CONTRIBUTION:	NTCO0362
DATE:	August 3, 2006
WORKING GROUP:	Network Working Group
TITLE:	Analysis of IP Address Tracking Options in DOCSIS Networks
ISSUES ADDRESSED:	Analysis of IP address tracking options.
SOURCE:	Jason Lowe Senior Cable Specialist Clearcable Networks 141 Hester Street Hamilton, ON L9A 2N9 Canada (905) 667 3909 jason@clearcable.ca
DISTRIBUTION:	NTWG Interested Parties
REFERENCE:	NTWG TIF 18 NTTF018D, IP Address tracking in Cable Networks. NTCO0359, IP Address tracking in Cable Networks.
FILE NAME:	NTCO0362.doc
NOTICE:	*This contribution has been prepared by Clearcable Networks to assist the Network Working Group as basis for discussion. This should not be construed as a binding proposal on Clearcable Networks. Specifically, Clearcable Networks reserves the right to amend, modify or withdraw this contribution at any time.*

BACKGROUND ON TRACKING IP ADDRESSES FOR THIRD PARTY ISPS

1. Multiple options exist that can allow Third party ISPs to track IP addresses on a DOCSIS network. Covered here are the following options: Static IP Addresses, MPLS POI, Reverse DNS, Access to DHCP Logs, and Service Selection Gateway/PPPoE. Tracking IP addresses is desirable for Third Party ISPs to track Internet usage (either for abuse programs or for billing), respond to law enforcement requests for information, or for potential VoIP services. Not all of the options will provide real time data to the Third party ISP (this is not a specific requirement of TIF 18).

2. The following is a high level comparison of the proposed solutions:

Solution	Effectiveness	Deployment Issues
Static IP Addresses	Very	• Difficult to operate for the MSO. • Conflicts with premium/business product offerings (service packages). • Increase to call centre volume.
MPLS POI	Depends on the proposed deployment.	• Requires a significant re-architecting of the MSO's IP Backbone. • Has an impact on CMTS CPU load.
Reverse DNS	Good (Not Real Time)	• Increases the Theft of Service risk for the MSO (specifically Modem MAC Cloning). • Decreases customer privacy. • Security/privacy issues can be addressed by using split-view DNS. • There will be data lag (not real time).
DHCP Logs	Good (Not Real Time)	• There can be significant data lag (not real time). • Data volume can be excessive. • Requires DHCP database/log polling.
Service Selection Gateway/PPPoE	Very	• Requires Client Software (or compatible network appliances). • May unfairly penalize the perception of the Third Party ISPs product offerings.

STATIC IP ADDRESSES

3. The use of static IP addresses will solve the IP address tracking problem (since the IP addresses will not change) but there are three basic issues in implementing wide scale static IP addressing: Static IP addresses are difficult to operate due to plant segmentation (topology changes). In some MSOs Static IP addresses are sold as a premium product either for home or business customers, offering it to the basic Third Party ISP subscribers will provide the Third Party ISP an unfair competitive advantage or will undermine the MSO's business product offerings. Finally, static IP addresses will increase call centre volume when subscribers are using non-PC net appliances (e.g. X-Box, Home Routers, etc.). The above noted problems exist regardless how static IP addresses are implemented (either through statically assigned DHCP or through truly static

configurations). The use of IP addresses that do not change will by default provide the Third Party ISP real time IP information.

4. When a MSO segments its plant (spits off a portion of an HFC node—creating a new node—to a new CMTS or new Layer 3 interface to relieve network congestion) it is common (best) practice to provide new IP scopes to the new segments. This allows the new segment to be first activated and tested before live customers are migrated to it. It also prevents the splitting of existing IP scopes into smaller less efficient scopes. When the customers are cut over to the new segment they receive new IP addresses. To deploy static IP addresses the IP addresses must be assigned so that they can (in the future) be moved as a group to a new interface when a node is split (IP addresses must be assigned based on future—predicted node splits so that only a portion of the node has one scope, allowing it to be move as a single entity to a new interface without renumbering the subscribers). Additionally the efficiency of the IP scopes will be greatly diminished, it is common practice for MSOs to re-assign and combine IP scopes (combining smaller scopes added for growth to improve efficiency). This activity requires the renumbering of the subscribers. The number of occurrences (frequency) of both activities cannot be predicted.

