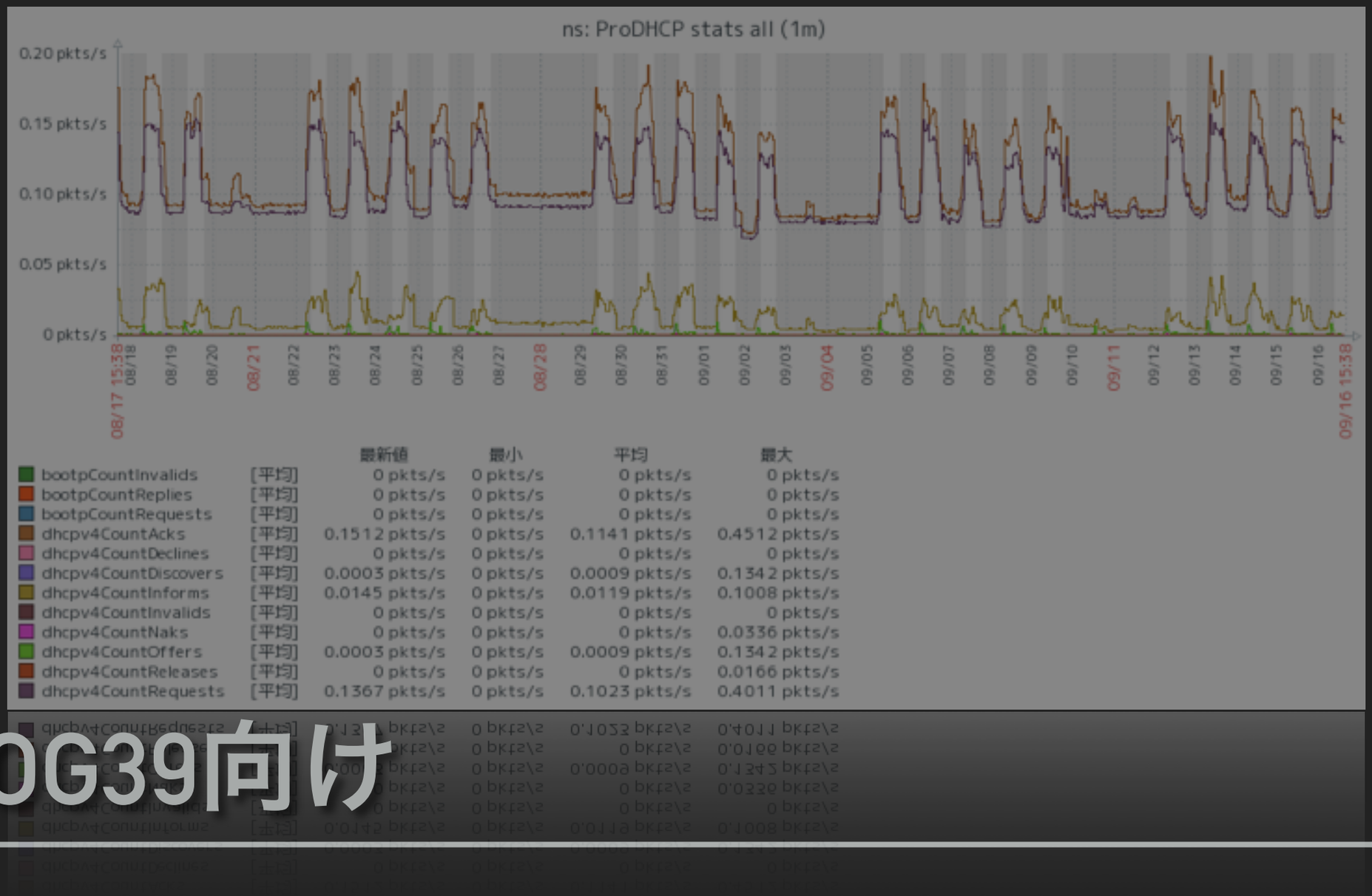


		最新値	最小	平均	最大
bootpCountInvalids	[平均]	0 pkts/s	0 pkts/s	0 pkts/s	0 pkts/s
bootpCountReplies	[平均]	0 pkts/s	0 pkts/s	0 pkts/s	0 pkts/s
bootpCountRequests	[平均]	0 pkts/s	0 pkts/s	0 pkts/s	0 pkts/s
dhcpv4CountAcks	[平均]	0.1512 pkts/s	0 pkts/s	0.1141 pkts/s	0.4512 pkts/s
dhcpv4CountDeclines	[平均]	0 pkts/s	0 pkts/s	0 pkts/s	0 pkts/s
dhcpv4CountDiscovers	[平均]	0.0003 pkts/s	0 pkts/s	0.0009 pkts/s	0.1342 pkts/s
dhcpv4CountInforms	[平均]	0.0145 pkts/s	0 pkts/s	0.0119 pkts/s	0.1008 pkts/s
dhcpv4CountInvalids	[平均]	0 pkts/s	0 pkts/s	0 pkts/s	0 pkts/s
dhcpv4CountNaks	[平均]	0 pkts/s	0 pkts/s	0 pkts/s	0.0336 pkts/s
dhcpv4CountOffers	[平均]	0.0003 pkts/s	0 pkts/s	0.0009 pkts/s	0.1342 pkts/s
dhcpv4CountReleases	[平均]	0 pkts/s	0 pkts/s	0 pkts/s	0.0166 pkts/s
dhcpv4CountRequests	[平均]	0.1367 pkts/s	0 pkts/s	0.1023 pkts/s	0.4011 pkts/s

JANOG39向け

DHCPも奥が深くて楽しいよ

日本シー・エー・ディー株式会社　小俣 光之

プロフィール

- 日本シー・エー・ディー株式会社(http://www.ncad.co.jp/)　代表取締役社長
  大学時代のアルバイトから社長まで全部の役職を経験？
- 著書12冊
  ルーター自作で分かるパケットの流れ
  プログラミングでメシが食えるか！？
  プログラムは技術だけでは動かない　など・・・

- プログラマー社長のブログ：http://blogs.itmedia.co.jp/komata/
- UNIX系OSでのC言語によるネットワークプログラミングしかできない
