Review Request Form

The Broadband Internet Technical Advisory Group, Inc. (BITAG) is an independent non-profit organization, whose mission is to bring together engineers and other similar technical experts to develop consensus on broadband network management practices or other related technical issues that can affect users' Internet experience, including the impact to and from applications, content and devices that utilize the Internet.

REVIEW REQUEST

1. Requesting Party Details:

Name of Organization	Comcast
Address of Organization	One Comcast Center, Philadelphia, PA, 19103
Organization URL	www.comcast.com
Name of Submitter	[redacted]
Position and Title of Submitter	[redacted]
Submitter Email	[redacted]
Submitter Phone #	[redacted]
BITAG Member (Y or N)	Y

2. Description of Underlying Technical Issue and Why TWG Review Would Inform the Public and Policymakers:

Please fully describe the underlying technical issue here. Attach additional documents or information as necessary. For example: relevant diagrams, illustrations, reports, studies, specifications, or standards. URLs to each of these are helpful as well.

a) Title of the Technical Issue:
Implications of and Practical Responses to SNMP DDoS Attacks
b) Detailed description of the Technical Issue:
Summary Comcast has observed large-scale SNMP reflection attacks where subscriber devices can in some cases be used unwittingly to generate significant and sustained levels of traffic, targeted against other networks or sites. This can be service-affecting for the targets. As a result, we believe ISPs may need to consider a range of potential network management responses to this issue. The request is that BITAG assess the likely technical implications of any potential network management responses and whether there are other alternative responses that ISPs may wish to consider. **Background** SNMP (Simple Network Management Protocol) is a service that runs on a network host and can be used by a remote administrator to ascertain the host's health status, as well as to perform maintenance functions. The SNMP 'community string' is a naming convention used by administrators. The community strings "public" and "private" are common defaults that administrators should change to follow good security practices. SNMP is typically used within a LAN or a company's WAN and not in public Internet space, partly because of security issues with the protocol and risks of exposing server and networking information to the general public. Controls are usually leveraged to disallow SNMP from being used on public interface ports on such hosts. SNMP uses UDP port 161, which is a connectionless protocol. It is therefore relatively easy to spoof the source IP, as no return traffic is required to elicit a response. **Overview of New SNMP Attacks Observed** Comcast has observed a new type of SNMP attack (or at least an attack at a unique scale). This attack works by spoofing the IP address of the intended victim, and sending an SNMP 'bulk get' query to a reachable device with the default community string of "public." Any device listening for SNMP requests that are configured with

the matching community string will then respond by sending its entire SNMP data set (Management Information Base, or MIB, tree). *A single request packet of about 122 bytes can generate 900 - 1,000 response packets.* So a single request packet can be amplified to 900 – 1,000 packets in response, and a typical response will generate about 21 KB of data. Thus, the attacker is sending very little data, which makes identification of the attacker's host(s) very difficult.

The devices affected appear to be customer-owned home gateway devices that are typically configured with the public SNMP community string, rather than ISP-managed devices since ISP-managed devices that typically are not so configured. Since home gateway devices are customer-managed and do not automatically update their firmware, this is a situation where an ISP is unable to remotely update or reconfigure devices that it does not control.

Network logs provided to Comcast from some of the attack targets indicate that most of the subscribers whose devices were unwittingly responding to the SNMP queries were using a NetGear WNR1000, Apple Airport (models prior to 2009), or SMC WBR14 (firmware versions prior to November 2011), though it is conceivable that other devices could be affected. We have also observed that some devices were delivered to market with SNMP enabled and listening on its public facing port with a community string of "public." And in some such models, the end user *does not* have a configuration option to disable the SNMP service or change the default community string.

Event History

In the Fall of 2011, Comcast observed online chatter concerning a script that could purportedly be used to attack Internet hosts by "reflecting" SNMP queries off of broadband subscribers. In early November we observed a large hosting provider come under a large, service-affecting DDoS attack. This reached peaks of 40 Gbps, and greater than 10 Gbps sustained for hours at a time. We observed additional DDoS events during November and December 2011, with similar patterns of attack. During those follow-on attacks, we observed peak attack traffic of over 60 Gbps. In addition, while in the initial attack Comcast seemed to be the primary ISP with customers unwitting involved in the DDoS attack, in the most recent incident other broadband ISP networks were involved, and we believe one European ISP network exceeded Comcast's 60 Gbps of traffic. This demonstrates that this form of attack affects multiple networks, and so is not or will not be unique to any particular ISP, and that the potential volume of attack traffic is quite large.

In each event, the volume of SNMP traffic did not negatively impact Comcast's networks, nor did it reach levels that triggered any alarms for general traffic volume, largely due to (i) the high broadband speeds offered on a per subscriber basis and (ii) the large capacity of our IP network.

Threat Analysis

Research of other major ISPs does not seem to suggest anything unique about this SNMP issue or the treatment of SNMP packets in Comcast's network as compared

to other networks. This assumption seems to have been validated in December 2011, given that the last incident involved a European ISP that did not share our access network technology, and that observed a greater volume of peak traffic than we did. *Networks, applications, and services that may be targets of such attacks are at risk of sustained, service-affecting disruptions to their services.*

Potential Mitigations

1. Device makers could update firmware to disallow the 'public' SNMP community string and/or turn off SNMP by default. While this is a good and apparently common practice for new devices, there are two problems with the embedded base of devices. First, device makers have little incentive to update firmware for old devices. Second, very few end users ever upgrade their firmware or even know how to do so.