5. Most MSOs do offer a limited Static IP product offering, these deployments are limited to a very small number of subscribers and are offered at a significant price premium (for example static IP addresses are sometimes offered to business customers to facilitate IP tunnel type services). The extra cost (and very limited deployments) of these services offsets the additional operational costs. In some cases these services are offered via tunnels or other routing protocols using MSO managed CPE routers to make the static IP address transparent to the HFC network (and to plant segmentation). The CPE router solution does not lend itself to Third Party Internet traffic due to cost and complexity. Migrating Third Party ISP traffic to static IP addresses will undermine this product offering since it will allow subscribers to obtain static IP addresses at a much lower monthly cost; this will give the Third Party ISP an unfair competitive advantage.

6. The connection of equipment behind cable modems is not always static. In many cases subscribers will remove the existing PC and replace it with a new network appliance (for example the temporary connection of a gaming device like an X-Box™, the temporary connection of a work assigned laptop, or the addition of a home router/firewall). In a static IP environment these devices will need to be assigned a new static IP prior to activation. This will require manual intervention by the MSO to assign the new IP address (including a customer call and intervention by higher tier support authorized to assign IP addresses). Under a fully DHCP deployment in most cases the subscriber just needs to reboot the modem to connect the new device (this may differ from MSO to MSO). This is either done by the subscriber without calling the MSO/Third Party ISP or via the direction of the MSO or Third Party ISP call centre; no manual intervention is required by the call centre staff or MSO operational staff.

MPLS POI

7. Deploying MPLS does not—by itself—solve the IP tracking problem. MPLS can be deployed to allow the Third Party ISP to deploy its own DHCP servers

and therefore track IP addresses in real time (this is done via a Layer 2 MPLS VPN). CableLabs does propose such a solution in section: *5.1.2 Multiple ISP L2VPNs; CM-SP-L2VPN-I01-06032, Data-Over-Cable Service Interface Specifications, Business Services over DOCSIS, Layer 2 Virtual Private Networks.*[1] The CableLabs specification was first released in August 2005 and has not been fully adopted by all CMTS manufactures (although most manufactures do provide a similar MPLS product offering). Overall—as outlined below in paragraph 8, and 9—a requirement to deploy a very specific MPLS architecture just to support IP address tracking will increase CMTS CPU load, increase cost through network redesign/new equipment, and will severely limit the flexibility in IP backbone architecture.

8. Deploying MPLS will require a significant backbone network re-architecting for MSOs not currently deploying MPLS. Even those that do will have to redesign the current product offerings to deploy MPLS as suggested by CableLabs. Third Party ISP traffic is currently routed using either MPLS (the MPLS deployments do not fully meet the requirements for IP address tracking) or Policy Based Routing (typically source based). In most cases the current MPLS deployments are completely transparent to the Third Party ISP. This in itself displays how just deploying MPLS is not a solution to the problem, only very specific deployment architectures are. For MSOs that do not currently deploy MPLS additional routing protocols must also be run to support MPLS (e.g. LDP, eBGP). Deploying MPLS is not as simple as turning on the protocol.

9. Depending on the CMTS platform deployed there may be a CPU impact when running MPLS. Some of the larger platforms have specific hardware "registers" to support MPLS tagging but even in these cases the additional routing protocols previously mentioned (paragraph 8) are run in software and are not typically hardware accelerated (they increase CPU load). For smaller (older) CMTS platforms activating MPLS will have a larger impact since both MPLS tagging and the additional required protocols are all run in CPU. The extra CPU load may be enough to force significant CMTS upgrades for smaller MSOs.