- DHCPサーバ・HTTPキャッシュ・MTA・情報セキュリティ製品など

DHCPとは

- BOOTPをベースにした、コンピュータがネットワーク接続する際に必要な情報を自動的に割り当てるプロトコル
  - ブロードキャストが多用される

クライアント				サーバ
初期化				
	→	DHCPDISCOVER	→	
	←	DHCPOFFER	←	
	→	DHCPREQUEST	→	
	←	DHCPACK/DHCPNAK	←	
延長・再/初期化・再割り当て				
	→	DHCPREQUEST	→	
	←	DHCPACK/DHCPNAK	←	
リリース				
	→	DHCPRELEASE	→	
辞退				
	→	DHCPDECLINE	→	
オプション取得				
	→	DHCPINFORM	→	
	←	DHCPACK	←	
リースクエリー				
	→	DHCPLEASEQUERRY	→	
	←	DHCPLEASEUNASSIGNED/DHCPLEASEUNKNOWN/DHCPLEASEACTIVE	←	

リレーエージェント

- 複数セグメントを一つのDHCPサーバで管理するために、セグメントごとに配置するエージェント
  - でも、ダイレクト：ユニキャストも使われる・・・

クライアント				リレーエージェント		サーバ
初期化						
	→	DHCPDISCOVER	→	中継	→	
	←	DHCPOFFER	←	中継	←	
	→	DHCPREQUEST	→	中継	→	
	←	DHCPACK/DHCPNAK	←	中継	←	
延長						
	→	DHCPREQUEST	→	ダイレクト	→	
	←	DHCPACK/DHCPNAK	←	ダイレクト	←	
再/初期化・再割り当て						
	→	DHCPREQUEST	→	中継	→	
	←	DHCPACK/DHCPNAK	←	中継	←	
リリース						
	→	DHCPRELEASE	→	ダイレクト	→	
辞退						
	→	DHCPDECLINE	→	中継	→	
オプション取得						
	→	DHCPINFORM	→	中継/ダイレクト	→	
	←	DHCPACK	←	中継/ダイレクト	←	

DHCPサーバの種類

- ISC-DHCPサーバ：Linuxなどに標準的に入っている
- MS-DHCP：WindowsServerに入っている
- DHCPサーバソフトウェア製品
- DHCPサーバアプライアンス

IPv4,IPv6

- IPv4とIPv6は全く別プロトコル
- IPv4はIPアドレスを配布
- IPv6はIPアドレスの配布もできるが、プレフィックス払い出しが中心
- 今回はIPv4のDHCPを話しの中心に・・・

