PPPoE - Point to point over Ethernet

Michal Krumnikl, kru106, 20.1.2006

Úvod

Praxe klade na současné síťové technologie řadu navzájem protikladných požadavků. Často požadujeme připojení více klientů ke společnému síťovému médiu, a zároveň vyžadujeme některé vlastnosti typické pro vytáčené linky. Jedná se například o účtování doby připojení, množství přenesených dat a lepší kontrolu nad připojenými uživateli.

PPPoE (point-to-point over ethernet) je síťový protokol, který zapouzdřuje PPP rámce do ethernetových rámců. Protokol byl vyvinut ve spolupráci organizací UUNET, Redback Networks, and RouterWare a je specifikován v RFC 2516.

PPPoE umožňuje vytvářet spoje typu bod-bod (*peer-to-peer*) na přepínaných ethernetových sítích. Klienti jsou připojeni k přístupovému bodu (*Access concentrator*), každý klient má své vlastní PPP spojení a jeví se jako nezávislý adaptér (*interface*). Kontrola přístupu, účtování, přístup ke službám je pak realizován na základě platného přihlášení uživatele, a ne na základě jeho IP adresy. Vytvořené spojení má ovšem nižší MTU než standardní ethernet (ethernet má běžně MTU 1500 bajtů, enkapsulace PPPoE má hlavičku délky 8 bajtů, MTU PPPoE rozhraní má tedy 1492 bajtů), což může výjimečně způsobovat problémy se špatně nakonfigurovanými firewally[1] . ISP používají PPPoE pro ověřování uživatelů připojovaných přes xDSL nebo kabelový modem.

Pro vytvoření PPP spojení (*PPP session*) musí klient znát MAC adresu vzdálené strany a jednoznačnou identifikaci spojení, tyto údaje získá během vyhledávací fáze (*discovery stage*).

[1] Při zahájení TCP mohou volitelně obě strany specifikovat maximální délku segmentu (MSS - Maximum Segment Size). V TCP spojení je pak datový tok rozdělen na segmenty, přičemž MSS specifikuje maximální délku segmentu, který daná strana přijme. Standardně se MSS volí jako rozdíl MTU odchozího rozhraní a délky TCP a IP hlavičky (40 bajtů), tedy 1460 bajtů pro ethernetové rozhraní.

V implementacích TCP je snaha o zamezení fragmentace paketů, čehož se dosahuje vhodnou volbou MSS. Na trase paketů se ale mohou vyskytovat spojení s nižším MTU, na kterých by docházelo k fragmentaci. Tento problém se řeší pomocí “path MTU discovery”, kdy je v IP paketech nastaven příznak nefragmentovat (DF - don't fragment). Síťové směrovače, které by musely paket fragmentovat jej zahodí a odešlou ICMP zprávu “Fragmentation-Required”.