REVERSE DNS

10. For reverse DNS to solve the IP tracking problem as defined in *TIF 18* and as outlined in *NTCO0359*[2] the CPE DNS entry must include an identifier, specifically the modem MAC so the Third Party ISP can easily identify the subscriber. Providing the modem MAC in the DNS entry for Internet subscribers (either the MSO's or the Third Party ISP's or both) will cause some security and customer privacy issues. Specifically it will increase theft of service via modem MAC or full modem cloning. It will also allow unauthorized parties to determine the IP addresses behind any subscribers modem and track them (potential privacy issues). Both issues can be solved by properly deploying a split-view DNS. Due to the security risks *Reverse DNS* should not be considered unless a split-view DNS can be implemented. The likely solution would require the Third

[1] http://www.cablemodem.com/downloads/specs/CM-SP-L2VPN-I01-060328.pdf, Page 7

[2] http://www.crtc.gc.ca/cisc/nt/NTCO0359.doc, paragraph 32, page 9

Party ISP to run a secondary DNS server which will be updated periodically from a primary server at the MSO. In this implementation the ISP's data will not be real time.

11. One method for theft of service on a Cable network is to clone the MAC address of a valid subscribers modem. To clone a modem MAC the illegitimate customer requires a list of valid MAC addresses. Adding the MAC address to the PC/CPE DNS entry allows the illegitimate subscribers to get a complete list of all valid MAC addresses in a MSO's network. This can be done by doing reverse DNS lookups for all known public IP space owned by said MSO or Third Party ISP (this is easily obtained). Mandating this entry without implementing split-view DNS will greatly increase the MSO risk for theft of service.

12. When adding the MAC address to a PC DNS entry a hacker or other outside party can use the DNS entries, with a reverse lookup, to determine all the CPE MAC addresses and IP addresses behind a specific customers modem. They can also use this method to track said devices. Overall this provides a potential risk to subscriber privacy. Once again a split-view DNS deployment will solve this issue.

13. By deploying split-view DNS the MSO and TPIA Partner(s) can have access to a CPE DNS entry that contains the modem MAC address. The DNS entry provided to the public Internet will not have the modem MAC address present. This will allow the Third Party ISP to track its subscribers IP addresses based on the modem MAC address while not allowing the public Internet access to this information. This solves the above noted security concerns and provides sufficient information for the ISP to track the subscribers. It should be noted that some ISPs already deploy such a system for VoIP but in this case it is used to hide the subscriber's phone number from the public internet yet make it available to the back office via the DNS entry. There may be a cost impact for this solution since not all provisioning systems will allow a split-view DNS as they are deployed; this will need to be commented on by the MSOs.

14. This solution will also have some data lag; the amount will depend on how often the Third Party's secondary DNS server is updated. Real time data is not a specific requirement of *TIF 18* but it may be required in the future (e.g. instantaneous VoIP ATA IP address tracking/verification for E911). A practical solution would be updates every 5 to 15 minutes.

DHCP LOGS

15. For the Third Party ISP to use the MSO's DHCP Logs to track subscriber IP addresses the Third Party ISP will likely require one of the following: access to the MSO's DHCP server's database, DHCP log access to perform "Query by MAC address" via DHCP Lease Query (if supported by the DHCP system), or they will require the MSO to provide periodic DHCP data dumps to the Third Party ISP (performed by the MSO using "Query by MAC address" or any other method). DHCP Logs will be effective for historically tracking IP addresses; it does not provide real time tracking unless real time querying is allowed (not recommended). There could be some deployment issues with this solution, mostly due to the overall server load and the long term scalability of this solution. The most likely solution would be to give a periodic dump to the Third Party

ISP(s) since it is good practice to limit the number (and frequency) of systems polling or querying the DHCP system (this is due to scaling and security concerns).