DHCPサーバ製品開発販売の裏話

- ルーティングやDNSに比べると地味なDHCP・・・
- 大規模向けDHCPサーバ「ProDHCP」開発販売で経験したDHCPの裏話
- 主に回線事業者向けで経験した話題
- ネットワーク製品の自社開発販売の裏話も
- 目的は、現場や製品の批判ではなく、あくまでも情報共有

DHCPサーバ開発のきっかけ

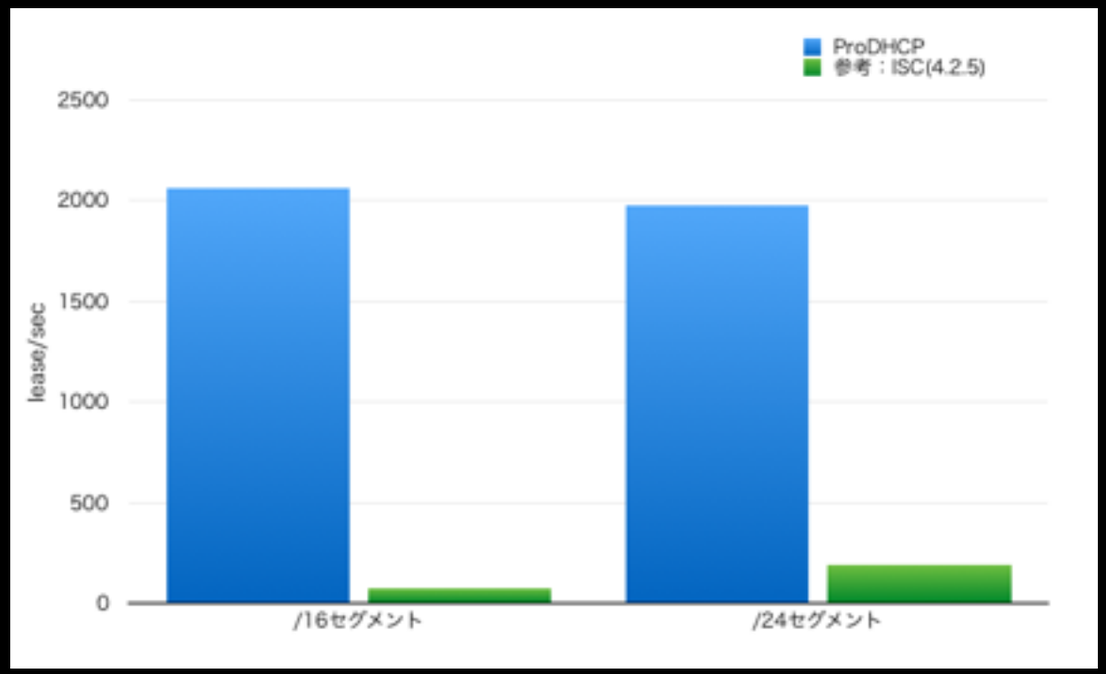
- 2005年に某回線事業者でISC-DHCPサーバを使ってサービスを構築していたSIerから相談がきた
  「設定反映時間がかかりすぎるので、改良して欲しい」
- 当時のISC-DHCPのReadmeには、「そこは要求しないで」と書かれていた気がする
- ISCのは、個人的にはカプセル化されすぎて読む気がしないソースだった・・・
- フルスクラッチでプロトタイプを3日間で作り、「改良ではなくフルスクラッチならやってもいい」と回答
- SIerから「回線事業者にフルスクラッチだとバレないようにやって」
- 1人月分しかもらえなかったので、使用権以外は渡さず、自社で製品化。

全く売れない→売れるまで

- とりあえず自社HPに載せたが、1年間問い合わせゼロ
  知名度も実績もないのであたりまえ・・・
- ソリトンシステムズからISC-DHCPを使ったアプライアンスで困っている
  と相談
  「ソースが読みやすいから」とOEM採用に
  でも、ライセンス料はごくわずかしか出せないと言われたので、「OEMしていることを公開させて」と依頼
- OEMのことを公開したらすぐに問い合わせがきて売れるようになった
  世の中とても分かりやすい、と学習

トピックス：払い出し性能

- 今どきは300万IPを管理した状態で1000リース/秒くらいは要求される？
- ProDHCPはシングルスレッド
  - 排他の問題
  - UDPの特性



公衆無線LAN

- 自社製品としての最初の実績は公衆無線LAN
- 短いリースタイム：特に駅では・・・？
- 当初は10万IP/サーバくらいであったが、あっという間に100万〜300万IP/サーバに・・・
- 特殊要件