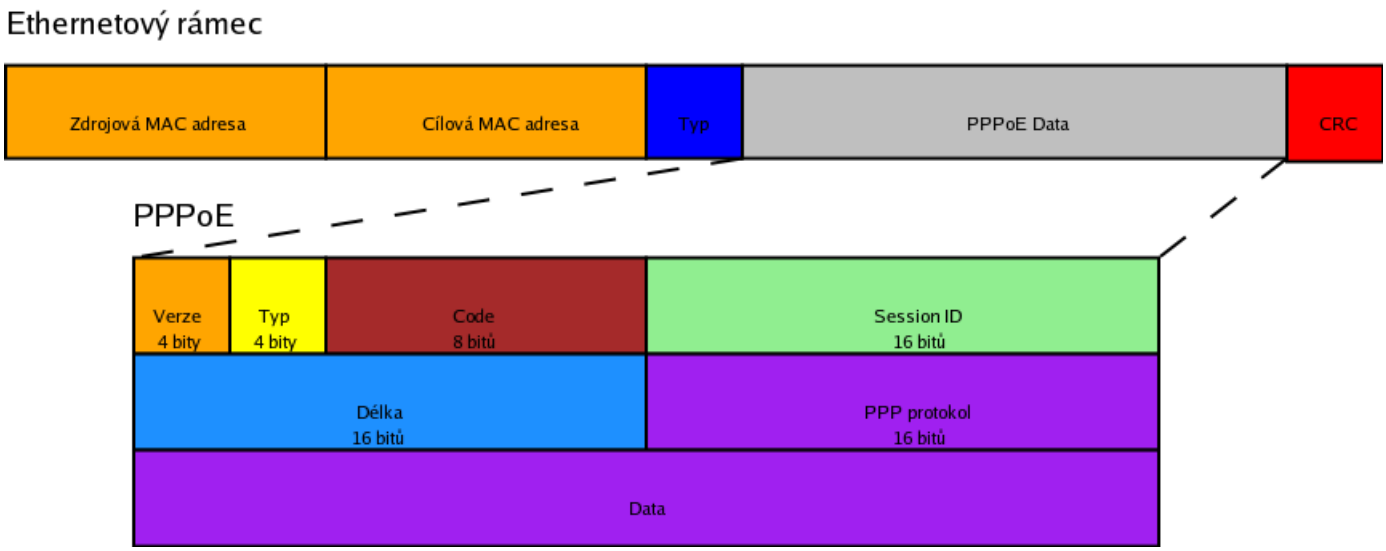
Nyní předpokládejme, že na trase paketů je firewall, který zahazuje veškeré ICMP zprávy. Klient, který je připojen k internetu pomocí PPPoE brány, otevře TCP spojení na webový server. Protože klient je připojen k ethernetu, navrhne MSS 1460 bajtů. Server, který se také naléza na ethernetu, navrhne MSS délky také 1460 bajtů. Klient pošle požadavek na server. Požadavky mají většinou krátkou délku a proto dojdou k serveru v pořádku. Server odpoví několika TCP segmenty, které mají délku MSS. Tyto segmenty dojdou až k PPPoE rozhraní, kde budou zahozeny (předpokládejme, že mají nastavený příznak DF). Vygenerované ICMP zprávy jsou ovšem zahozeny firewallem. Server se tedy nedoví, že pakety byly zahozeny a ke klientu nedorazí požadované segmenty.

PPPoE protokol

Protokol PPPoE má dvě fáze - vyhledávání přístupového bodu (*Discovery stage*) a udržování PPP spojení (*PPP session*). Klient požadující spojení musí získat MAC adresu přístupového bodu a identifikaci spojení (*SESSION_ID*). Tyto informace získá během první fáze. Zatímco PPP spojení definuje vztah pouze mezi dvěmi stanicemi, v průběhu vyhledávácí fáze může dojít ke komunikaci klienta s více přístupovými body (na žádost PADI přijde více PADO odpovědí).

V průběhu první fáze hledá klient svůj přístupový bod. V závislosti na topologii sítě může klient objevit jeden nebo více přístupových bodů, z kterých si vybere jeden, se kterým vytvoří spojení. Po úspěšném nalezení přístupového bodu se zahajuje druhá fáze - vytvoření a udržování PPP spojení.

Obsah PPPoE paketů



Typ (ethernetový rámec)
0x8863 (Discovery Stage) - vyhledávání přístupového bodu všesměrovým vysíláním, vytváření a rušení PPPoE spojení
0x8864 (PPP Session Stage) - přenos PPP rámců

Verze - vždy hodnota 0x1
Typ - vždy hodnota 0x1

Code - Používá se v průběhu vyhledávácí fáze PPPoE, určuje typ rámce této fáze. Během PPP fáze má hodnotu vždy 0x00.

0x00 - Session Data
PADO (PPPoE Active Discovery Offer)
PADI (PPPoE Active Discovery Initiation)
PADR (PPPoE Active Discovery Request)
PADS (PPPoE Active Discovery Session-confirmation)
PADT (PPPoE Active Discovery Termination)

Session ID - identifikuje PPP spojení

Délka - velikost zapouzdřeného rámce (nezahrnuje tedy délku hlaviček Ethernetu a PPPoE)

PPP Protokol - hodnota definuje typ zapouzdřeného datagram (na obr. pole data). Struktura této položky odpovídá ISO 3309.

