Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 15, 2014

G. Chen
Z. Cao
China Mobile
M. Boucadair
France Telecom
A. Vizdal
Deutsche Telekom AG
L. Thiebaut
Alcatel-Lucent

July 14, 2013

Analysis of Port Control Protocol in Mobile Network
draft-chen-pcp-mobile-deployment-04

Abstract

This memo provides a motivation description for the Port Control Protocol (PCP) deployment in a 3GPP mobile network environment. The document focuses on a mobile network specific issues (e.g. cell phone battery power consumption, keep-alive traffic reduction), PCP applicability to these issues is further studied and analyzed.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The Port Control Protocol[RFC6887] allows an IPv6 or IPv4 host to control how incoming IPv6 or IPv4 packets are translated and forwarded by a network address translator (NAT) or simple firewall(FW), and also allows a host to optimize its outgoing NAT keepalive messages. A 3rd Generation Partnership Project (3GPP) network can benefit from the use of the PCP service. Traffic in a mobile network is becoming a complex mix of various protocols, different applications and user behaviors. Mobile networks are currently facing several issues such as a frequent keepalive message, terminal battery consumption and etc. In order to mitigate these issues, PCP could be used to improve terminal behavior by managing how incoming packets are forwarded by upstream devices such as NAT64, NAT44 translators and firewall devices.

It should be noticed that mobile networks have particular characteristics and therefore, there are several factors that should

be investigated before implementing PCP in a mobile context. Without the particular considerations , PCP may not provide desirable outcomes. Some default behaviors may even cause negative impacts or system failures in a mobile environment. Considering very particular environment of mobile networks , it's needed to have a document describing specific concerns from mobile network side. That would also encourage PCP support in mobile network as well.

This memo covers PCP-related considerations in mobile networks. The intension of publishing this memo is to elaborate major issues during the deployment and share the thoughts for potential usages in mobile networks. Such considerations would provide a pointer to parties interested (e.g. mobile operators) to be included in their UE profile requirements. Some adaptation of PCP protocol might be derived from this document. Such a work would be documented in separated memo(s).

2. Benefits of Introducing PCP in Mobile Networks

2.1. Restoring Internet Reachability

Many Mobile networks are making use of a Firewall to protect their customers from an unwanted Internet originated traffic. The firewall is usually configured to reject all unknown inbound connections and only permit inbound traffic that belongs to a connection initiated from the Firewall or NAT/PAT device. The behavior is described as Category I in [I-D.ietf-opsawg-firewalls].There are applications that can be running on the mobile device that require to be reachable from the Internet or there could be services running behind the terminal that require reachability from the Internet. For example, mobile phones should be able to reachable for instant message or online game. PCP enabled applications / devices could request a port from the Firewall to ensure Internet reachability, and thus would lighten the traffic flow of keep-alive by reducing the number of sending packets. This would result in resource savings on the Firewall node whilst still keeping the customer protected from the unwanted traffic.

2.2. Radio Resource Optimization

3GPP network use different radio channels to transmit control messages(e.g. signaling) and data packages(e.g. voice packages or data flows). Always-on applications, e.g. IM(Instant Message), VoIP or P2P based applications always generate a fair amount of keepalive messages periodically. It's observed that a number of trivial keepalive messages may occupy the data channel. For example, 16% of traffic caused by instant signaling message would consume 50%~70% radio resource in some area. It likely causes the air congestion with voice calls and service data transmission. PCP could help to

reduce the frequency of periodic messages aimed at refreshing a NAT/FW binding by indicating to the mobile device the Life time of a binding.

2.3. Energy Saving

Devices with low battery resources exist widely in mobile environments, such as mobile terminals, advanced sensors, etc. mobile terminals often go to "sleep" (IDLE) mode to extend battery life and save air resources. Host initiated message needs to "wake-up" mobile terminals by changing the state to CONNECTED. That would cause more energy on such terminals. Testing reports show that energy consumption is dramatically reduced with prolonged sending interval of signaling messages [VTC2007_Energy_Consumption].

3. Overviews of PCP Deployment in Mobile Network

The Figure 1 shows the architecture of a mobile network. Radio access network would provide wireless connectivity to the MN. Packets are transmitted through Packet Switch(PS) domain heading to MGW. MGW bear the responsibilities of address allocation, routing and transfer. The connection between MN and MGW normally is a point-to- point link, on which MGW is the default router for MN. NAT/Firewall could either be integrated with MGW or deployed behind MGW as standalone. The traffic is finally destined to application servers, which manage subscriber service.

```
      MN                                                        Internet
       |               +---------------+                     +----------------+
     +-+     +-----+   |            +--|--+     +-------+    |  +----------+  |
     | | /|/ | RAN |---| PS Network | MGW |---- |NAT/FW |----|  |APP Server|  |
     +-+     +-----+   |            +--|--+     +-------+    |  +----------+  |
                       +---------------+                     +----------------+
     MN:  Mobile Nodes
     RAN: Radio Access Network
     PS:  Packet Switch
     MGW:Mobile GateWay
     NAT/FW: Network Address Translator or Firewall
```