  RFCに反して「毎回絶対に違うIPを払い出す機能」

  認証との連携

  犯罪調査

ケーブルネットワーク

- ケーブルネットワークはDOCSISでOption82！
  - でも、Option82はリレーエージェントが付加するオプション：ユニキャストはどうする？
- Option82で払い出しセグメントをコントロール
- とはいえ、最近は「Option82はログに出れば良い」というだけのケースも多い
- 統合が進んでいるのか、参加の事業者全てを1サーバでまかなう案件が多い？：本数が売れない・・・
- 逆に地域密着型も多いけど：たくさん売れる？

オレオレ仕様

- 某携帯事業者のWiFiサービス向け
- 一度払い出したIPアドレスは上位からアンロックするまで払い出さないこと
- 上位から予約したものだけを払い出すこと

  「このMACアドレス用にこのIPを予約」と上位からDHCPサーバに司令が来る

  プロトコルだけDHCP？

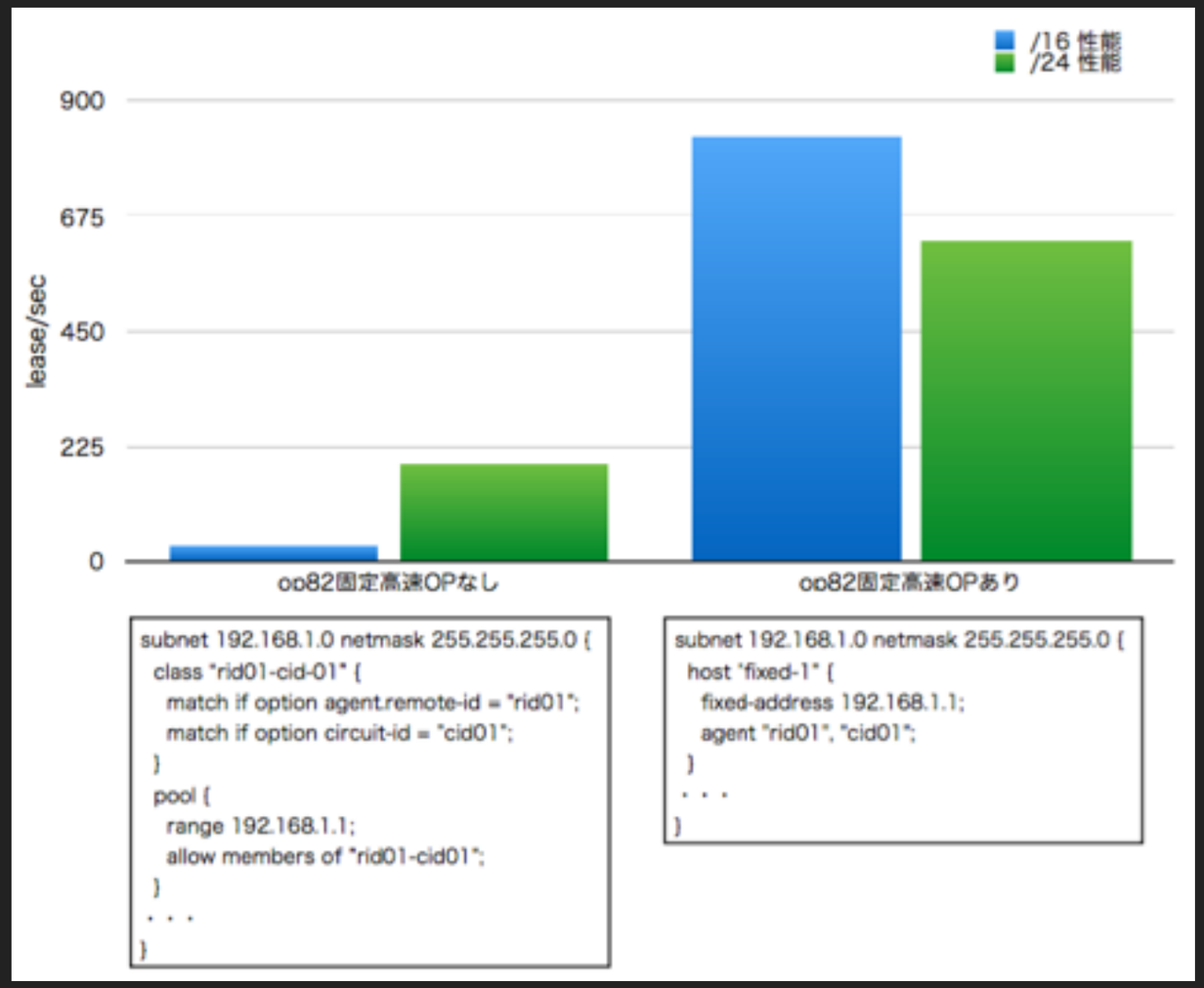
- おたくの会社が倒産すると困るから、ソースも欲しいと言われた

  保守用ソースコードライセンスも販売：それでも他社よりはるかに安いから全く問題ないと言われた・・・

OPTION82で固定IP