0x0021 – IP (Internet Protocol)
0x80fd – CCP (Compression Control Protocol)
0x8021 – IPCP (IP Control Protocol)
0xc021 – LCP (Link Control Protocol)
0xc223 – CHAP (Challenge Handshake Authentication Protocol)

Data - obsahuje datagram protokolu specifikovaného v položce PPP protokol.

PPPoE pakety mohou obsahovat jeden nebo více příznaků (*tag*). Příznaky se připojují za hlavičku PPPoE paketu. Příznaky mají definovaný tento formát:

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
TAG type	TAG length
TAG value	

Některé typy příznaků budou popsány u paketů discovery fáze, kterých se přímo týkají.
Vyskytuje-li se v paketu příznak, který není příjemci znám, musí být příjemcem ignorován, čímž je zaručena kompatibilita se staršími verzemi PPPoE.

Discovery stage (hledání přístupového bodu)

Fázi Discovery stage můžeme rozdělit na 4 kroky, po jejichž úspěšném provedení znají oba účastnící spojení (klient a přístupový bod) veškeré informace, které jsou nutné pro vytvoření PPPoE spojení - SESSION_ID a vzájemné MAC adresy.

Klient nejdříve vysílá všesměrově *(broadcast)* úvodní pakety *(Initiation packet)*; jeden nebo více přístupových bodů *(Access concentrators)* mu odpoví nabídkou připojení *(Offer packet)*. Z těchto přístupových bodů si klient vybere jeden a dále s ním již komunikuje přímo *(unicast)*. Klient pošle žádost o zřízení spojení *(Session request packet)* a přístupový bod mu potvrdí připojení *(Confirmation packet)*. Jakmile klient přijme potvrzení *(Confirmation packet)*, může přejít do druhé fáze - PPP spojení.

Všechny rámce této fáze (Discovery) mají nastavenou položku **ETHER_TYPE** na hodnotu **0x8863**.

PPPoE Active Discovery Initiation (PADI) packet

PADI paket je první paket, který vysílá klient požadující připojení. Protože klient nezná MAC adresu přístupového bodu, nastaví cílovou MAC adresou na všesměrové vysílání (broadcast).
Položka **CODE** je nastavena na **0x09** a **SESSION_ID** musí mít hodnotu **0x0000**.

PADI paket musí obsahovat právě jeden příznak (*tag*) typu **Service-name**, ve kterém udává službu kterou klient požaduje. Celková délka paketu nesmí přesáhnout 1484 B.
Příznak **Host-uniq** jednoznačně přiřazuje odpovědi daného přístupového bodu (PADO, PADS) k jednotlivým požadavkům klienta (PADI, PADR).

Příklad

```
No.     Time        Source                Destination           Protocol Info
      1 0.000000    XnetTech_18:85:01     Broadcast             PPPoED   Active Discovery Initiation (PADI)

Ethernet II, Src: XnetTech_18:85:01 (00:05:1c:18:85:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: XnetTech_18:85:01 (00:05:1c:18:85:01)
    Type: PPPoE Discovery (0x8863)
PPP-over-Ethernet Discovery
    Version: 1
    Type: 1
    Code: Active Discovery Initiation (PADI)
    Session ID: 0000
    Payload Length: 22
PPPoE Tags
    Tag: Service-Name
      String Data: MojeSluzba
    Tag: Host-Uniq
      Binary Data: (4 bytes)
```

PPPoE Active Discovery Offer (PADO) packet

Přístupový bod odpovídá na PADI jemu určené (při shodě příznaku **Service-name**) PADO paketem. Cílová MAC adresa PADO paketu je zdrojovou MAC adresou odesílatele PADI paketu.
Položka **CODE** má hodnotu **0x07** a **SESSION_ID** má hodnotu **0x0000**.