Figure 1: Mobile Networks Scenario

A PCP client could be located on MN to control the outbound and inbound traffic on PCP servers. The PCP server is hosted by the NAT/FW respectively. Corresponding to the various behaviors of PCP client, MN would perform PCP operation using MAP, PEER or ANNOUNCE opcodes. A specific application programming interface may be provided to applications. More discussions and recommendations are presented in following sub-sections.

4. PCP Server Discovery

A straightforward solution seems that MN assume their default router as the PCP Server. However, NAT/FW normally is deployed in a different node than the MGW. Thus there is the need to ensure that MN get information allowing them to discover a PCP server.

[I-D.ietf-pcp-dhcp] specified name options in DHCPv4 and DHCPv6 to discover PCP server. It's expected the same mechanism could be used in mobile network. 3GPP network allocates IP address and respective parameter during the PDP (Packet Data Protocol)/PDN(Packet Data Network) context activation phase (PDP and PDN represent terminology in 3G and LTE network respectively). On the UE, a PDP/PDN context has same meaning which is equivalent to a network interface.

It should be noted that the Stateful DHCPv6-based address configuration[RFC3315]is not supported by 3GPP specifications. 3GPP adopts IPv6 Stateless Address Auto-configuration (SLAAC) [RFC4861]to allocate IPv6 address. The UE uses stateless DHCPv6[RFC3736] for additional parameter configuration. The MGW acts as the DHCPv6 server. PCP servers discovery could leverage current process to perform the functionalities. The M-bit is set to zero and the O-bit may be set to one in the Router Advertisement (RA) sent to the UE. To carry out PCP sever discovery, a MN should thus send an Information-request message that includes an Option Request Option (ORO) requesting the DHCPv6 PCP Server Name option.

Regarding the IPv4 bearer, MN generally indicates that it prefers to obtain an IPv4 address as part of the PDP context activation procedure. In such a case, the MN relies on the network to provide IPv4 parameters as part of the PDP context activation/ PDN connection set-up procedure. The MN may nevertheless indicate that it prefers to obtain the IPv4 address and configuration parameter after the PDP Context activation by DHCPv4, but it is not available on a wide scale[RFC6459]. MN usually receive those configurations in PCO(Protocol Configuration Options) . PCP server name options in DHCPv4 would not help the PCP servers discovery in that case.

A specific method in 3GPP is to extend PCO [TS24.008]information element to transfer a request of PCP server name. However, additional specification efforts are required in 3GPP to make that happen.

[I-D.cheshire-pcp-anycast]and [I-D.kiesel-pcp-ip-based-srv-disc]propose anycast-based solutions to discover the closest PCP server on the data path. It may be worth to consider the case when a subscriber roams to different areas, where anycast configurations may be unavailable or operators use other

provisioning method, for example [I-D.ietf-pcp-dhcp]. Asymmetric routing should also be considered in the anycast-based solution. Otherwise, the traffic would likely loses the mapping information for the inbound traffic.

5. MN and multi-homing

As a MN may activate multiple PDP context / PDN connection, it may be multi-homed (the UE receives at least an IP address / an IPv6 prefix per PDN connection). Different MGWs are likely to be associated with each of these PDP context / PDN connection and may thus advertise different PCP servers (using the mechanism described in the previous section). In that case, a MN has to be able to manage multiple PCP servers and to associate an IP flow with the PCP server corresponding to the PDP context / PDN connection used to carry that IP flow.

6. Retransmission Consideration

Mobile devices are usually powered with limited battery . Users would like to use such MN for several days without charging, even several weeks in sensor case. Many applications do not send or receive traffic constantly; instead, the network interface is idle most of the time. That could help to save energy unless there is data leading the link to be activated. Such state changes is based on network-specific timer values corresponding to a number of Radio Resource Control (RRC) states(see more at Section 8.2.2 3GPP[TS23.060]. In order to maximize battery life, it's desirable that all activities on battery-powered devices needs to be coordinated and synchronized. It's not specific to PCP. Whereas , those concerns also can be applied to PCP retransmission behavior.