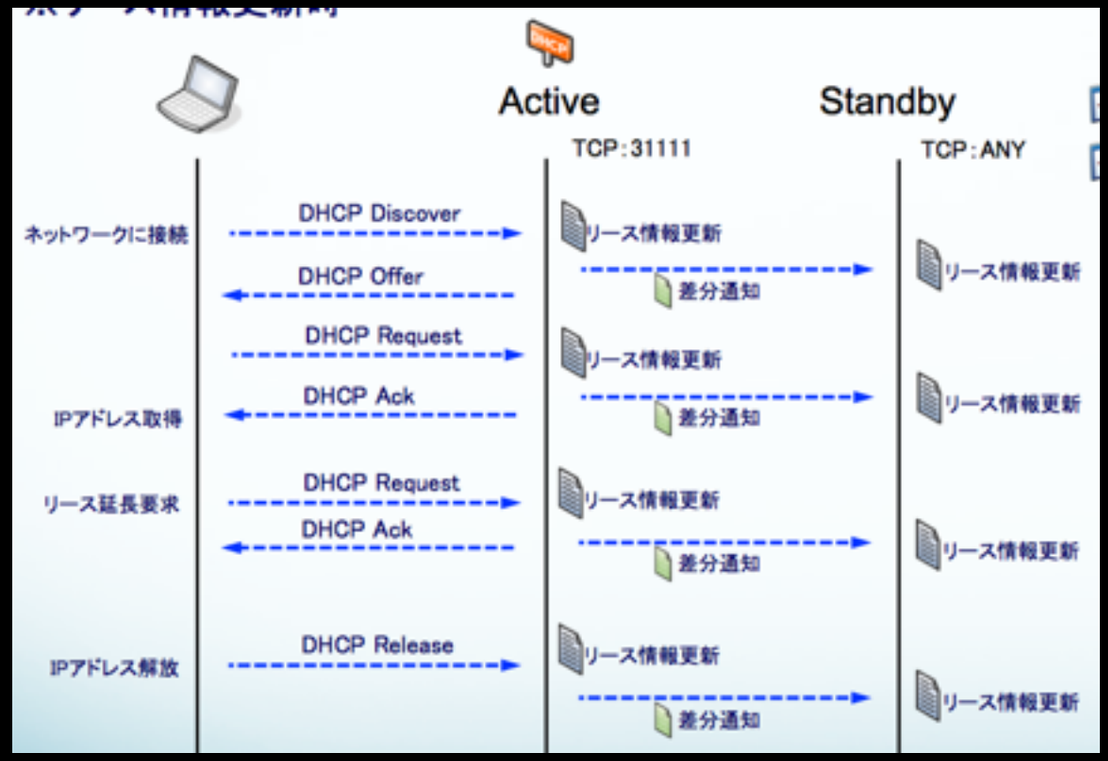
- 某回線事業者のあるサービスで、Option82で固定IP払い出しをしたいと言われる：機器交換が容易なようにclass,subclassを使って実現
- 最初は加入者が少なかったので問題なかったが、人気が出て払い出し性能が問題に

  class,subclassやmatch ifなどは、なんでもできるが遅い・・・
- 仕方ないので、host定義でOption82を記述できるようにして高速化



トピックス：冗長化

- DHCPではIPアドレス重複払い出しは致命的
  IP電話が繋がらないなど・・・
- ディスク共有は意外と問題が起きる
  アンマウントできないとか
- ProDHCPでは常時差分同期
  いつ切り替えてもOK
  本番機でビシバシ切り替え確認したら担当者がビビっていた！？



DDOS攻撃？

- 某社のルーターは一定時間内にDHCP応答が得られないと、狂ったようにDHCP要求を投げ続ける
- それに対応することでDHCPサーバが遅くなる
- 他の同一ベンダーのルーターも狂ったようにDHCP要求を投げ始める
- ProDHCPでは同一MACアドレスからの連続リクエストのフィルター機能をつけ、簡単に実装できたわりに喜ばれた

