Internet Product Disclosure

Network Practices

Congestion Management Policy

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

When network congestion is identified, iRis Networks uses various techniques to create a good customer experience. Our network management techniques include preventing virus/spam delivery to customer email accounts. We also reinforce our network with additional capacity in areas where congestion is identified or as part of standard network engineering design plans. Also, we may seek to ensure that our customers are not excessively using the service. In very rare cases, we may need to downgrade the service available to existing customers or even disconnect services.

The links iRis Networks and other networks use to exchange traffic may also become congested at times. iRis Networks 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, iRis Networks 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 iRis Networks' 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 iRis Networks 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. Unfortunately, iRis Networks 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.

Application-Specific and/or User-Specific Policy

iRis Networks 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, iRis Networks deploys Type of Service (ToS) and Differentiated Service (DiffServe) capabilities at the customer modem and in limited network equipment deployed across the iRis Networks High-Speed Internet network 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.

iRis Networks 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 its EUP policies, practices described above and the security practices described in the security policy section below.

iRis Networks 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.

Security Policy

iRis Networks engineers are dedicated to managing our network to ensure that all customers receive the most secure online experience. We use industry standard security practices to manage our network, provide services to our customers, and ensure compliance with our Acceptable Use Policy and the terms of our High-Speed Internet agreement. 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, iRis Networks engineers employ various techniques to help provide a positive customer experience. Our security management techniques include ensuring that customer systems are not propagating viruses, distributing spam email, or engaging in other malicious behavior. For example, we use industry best practices to prevent virus/spam delivery to customer email accounts. We provide antivirus and antimalware applications at no additional charge to our High-Speed Internet customers. We also automatically detect and mitigate DoS (Denial of Service) attacks for our High-Speed Internet customers. We 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.

We reserve the right at any time to take action to protect the integrity and normal operation of our networks and to safeguard our 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 iRis Networks 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.

iRis Networks 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.

iRis Networks 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.

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

iRis Networks 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

iRis Networks 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 like iRis Networks 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."

More information regarding the MAAWG Port 25 filtering best practices can be found at http://www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf.

UDP Port 1900 Blocking

iRis Networks 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 iRis Networks High-Speed Internet access service, the service we quote you is based on an advertised "up to" connection speed. We continually upgrade our network, but our quoted speed is based on the characteristics of the relevant network facilities at the time you order. We will confirm your advertised speed at the time of installation.

The actual throughput you experience may vary. During most periods, based on iRis Networks' evaluation, most customers, except for Gigabit customers 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 provisioned between the network device and the in-premises modem and may vary due to physical condition of the line and other factors. The percentage of throughput achieved will vary depending on the amount of bandwidth our network uses in delivering service to you, as well as other factors outside of iRis Networks control such as customer location, the quality of the inside wiring within the home, the websites accessed by the customer, usage of the network during peak periods of the day and the customer's equipment within the home or premises.

The ultrafast gigabit service delivers a line rate of 1 Gb/s* speed from the network to the home with an IP bandwidth throughput of up to 940Mb/s.   Protocols within the gigabit service technology and Internet protocol consume a small portion (around 60Mb/s) of the 1Gb/s line rate for signaling and control to ensure the data is reliably delivered.   All devices within a premise will share the available bandwidth within the gigabit service. If multiple users or devices are connected to the service, any given speed test will show results of less than 940Mb/s.   Speed test results for gigabit service can be impacted by the same factors as other broadband products. These factors may be outside iRis Networks’ control and include customer location, the quality of the inside wiring within the home, the websites accessed by the customer, usage of the network during peak periods of the day, and the customer's equipment within the home or premises.

* - Note: 1Gb/s = 1,000 Mb/s.

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. iRis Networks measures latency by measuring the round-trip time from the consumer's home to the closest measurement server and back. iRis Networks High-Speed Internet customers should expect roundtrip latency to most general Internet sites in the range from 50-150 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. iRis Networks denotes a packet as lost if the latency exceeds 3 seconds or if the packet is never received. iRis Networks High-Speed Internet customers should generally expect to experience packet loss at the rate significantly below 1% or at levels unlikely to significantly affect customer experience.

Consumers may also determine the High-Speed Internet speeds available at their address on the iRis Networks website located at www.iRis Networks.com. For a full description of the iRis Networks High-Speed Internet service, please refer to your service agreement.

Once service is installed, customers can also determine the throughput of their High-Speed Internet service via the (iRis Speed Test Link here)

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

Network speeds for iRis Networks High-Speed Internet services provided over Wi-Fi services may vary. The performance the user experiences, once they connect, may vary based on any number of factors, such as the maximum bandwidth allocated for Wi-Fi services, the number of other users trying to use the same Wi-Fi at the same time, the user's computer or wireless device, the Wi-Fi receiving antenna, and the distance from the Wi-Fi router. These Wi-Fi routers use spectrum that the FCC has allocated for "unlicensed" use, which means that, like wireless routers used for in-premise 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.

iRis Networks Hosted Phone Product

iRis Networks offers an Internet Protocol-voice based service to customers with iRis Networks High-Speed Internet service which, due to the product's sensitivity to latency, receives quality of service (QoS) treatment on the iRis Networks network where it is available. This treatment of VoIP traffic should have no material impact on capacity or bandwidth availability for Broadband Internet Access.

Customers purchasing iRis Networks Phone Product may experience a higher quality of service through improved latency for upstream voice packets carried over the iRis Networks High-Speed Internet network. This higher quality of service is enabled through Type of Service (ToS) and Differentiated Service (DiffServe) capabilities at the customer modem and in limited network equipment deployed across the iRis Networks high speed Internet network. The setting established at the modem may be modified by our customers.

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.

Customers may also speak with an iRis Networks representative to learn about services in their area by calling iRis Networks at 1-888-273-5881.

Privacy Policy

Like most companies, we have certain information about our customers and use it to provide our services. We also share it as needed to meet our business goals or fulfill our legal obligations. We protect the information we have about our customers, and we require those we share it with to protect it, too. We use information generated on our networks to manage those networks, to plan for future development, and to keep our services running reliably and efficiently. For example, we monitor data to check for viruses, to control spam, to prevent attacks that might disable our services, to ensure that your traffic does not violate your subscriber agreement or our acceptable use policies, and to guard against other inappropriate or illegal activity. This may involve looking at the characteristics of our network traffic, such as traffic volumes, beginning and ending points of transmissions, and the types of applications being used to send traffic across our network. In limited circumstances, we need to look into the content of the data (such as the specific websites being visited, files being transmitted, or application being used) for the purposes described above, in circumstances when we are concerned about fraud or harassment, to repair a problem we detect or that a customer contacts us about, or when we are providing the content of broadband traffic to law enforcement which we only do as authorized by law.

Redress Options Policy

If you have any questions or concerns regarding iRis Networks High-Speed Internet services and the subjects of this disclosure, you may send an email to:

noc@iRistransport.com

Please include the following information:

- **Subject Line:** Internet Management Disclosure
- **Name:** (Optional)
- High-Speed Internet Service Address
- A brief summary of the nature of your concern

iRis Networks takes all such questions and concerns seriously. The appropriate iRis Networks personnel will review all such submissions and respond in a timely manner.