PADO paket musí obsahovat příznak **AC-Name**, tedy název přístupového bodu a další příznaky odpovídající dalším službám přístupového bodu. Pokud přístupový bod nepodporuje službu žádanou v PADI, nesmí odpovědět PADO paketem.

Příznak **Host-uniq** odpovídá hodnotě zaslané v požadavku klienta (PADI, PADR); hodnota nesmí být změněna.
Volitelný příznak **AC-Cookie** se používá pro zamezení DoS útokům. Klient, který obdrží tento příznak jej nezměněn pošle zpět v PADR paketu.

Příklad

```
No.     Time        Source                Destination           Protocol Info
      2 0.000231    Intel_05:6e:7c        XnetTech_18:85:01     PPPoED   Active Discovery Offer (PADO)

Ethernet II, Src: Intel_05:6e:7c (00:02:b3:05:6e:7c), Dst: XnetTech_18:85:01 (00:05:1c:18:85:01)
    Destination: XnetTech_18:85:01 (00:05:1c:18:85:01)
    Source: Intel_05:6e:7c (00:02:b3:05:6e:7c)
    Type: PPPoE Discovery (0x8863)
PPP-over-Ethernet Discovery
    Version: 1
    Type: 1
    Code: Active Discovery Offer (PADO)
    Session ID: 0000
    Payload Length: 55
PPPoE Tags
    Tag: AC-Name
      String Data: MujAC
    Tag: Service-Name
      String Data: MojeSluzba
    Tag: AC-Cookie
      Binary Data: (20 bytes)
    Tag: Host-Uniq
      Binary Data: (4 bytes)
```

PPPoE Active Discovery Request (PADR) packet

Protože byl paket PADI poslán všesměrově *(broadcast)*, může klient obdržet více než jednu odpověd PADO. Klient si vybere z PADO paketu jeden na který odpoví, např. podle AC-Name nebo nabízených služeb. Klient pošle PADR paket přístupovému bodu, cílová MAC adresa odpovídá MAC adrese přístupového bodu z PADO paketu.

Položka **CODE** je nastavená na **0x19** a **SESSION_ID** musí být nastavená na **0x0000**.
PADR paket musí obsahovat příznak **Service-name**, která odpovídá službě, kterou klient žádá.

Příklad

```
No.     Time        Source                Destination           Protocol Info
      3 0.002084    XnetTech_18:85:01     Intel_05:6e:7c        PPPoED   Active Discovery Request (PADR)

Ethernet II, Src: XnetTech_18:85:01 (00:05:1c:18:85:01), Dst: Intel_05:6e:7c (00:02:b3:05:6e:7c)
    Destination: Intel_05:6e:7c (00:02:b3:05:6e:7c)
    Source: XnetTech_18:85:01 (00:05:1c:18:85:01)
    Type: PPPoE Discovery (0x8863)
PPP-over-Ethernet Discovery
    Version: 1
    Type: 1
    Code: Active Discovery Request (PADR)
    Session ID: 0000
    Payload Length: 46
PPPoE Tags
    Tag: Service-Name
      String Data: MojeSluzba
    Tag: Host-Uniq
      Binary Data: (4 bytes)
    Tag: AC-Cookie
      Binary Data: (20 bytes)
```

The PPPoE Active Discovery Session-confirmation (PADS) packet

Jakmile přijme přístupový bod PADR paket, tak dojde k rezervaci prostředků pro sestavení PPP spojení. Vygeneruje unikátní SESSION_ID pro dané PPPoE přípojení a odpoví klientovi PADS paketem. Cílová MAC adresu paketu je MAC adresa klienta, který odeslal PADR.

Položka **CODE** má hodnotu **0x65** a **SESSION_ID** obsahuje unikátní hodnotu vygenerovanou pro dané spojení.

PADS paket musí obsahovat příznak **Service-name**, ve kterém je specifikováno, jakou službu přístupový bod akceptoval pro dané PPPoE spojení.

Nesouhlasí-li přístupový bod s příznakem Service-Name v PADR paketu, pak musí odpovědět PADS paketem s nastaveným příznakem Service-Name-Error a SESSION ID musí mít hodnotu 0x0000.