2. ISPs could allow only "good" source IPs that are not spoofed. While Comcast already enforces this policy on its network, many other ISPs do not appear to enforce this policy. This leaves them vulnerable for attacks originating from hosts in their networks. Encouraging other ISPs to implement this policy is a long-term effort and it is therefore unlikely to have a near-term impact on this particular issue.

3. An ISP could place addresses that are the target of the SNMP reflection attacks into a null route and propagate the route to all routers for 24 hours or longer. However, this effectively prevents all subscriber traffic from reaching the targeted IP address ranges, which contain lawful services and applications.

4. An ISP could block the SNMP protocol (UDP/161) in some or all devices.

    a. In all devices, which could negatively affect business users that appear to regularly use SNMP.

    b. In only residential devices, where the use of SNMP appears to be negligible to non-existent.

    c. On only selected tiers of service, on a more finely grained basis that (b) above.

    d. On a per-customer basis, which is likely to be quite costly and unlikely to scale well.

c) Describe which BITAG Member Categories are affected by this issue (i.e., Applications Providers, Community Representatives, Content Producers, Equipment Manufacturers, Internet Connectivity Providers):

All elements of the Internet community described above are potentially affected by this issue.

- Equipment Manufacturers make home gateway devices and provide updated firmware for existing devices.
- ISPs could have their users unwittingly used to originate the attack traffic or for the reflection part of the attack.
- Members of the community, such as end users, could be affected by being an unwitting participant in one of the stages of the attack, or by the effects of mitigating efforts.
- All elements of the community may become a target of such an attack.

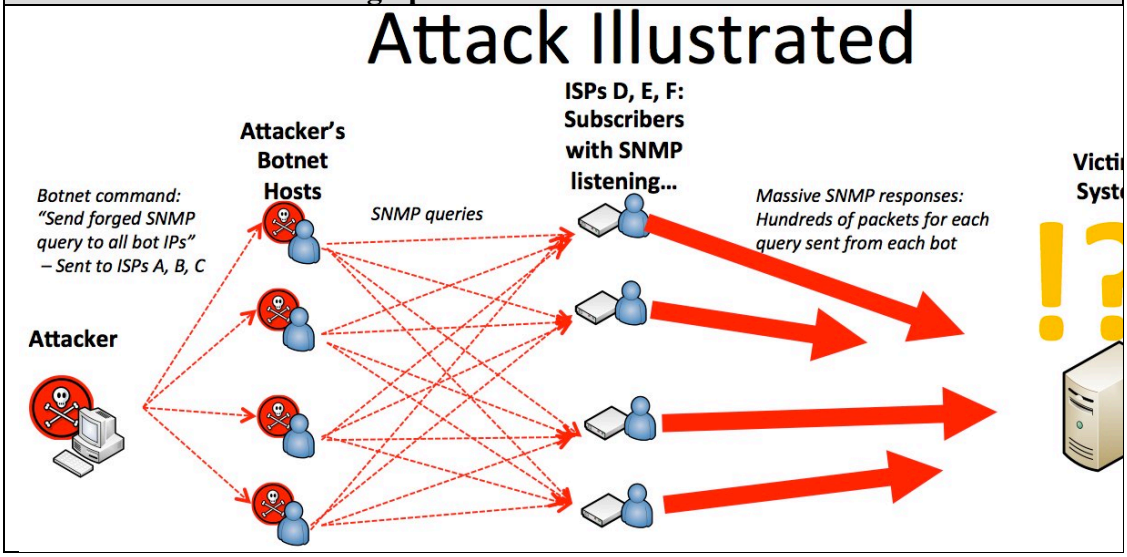
d) Describe why a BITAG Technical Working Group Review of this technical issue would inform policymakers and the public:

We believe we may be observing early phases of this type of attack used at this scale, which could soon affect other ISPs. In addition, we think it is important to understand any possible implications of various potential network management responses. There are also likely recommended practices for equipment manufacturers and ISPs.

e) What relevant standards or standards bodies are directly implicated or related to this issue:

Standards bodies: Potential exists for an IETF BCP on SNMP

f) Please Provide or attach additional diagrams or items that would be helpful to other Technical Working Group Representatives in evaluating the merits of taking up this technical issue for review:



g) Additional items that may be relevant:
N/A

3. Identify Any Potential Adverse Parties (attach additional page(s) if necessary):

Name	Reason for Adversity

4. Filing Fee:

Review requests will not be considered complete or examined until we receive the requisite filing fee (if applicable). Please contact reviewrequest@bitag.org about submitting your filing fee.

Filing Fee for 2012:

Industry Tier (revenue)	**Member**	**Non-Member**
Above $5B	No Charge for Members	$30,000
$1B to $5B	No Charge for Members	$15,000
$100M to $1B	No Charge for Members	$13,500
Under $100M	No Charge for Members	$12,000
Trade Association Tier (budget)	**Member**	**Non-Member**
Any Size Budget	$25,000	$30,000
Community Representative Tier (budget)	**Member**	**Non-Member**
Any Size budget	No Charge for Members	$5,000
Individual Tier	**Member**	**Non-member**
Any Individual	No Charge for Members	$5,000

5. Declaration:

The information provided in this request is true to the best of my knowledge. I understand that upon submission, this request and any attached documents become the property of BITAG, Inc. I also understand that all review requests must be germane to the Technical Working Group (TWG) and its mission. Further, I understand that BITAG reserves the right to reject any request not filled out properly, not germane to the TWG mission, or where the requisite filing fee (if applicable) is not received.

DATE: ____2/1/2012_____

SIGN: [redacted]

PRINT: [redacted]