PCP designed retransmission mechanisms on the client for reliable delivery of PCP request. If a PCP client fails to receive an expected response from a server, the client must retransmit its message. The retransmission method may cause unnecessary power consumption when a subscriber roams to a network, in which PCP is not deployed. Several timers are specified to control the retransmission behavior. Therefore, an appropriate implementation and configuration are desirable to help to alleviate the concern. For example, the time transiting to idle is normally less than default Maximum Retransmission Time (MRT), i.e. 1024 seconds. With "no maximum" setting of Maximum Retransmission Duration (MRD), it would cause devices activating their uplink radio in order to retransmit the request messages. Furthermore, the state transition and the transmission take some times, which causes significant power consumption. The MRD should be configured with an optimal time which in line with activated state duration on the device.

The power consumption problem is made complicated if several PCP clients residing on a MN. Several clients are potentially sending requests at random times and by so doing causing MN uplink radio into a significantly power consuming state for unnecessarily often. It's necessary to perform a synchronization process for tidy up several PCP clients retransmission. A time-line observer maybe required to control different PCP clients resending requests in an optimal transmission window. If the uplink radio of MN is active at the time of sending retransmission from several clients, a proper MRD described as above should be set in a client. If the uplink radio of MN is in idle mode, the time-line observer should hold Initial Retransmission Time(IRT) for while to synchronize different retransmitted PCP requests into same optimal transmission window.

7. Unsolicited Messages Delivery

When the states on NAT/FW have been changed like reboot or changed configuration, PCP servers can send unsolicited messages (e.g. ANNOUNCE messages or unicast PCP MAP or PEER responses) to clients informing them of the new state of their mappings. This aims at achieving rapid detection of PCP failure, rapid PCP recovery or PCP mapping update. When those messages are delivered in a mobile environment, it should be noted multicast delivery may not be available in 3GPP network. PCP servers would use unicast delivery. More considerations are listed as the below.

- This requires PCP servers to retain knowledge of the IP address(es) and port(s) of their clients, for example using redundancy design based on hot-standby, even though they have rebooted

- Care should be taken not to generate floods of unicast messages, e.g. to multiple thousands of MN that were served by a PCP server that has rebooted. Such flood may have impacts on Mobile Networks as it may imply the simultaneous generation of Paging process(see more at Section 8.2.4 3GPP[TS23.060]) for very big numbers of MN.

- Paging function is optionally supported at some particular nodes, e.g. Traffic Offload Function (TOF) in Selected IP Traffic Offload architecture (more discussions on this issues is described in Section 7). The delivery of unsolicited messages would fail in this case.

8. SIPTO Architecture

Since Release 10, 3GPP starts supporting of Selected IP Traffic Offload (SIPTO) function defined in [TS23.060], [TS23.401].The SIPTO function allows an operator to offload certain types of traffic at a network node close to the UE's point of attachment to the access network. It can be achieved by selecting a set of MGWs that is geographically/topologically close to a UE's point of attachment. Two variants of solutions has specified in 3GPP.

The mainstream standard deployment relies on selecting a MGW that is geographically/ topologically close to a UE's point of attachment. This deployment may apply to both 3G and LTE. The MN may sometimes be requested to re-activate its PDP context / PDN connection, in which case it is allocated a new MGW and thus a new IP address and a new PCP server. In this case, host renumbering is inevitable. Some considerations have been described as Address Change Events at Section11.5 of [RFC6887]. The deletions of the mapping information on the old MGW is necessary in order to avoid traffic sending to the old IP address. In a mobile device context, PCP client may take the NAS(Non-Access Stratum) layer message (e.g. "reactivation request" or "detach request" message) as a notification to delete the old mapping information before the subscriber moved to new MGW. Afterwards, PCP clients install new mappings for its new IP address.

As an implementation option dedicated to 3G networks, it is also possible to carry out Selected IP Traffic Offload in a TOF(Traffic Offload Function) entity [TS23.060]located at the interface of the Radio Access Network, i.e. in the path between the radio stations and the Mobile Gateway. The TOF decides on which traffic to offload and enforces NAT for that traffic. The deployment of a TOF is totally transparent for user's equipments that even cannot know which traffic is subject to TOF (NATed at the TOF) and which traffic is processed by the MGW. The PCP server advertised by the MGW does not take into account the NAT carried out by the TOF function. Therefore, PCP client doesn't know which PCP servers should be selected to send the request. [I-D.rpcw-pcp-pmipv6-serv-discovery]provides a solution in the similar architecture, in which a PCP proxy with advanced functions[I-D.ietf-pcp-proxy] is required on the offloading point to dispatch requests to a right PCP server. Additional consideration will be given for determining the each traffic flow, since TOF inspects the NAS and RANAP(Radio Access Network Application Part) messages to build the local UE context and local session context. The traffic flow can't be identified with 5 tuples. The offloaded IP flow is indicated with Radio Access Bearer Identifier (RAB-ID). PCP proxy must understand RAB-ID and map the identifier with each IP flow.