Příklad

```
No.     Time        Source                Destination           Protocol Info
      4 0.002853    Intel_05:6e:7c        XnetTech_18:85:01     PPPoED   Active Discovery Session-confirmati

Ethernet II, Src: Intel_05:6e:7c (00:02:b3:05:6e:7c), Dst: XnetTech_18:85:01 (00:05:1c:18:85:01)
    Destination: XnetTech_18:85:01 (00:05:1c:18:85:01)
    Source: Intel_05:6e:7c (00:02:b3:05:6e:7c)
    Type: PPPoE Discovery (0x8863)
PPP-over-Ethernet Discovery
    Version: 1
    Type: 1
    Code: Active Discovery Session-confirmation (PADS)
    Session ID: 0001
    Payload Length: 22
PPPoE Tags
    Tag: Service-Name
      String Data: MojeSluzba
    Tag: Host-Uniq
      Binary Data: (4 bytes)
```

PPPoE Active Discovery Terminate (PADT) packet

Tento paket může být poslán kdykoliv během navázaného spojení a oznamuje, že PPPoE spojení bylo zrušeno. Paket může být odeslán jak klientem tak i přístupovým bodem.
Položka **CODE** je nastavena na **0xa7** a **SESSION_ID** musí korespondovat s identifikací spojení, které má být zrušeno.

Po přijetí PADT paketu není povoleno posílat další PPP provoz ani PPP pakety rušící spojení. Je doporučeno používat LCP protokol pro oznámení ukončení spojení, PADT může být použit jen tehdy, když nemůže být použit PPP protokol.

Volitelný příznak **Generic-Error** slouží k indikaci chyby. Může být připojen k PADO, PADR nebo PADS paketu pokud dojde k neopravitelné chybě. Obsahuje-li data, pak se musí jednat o textový řetězec v UTF8 kódování, který nesmí být ukončen nulovým symbolem (NULL).

Příklad

```
No.     Time        Source                Destination           Protocol Info
     34 6.557513    XnetTech_18:85:01     Intel_05:6e:7c        PPPoED   Active Discovery Terminate (PADT)

Ethernet II, Src: XnetTech_18:85:01 (00:05:1c:18:85:01), Dst: Intel_05:6e:7c (00:02:b3:05:6e:7c)
    Destination: Intel_05:6e:7c (00:02:b3:05:6e:7c)
    Source: XnetTech_18:85:01 (00:05:1c:18:85:01)
    Type: PPPoE Discovery (0x8863)
PPP-over-Ethernet Discovery
    Version: 1
    Type: 1
    Code: Active Discovery Terminate (PADT)
    Session ID: 0001
    Payload Length: 83
PPPoE Tags
    Tag: Host-Uniq
      Binary Data: (4 bytes)
    Tag: Generic-Error
      String Data: RP-PPPoE: System call error: Input/output error
    Tag: AC-Cookie
      Binary Data: (20 bytes)
```

PPP session

Jakmile je vytvořené PPPoE spojení, začínají se posílat data PPP protokolu. Položka **ETHER_TYPE** má hodnotu **0x8864**. Hodnota **CODE** musí být **0x00** a položka **SESSION_ID** se nesmí změnit během PPPoE spojení.

MTU PPP spojení nesmí být větší než 1492. (1500 (MTU Ethernetu) - 6 (hlavička PPPoE) - 2 (PPP protocol id))
Při ukončení spojení pomocí LCP nesmí klient ani server používat toto spojení. Pokud si klient přeje vytvořit nové PPP spojení, musí zahájit znovu vyhledávácí (Discovery) fázi.

Použitá literatura

RFC 2516 (www.faqs.org/rfcs/rfc2516.html)
RFC 1661 (http://www.ietf.org/rfc/rfc1661.txt)
Cisco - PPPoE Baseline Architecture (www.cisco.com/warp/public/794/pppoe_arch.html)
Wikipedia - PPPoE (en.wikipedia.org/wiki/PPPoE)
