

Dlaczego PPPoE (wersja 0.1) ?

Jakub Wartak <vnull@pcnet.com.pl>

Zalety PPPoE:

- Koncentrator lub serwer RADIUS przydziela adresy IP dla klientow, co w praktyce oznacza:
 - brak konfliktow adresow IP
 - praktyczny brak ARP w sieci (trudniej o podszytie sie pod klienta nawet w przypadku static IP+MAC)
 - brak ARP => wyciecie ARP na AP => ograniczenie “siania” ruchu ARP generowanego przez wirusy
 - łatwa zmiana adresu IP i DNSow dla klienta
 - lepsze wykorzystanie przestrzeni adresowe => nigdy nie ma 100% klientow w sieci, wiec można im publiczna przestrzen przydzielac
 - mozliwe przydzielanie statycznych adresow IP (usługa dodatkowa; wieksze dochody)

- Autoryzacja:
 - minium to login+haslo
 - dodatkowo, mozemy decydowac (serwerem RADIUSowym) czy wpuscimy klienta sprawdzajac takie warunki jak:
 - ♦ godzina, dzien tygodnia, etc.
 - ♦ adres MAC
 - ♦ polaczenie do wlasciwego koncentratora?
 - ♦ mozemy nie wpuscic klienta do sieci, jesli lacza sa przeciazone (brutalna metoda)
 - ♦ ilosc dotychczasowych polaczen , calkowicie , per dzien, per tydzien , etc.
 - ♦ ilosc dotychczasowych minut spedzonych w sieci, per dzien, per tydzien, etc. (tak jak w dialupie)
 - ♦ ilosc wyslanych/odebranych danych, per dzien, per tydzien, etc. (limitu transferu)

- Mamy calkowity nadzor nad komunikacja klient1 do/z klient2 (nawet na tej samej antenie) => wszystko przechodzi przez koncentrator, co umozliwia na wieksza wydajnosć sieci / lepsze filtrowanie ruchu / lepsze statystyki / latwiej namierzyc PC-ety z wirusami

- [Pelen automat]: A jak namierzymy juz PC-eta z wirusem, to modyfikujemy w bazie pole ze jest zawirusowany, rozlaczamy delikwenta, i RADIUS juz go nie wpusci; ewentualnie przekieruje ruch na strone z powiadomieniem

- Dynamiczne przydzielanie przepustowosci w chwili laczenia (na podstawie obciazenia lacz)

- Dynamiczne przydzielanie przepustowosci dla programow peer-to-peer w chwili laczenia (na podstawie obciazenia lacz)

- Mozliwe rozlaczenie klienta po pewnym czasie (Session-Timeout)

- Wszystko jest w pelni dynamiczne, brak restartowania firewalli w celu zmiany parametrow uslugi itp.

- Haslo do polaczenia moze byc przysylane:
 - jawnym tekstem
 - szyfrowane (CHAP)

- Sesja/polaczenie moze byc szyfrowana z moca:
 - 48 bitami
 - 64 bitami
 - 128 bitami

- Możliwość płynnego przechodzenia ze starego systemu ethernetowego/arp/ip na PPPoE – pojedynczymi klientami
- Rzeczywiste statystyki kto jest zalogowany / statystyki aktualnej ilości klientów połączonych
- Kto / o której i skąd się łączył, jaki miał ip i mac, ile wysłał i ile odebrał (informacje te często są bardzo potrzebne dla prokuratury w celu ustalenia sprawców przestępstw internetowych)
- Skomplikowane miesięczne schematy ograniczanie pasma łączone z limitami transferów np.:
 - Klient kupuje 128kbit/s z limitem transferu 5GB; po przesłaniu 5GB każde następne połączenie odbywa się z przydzielonym pasmem do 32kbit/s (cos ala TP Neo+)
- Możliwość ustawienia revDNSu w chwili łączenia się klienta
- Możliwość odpalania dodatkowych skryptów przy autoryzacji klienta na koncentratorach/routerach, np.: wysyłanie SMSa w przypadku połączenia się któregoś z klientów, odpalenie tcpdumpa z zapisem wszystkich przesłanych danych do pliku, logowanie początków połączeń do SQLowej itd.

Wady PPPoE:

- Wymagany jest klient PPPoE u klienta korzystającego z tej technologii,
 - Windows 2000 / XP i nowsze posiadają wbudowanego klienta
 - Do Windows 95 i 98 można doinstalować klienta
 - Większość dystrybucji Linuksowych wspiera natywnie PPPoE (to samo dotyczy się m.in. FreeBSD i OpenBSD)
- W przypadku stosowania szyfrowania znacząco obciążony jest CPU koncentratora. Gdy nie jest używane szyfrowanie wydajność przesyłu nie odbiega znacznie od wydajności bez PPPoE. W przypadku Linuxa jest to pojedyncze zwiększenie wskaźnika (ang. “pointer”) w przestrzeni jądra...

Software:

- Możliwość integracji z LMS (<http://lms.rulez.pl>) lub napisania własnego systemu obsługi klientów
- Serwer RADIUS: FreeRADIUS, działający na:
 - FreeBSD-STABLE (zalecany system)
 - Linux , dowolna stabilna dystrybucja
- Baza danych:
 - MySQL
 - PostgreSQL
 - Oracle
 - (ODBC – dowolna wspierana baza przez unixODBC)
- Wspierane koncentratory:
 - Linux 2.6.x z rp-pppoe
 - FreeBSD od 5.3
 - OpenBSD od 3.7

Zaawansowane, wysokodostępne konfiguracje:

- Dwa redundantne serwery RADIUS w różnych lokalizacjach, podpiete do tego samego szkieletu
 - Jeden pierwszorzędny, drugi zapasowy (na wypadek padu pierwszego)
 - Pełna replikacja danych pomiędzy nimi.
 - Pełna integralność danych po poprawnym “wstaniu” pierwszego.
 - Pierwszy to także serwer WWW obsługujący panel administracyjny / LMS.
- Dwa niezależne wyjścia na świat, pełna niezawodność dzięki BGP i OSPF