16. By dumping the appropriate DHCP information periodically to the Third Party ISP the historical IP addresses of the Third Party's subscribers can be determined. This data will not be real time and may not fully meet some of the Third Party ISP's future requirements (e.g. instantaneous VoIP ATA IP address tracking/verification for E911). It will meet the requirement of historically tracking IP addresses for the purpose of lawful access to subscriber information or usage billing. The overall time delay will depend on how often the data dump is provided to the Third Party ISP (or how often the DHCP system is polled or queried). The number of times the data is provided to the Third Party ISP raises the concern of system load for this type of solution and the overall manageability of the data dumps by the Third party ISP.

17. For this solution to approach the capabilities of the Reverse DNS solution the appropriate DHCP information will need to be provided to the Third Party ISP every 5 to 15 minutes. Although this is possible it may not be practical for large MSO's to provide the data this often (due to the required frequent polling and size of the DHCP database or logs). When future large scale deployments are considered the overall exchange of information load may not be practical for either the ISP or MSO. A more practical solution would be for the MSO to provide the appropriate DHCP information four times a day; this will be more manageable for both the MSO and the Third Party ISP(s). This would mean that the ISP's CPE IP address information could be as much as 6 hours out of date.

SERVICE SELECTION GATEWAY/PPPoE

18. For the purpose of this response Service Selection Gateway (SSG) and PPPoE have been grouped together since they can be interrelated (depending on the deployment) and they both have similar limitations. Both solutions will allow the Third Party ISP to actively monitor/control the subscribers IP addresses. The main limitation to both of these technologies is the requirement for the Third Party's subscribers to use CPE based client software (or a compatible network appliance) and to log in for each session. Additionally this solution is not compatible with all network appliances and may therefore penalize the Third Party ISP, limiting the products that can be deployed by its subscribers or the technologies the ISP can deploy. There are other limitations such as additional packet overhead, smaller MTU size, and traffic transparency.

19. The requirement for client based software and/or compatible devices are the largest drawback of these technologies. For Third Party subscribers with just a PC connected to a cable modem, the PC will require client software and may be required to logon to the service (depending on the client and network appliances a Radius solution could be implemented in place of a login). This will differentiate the Third Party's service from the MSO's incumbent Cable Internet service (possibly negatively) since the Third Party ISP's service will no longer be perceived as "always on" (it will be similar to DSL based services). The Third Party ISP will also have to provide technical support for the additional client based software (adding extra cost). The extra effort in supporting the client

software will depend on the Third Party ISP's experience with DSL. This limitation will also impact the ability of the Third Party's subscribers to switch between CPE devices.

20. Due to the client based nature not all network appliances will be supported. There may be compatibility issues with gaming devices, some home gateways, and some ATAs (used for VoIP).

21. The extra overhead, potentially smaller MTU size, and traffic transparency may negatively impact the TPIA subscribers. The extra overhead associated with these technologies will increase bandwidth requirements. In the case of PPPoE the maximum MTU size will be somewhat smaller than a standard Ethernet packet; this can have a performance impact for the TPIA subscriber. Finally, the transparency of the traffic will be jeopardized, making it more difficult for the MSO to provide similar QoS profiles for the TPIA customers as it does its own Internet subscribers (based on traffic type).

CONCLUSIONS

22. Each solution has its own limitations; in some cases these limitations will unfairly penalize the MSO or Third Party ISP. Both Reverse DNS (with split DNS) and Third Party Access to DHCP Logs solve the requirement for IP address tracking but neither provides real time tracking for the Third Party ISP (which is not a specific requirement of TIF 18 but is a limitation none the less). The deployment of a MPLS Layer 2 VPN will solve the issue but it will force the MSO to deploy a very specific network (this will limit IP backbone flexibility; it may have a significant deployment cost impact and is an excessive solution if deployed solely for the purpose of tacking IP addresses). Static IP addresses increase MSO operational complexity and will conflict with current MSO product offerings. SSG/PPPoE will differentiate the Third Party ISP's service compared to the MSO's service due mostly to the required CPE client/network appliance support.