Xbox One

Technical information on P2P Networking Behavior

Version 1.0

Last updated: October 6, 2013

Many gaming and app scenarios on Xbox® One rely on low-latency peer-to-peer (P2P) networking capabilities. The platform for these capabilities leverages **IPv6, Teredo, and IPsec Internet standards**.

The primary purpose of this document is provide technical information on Xbox One P2P behavior, so that network operators and network equipment manufacturers can address possible configuration issues and ensure end-users have a positive experience.

# IPv6 and IPsec

One of the many benefits of IPv6 is simplified connectivity between peers on the Internet. Xbox One takes advantage of this, and IPv6 ***may*** be attempted as a connectivity mechanism between peers if available.

Proper authentication of peers and integrity of data traffic is critical to fair, safe gaming. To this purpose, transport-mode IPsec is used for most P2P traffic in most games, with IKEv2 used for security setup ([RFC 5996](http://tools.ietf.org/html/rfc5996)).

[RFC 6092](http://tools.ietf.org/html/rfc6092) provides useful guidelines on the security and filtering behavior for IPv6 customer premise equipment.

* **Allow IPsec and IKE**
	+ In general P2P traffic will be used with IPsec with the encapsulating security payload (ESP) option. Section 3.2.4 provides guidelines on interacting with IPsec.
		- *“The Internet Protocol security (IPsec) suite offers greater flexibility and better overall security than the simple security of stateful packet filtering at network perimeters. Therefore, residential IPv6 gateways need not prohibit IPsec traffic flows.”*
		- Ensure that you are not filtering inbound IKE traffic – which is UDP on port 500 and port 4500.
* **Enable transparent operation**
	+ We also note Recommendation 49. This may be relevant for users troubleshooting connectivity issues or who in general desire transparent operation.
		- *“Internet gateways with IPv6 simple security capabilities MUST provide an easily selected configuration option that permits a "transparent mode" of operation that forwards all unsolicited flows regardless of forwarding direction, i.e., not to use the IPv6 simple security capabilities of the gateway. The transparent mode of operation MAY be the default configuration.”*

# Teredo

IPv6 is not yet globally available in the consumer Internet market. For the majority of users, Teredo will be used to provide P2P connectivity. Teredo is an IPv6 transition technology that provides Teredo clients a tunneled IPv6 address for P2P connectivity.

Teredo can also be used to provide connectivity to hosts on the native IPv6 Internet, using a Teredo relay. However, that capability will be rarely used by Xbox One.

The Teredo implementation on Xbox One behaves similar to that on Windows® 7 and 8.1. The design of Teredo is described in [RFC 4380](http://tools.ietf.org/html/rfc4380), [RFC 5991](http://tools.ietf.org/html/rfc5991), and [RFC 6081](http://tools.ietf.org/html/rfc6081). We have [additional documentation on Teredo available on TechNet](http://technet.microsoft.com/en-us/library/bb457011.aspx).

Even for users that do have native IPv6 – Teredo will be used to interact with IPv4-only peers, or in cases where IPv6 connectivity between peers is not functioning. In general, Xbox One will dynamically assess and use the best available connectivity method (Native IPv6, Teredo, and even IPv4). The implementation is similar in sprit to [RFC 6555](http://tools.ietf.org/html/rfc6555).

For that reason, it is important for all interested network operators to understand Teredo operating requirements. Xbox One does not support operating on an IPv6-only network because of the need to reliably interoperate with nodes on IPv4-only networks.

* **Allow UDP**
	+ Teredo uses UDP to create port mappings in NAT equipment and to communicate with Teredo peers. [RFC 4787](http://tools.ietf.org/html/rfc4787) and [RFC 6888](http://tools.ietf.org/html/rfc6888) provide recommendations on UDP behavior of network equipment. Sections 4-6 of RFC 4787 are especially relevant to network operators and equipment vendors.
* **Configure open NATs, avoid symmetric**
	+ RFC 6081, Section 3, provides a connectivity matrix for Teredo. In general, cone, address restricted, and port restricted NATs, work fine with Teredo. Networks that block UDP traffic will not support P2P gaming. The more “open” a NAT, the more likely the user will be able to communicate directly with others, and in general the better experience the user will have.
* **Avoid requiring frequent keep-alives**
	+ Even with networks that support UDP, if the keep-alive interval for UDP port mappings is less than 60 seconds – then connectivity issues may arise for end-users.
	+ RFC 4787 recommends 5 minutes.
	+ Teredo will refresh port mappings approximately every 30 seconds.
* **Support hairpinning**
	+ Networks should support hairpinning (Section 6 of RFC 4787), to allow multiple Teredo clients on the same network to communicate with one another. Compliance with this recommendation is especially important for network operators who are deploying carrier-grade NAT functionally.
* **Don’t block encapsulated IPsec**
	+ With Teredo, IPv6 packets are encapsulated in an IPv4 UDP datagram. These IPv6 packets will be secured with IPsec, as described earlier.
	+ If for any reason a network administrator performs de-encapsulation of Teredo traffic for inspection purposes, they should allow IPsec traffic, and generally follow the guidelines provided earlier for IPv6 security.

## Teredo Ports

Teredo clients will initiate contact with a Teredo server that is listening on port 3544, using UDP, as part of the Teredo client qualification procedure. The local port is from the dynamic range. Enabling port forwarding for port 3544 is not necessary or helpful.

**For actual P2P traffic, Teredo will attempt to use local port 3074, again with UDP. This is the same port that Xbox 360 uses. Enabling inbound communication to this port using explicit port forwarding rules is helpful, though rarely required.** Teredo will attempt to use UPnP and UDP messages to ensure inbound connectivity to the Teredo port.

If 3074 is unavailable, a local port from the dynamic port range (49152-65535) will be used – and again Teredo will attempt to automatically provide inbound connectivity without the need for explicit port forwarding rules.

Xbox One IPv4 P2P traffic may be distinguished from other types of IPv4 traffic by identifying:

1. The ***typical*** usage of port 3074 in a UDP datagram.
2. That the traffic is embedding Teredo packets.
	1. One can identify this by looking for the four bytes for the 2001:0000 prefix in the IPv6 header.
3. That the embedded Teredo packets use an ESP header.

We expect this **combination** should be fairly unique to Xbox One. Items 2 and 3 can be used to distinguish Xbox One traffic from Xbox 360 traffic, and items 1 and 3 can be used to distinguish Xbox One traffic from common Teredo traffic. We recommend network administrators treat Xbox One and Xbox 360 traffic similarly.



Figure 1 - Packet format with Teredo and IPsec, as used by Xbox One.

# Monitoring and Support

If authorized by the end-user, Microsoft® collects telemetry on the performance and reliability of P2P networking on Xbox One. This information will be used to engage with network operators if geographically specific issues are found.

Xbox One includes a network troubleshooter, which can inform the user if their network is not compliant with the above requirements.

Network operators and equipment vendors can address questions and concerns to xboxteredo@microsoft.com.