitoring: Viruses, worms, Trojans, and other “malware” or “spyware” pose a significant threat to the uninhibited and beneficial access to the resources on the Internet. One of the more prevalent forms of such disruptions is found in infections from viruses and worms perpetrated by SPAMMERS for the sole purpose of using unsuspecting Internet users’ computers to send out their illicit email. In an effort to minimize the impact of this type of infection, FPB constantly monitors the activity and traffic patterns of its network.

Infected messages: FPB employs industry standard virus scanning and prevention techniques on its email platform for mail inbound from the public network.

Storage of network traffic information: DHCP (Dynamic Host Configuration Protocol) information is a code included in all network traffic that associates that traffic with a particular cable modem sending or receiving the traffic. We store DHCP information for at least 3 months.

Provision of network traffic information to third parties: We may disclose network traffic information to third parties solely for purposes of providing and maintain our broadband product or if required by law.

Use of network traffic information for non-network management purposes: FPB does not use network traffic information for non-network management purposes.

Website and Subscriber Privacy: FPB collects and stores information from many sources as it relates to providing and maintaining service to its customers. As a general rule, this data is only used directly in support of its products and services. Personally identifiable information is only disclosed outside under compulsion of law.

Redress Options

Practices for resolving end-user and edge provider complaints and questions: End-users or edge providers with complaints or questions relating to these disclosures should contact:

Frankfort Plant Board
151 Flynn Avenue, Frankfort, KY 40601
502-352-4372
Email: help@fewpb.com

Questions: We will endeavor to answer questions promptly via email or voice.

Complaints: We will provide an initial response in writing within 15 business days of receipt. We will attempt to resolve complaints informally, escalating the matter to senior management if needed.