9. Authentication Consideration

The general authentication requirements have been analyzed in [I-D.reddy-pcp-auth-req]. In mobile networks, it is desirable to reuse the existing credentials on the UE for the pcp authentication between involved entities. This way makes the deployment of authentication easiler.

The [I-D.ietf-pcp-authentication] has provided solutions for PCP authentication, in which an EAP option is included in the PCP requests from the devices. In the EAP framework, the EAP authentication server could be the co-located with the PCP server or separated and located on a third-party entity. If the EAP authentication server is placed on the AAA/Radius server, there is a need of an interface between the PCP server and AAA. But per our investigation of 3GPP networks, most exisiting NAT devices do not have such an interface with AAA. So in practical deployment, this could be taken into consideration.

10. Conclusion

PCP mechanism could be potentially adopted in different usage contexts. The deployment in mobile network described applicability analysis, which could give mobile operators a explicit recommendation for PCP implementation. Operators would benefit from such particular considerations. The memo would take the role to document such considerations for PCP deployment in mobile network.

11. Security Considerations

TBD

12. IANA Considerations

This document makes no request of IANA.

13. Acknowledgements

The authors would like to thank Dan Wing, Stuart Cheshire, Ping Lin and Tao Sun for their discussion and comments.

Many thanks to Reinaldo Penno and Tirumaleswar Reddy for their detailed reviews.

14. References

14.1. Normative References

[I-D.ietf-pcp-authentication]
Wasserman, M., Hartman, S., and D. Zhang, "Port Control Protocol (PCP) Authentication Mechanism", draft-ietf-pcp-authentication-01 (work in progress), October 2012.

[I-D.ietf-pcp-dhcp]
Boucadair, M., Penno, R., and D. Wing, "DHCP Options for the Port Control Protocol (PCP)", draft-ietf-pcp-dhcp-07 (work in progress), March 2013.

[I-D.ietf-pcp-proxy]
Boucadair, M., Penno, R., and D. Wing, "Port Control Protocol (PCP) Proxy Function", draft-ietf-pcp-proxy-03 (work in progress), June 2013.

[I-D.reddy-pcp-auth-req]
Reddy, T., Patil, P., Wing, D., and R. Penno, "PCP Authentication Requirements", draft-reddy-pcp-auth-req-04 (work in progress), July 2013.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.

[RFC3736] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC6887] Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", RFC 6887, April 2013.

[TS23.060]
, "General Packet Radio Service (GPRS); Service description; Stage 2", June 2012.

[TS23.401]
, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", June 2012.

14.2. Informative References

[I-D.cheshire-pcp-anycast]
Cheshire, S., "PCP Anycast Address", draft-cheshire-pcp-anycast-01 (work in progress), March 2013.

[I-D.ietf-opsawg-firewalls]
Baker, F. and P. Hoffman, "On Firewalls in Internet Security", draft-ietf-opsawg-firewalls-01 (work in progress), October 2012.

[I-D.kiesel-pcp-ip-based-srv-disc]
Kiesel, S. and R. Penno, "PCP Server Discovery based on well-known IP Address", draft-kiesel-pcp-ip-based-srv-disc-00 (work in progress), February 2013.

[I-D.rpcw-pcp-pmipv6-serv-discovery]
Reddy, T., Patil, P., Chandrasekaran, R., and D. Wing, "PCP Server Discovery with IPv4 traffic offload for Proxy Mobile IPv6", draft-rpcw-pcp-pmipv6-serv-discovery-02 (work in progress), February 2013.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC6459] Korhonen, J., Soininen, J., Patil, B., Savolainen, T., Bajko, G., and K. Iisakkila, "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)", RFC 6459, January 2012.

[TS24.008]
, "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3", 9.11.0 3GPP TS 24.008, June 2012.

[TS33.220]
, "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)", 10.1.0 3GPP TS 33.220, March 2012.

[VTC2007_Energy_Consumption]
, "Energy Consumption of Always-On Applications in WCDMA Networks", 2007.

Authors' Addresses

Gang Chen
China Mobile
No.32 Xuanwumen West Street
Xicheng District
Beijing 100053
China

Email: phdgang@gmail.com

Zhen Cao
China Mobile
No.32 Xuanwumen West Street
Xicheng District
Beijing 100053
China

Email: caozhen@chinamobile.com

Mohamed Boucadair
France Telecom
No.32 Xuanwumen West Street
Rennes,
35000
France

Email: mohamed.boucadair@orange.com

Vizdal Ales
Deutsche Telekom AG
Tomickova 2144/1
Prague 4, 149 00
Czech Republic

Email: ales.vizdal@t-mobile.cz

Laurent Thiebaut
Alcatel-Lucent

Email: laurent.thiebaut@alcatel-lucent.com