ブロードキャストフラグとトランザクションID

- ブロードキャストしか受信できない状態のクライアントはブロードキャストフラグを1にすべき
- クライアントはトランザクションIDで自分への応答かどうかを判断すること、トランザクションIDは他の端末と重複しないように乱数などを使用すること
- WindowsXPまでのWindowsはブロードキャストフラグを0で送っていたが、1で応答しないとリレーエージェントが仲介できないケースがあり、ブロードキャストフラグを常に1だと考えて処理することをDHCPサーバ側で指定できるようにしていた
- あるルーターのDHCPクライアント機能はトランザクションIDを毎回ゼロで送ってくるため、ブロードキャストフラグを常に1だと考えて処理すると、ブロードキャストされるため、トランザクションIDを他の機器への応答と取り違えておかしな動きになる問題が発生した・・・
- http://blogs.itmedia.co.jp/komata/2015/03/dhcpid.html

オプションの応答順序

- あるDHCPクライアントは、DHCP応答のsubnet-maskがオプションの中で早めにないとうまく処理できないという問題があった
- DHCPサーバのベンダーなのだからこのくらい知っていないと！と言われた・・・

ISCの固定IP定義

- ISCのDHCPサーバでは、以下のような固定IP定義は思惑通りに動かない

```
subnet 192.168.33.0 netmask 255.255.255.0 {
    range 192.168.33.10 192.168.33.20;
    max-lease-time 7200;
    default-lease-time 3600;
    option routers 192.168.33.254;
    host some-fix-host {
        hardware ethernet 02:00:00:00:00:00;
        fixed-address 192.168.33.10;
    }
}
```

- 192.168.33.10はrangeに含まれているので、02:00:00:00:00:00以外の端末からのリクエストにも払い出される
- 実は「Dynamic and static leases present for 192.168.33.10. Remove host declaration some-fix-host or remove 192.168.33.10 from the dynamic address pool for 192.168.33.0/24」こんな警告がログに出る
- rangeはあくまでも動的として使われる：：固定IP定義でIPアドレス封鎖はできない！
- 意外と知らない人が多く（私も知らなかった）、「ISCのは固定にしていても使われちゃうんだよね〜」という話しを聞く・・・
- http://blogs.itmedia.co.jp/komata/2016/08/iscdhcpip.html

DHCPのクライアントIDオプション

- クライアントからのリクエストに「クライアントID」が指定されていたら、サーバは「クライアントID」でクライアントを識別し、指定されていなければ「クライアントハードウェアアドレス：MACアドレス」で識別
- MacOSではユーザが簡単にクライアントIDを指定できる
- こんな機能使うの？？
- http://blogs.itmedia.co.jp/komata/2014/10/dhcpid-c2e1.html

DHCP負荷テストツール無償公開中！

- https://www.ncad.co.jp/~prodhcp/download.html

DHCP負荷試験ツール - DHCP load test tool

「DHCP負荷試験ツール」 dhcpperf は、DHCPサーバに対し複数のクライアントが同時にDHCPアドレスを取得する動作を模倣し、高負荷時の性能試験・評価を行うためのツールです。

The DHCP load testing tool simulates the sending of DHCP address requests by multiple clients simultaneously to a DHCP server in order to test and evaluate its performance under high loads.

- dhcpperf-0.3.5 CentOS5 64bit (RPM) (tgz) (readme JP EN)
- dhcpperf-0.3.5 CentOS6 64bit (RPM) (tgz) (readme JP EN)
- dhcpperf-0.3.5 CentOS7 64bit (RPM) (tgz) (readme JP EN)
- DHCP性能比較資料（2698KB PDF） download

DHCPv6負荷試験ツール

「DHCPv6負荷試験ツール」 dhcp6perf は、DHCPv6サーバに対し複数のクライアントが同時にDHCPv6アドレスを取得する動作を模倣し、高負荷時の性能試験・評価を行うためのツールです。

- dhcp6perf-0.1.3 CentOS5 64bit (RPM) (tgz) (readme JP)
- dhcp6perf-0.1.3 CentOS6 64bit (RPM) (tgz) (readme JP)
- dhcp6perf-0.1.3 CentOS7 64bit (RPM) (tgz) (readme JP)

議論のネタ

- DHCPで困ったことありますか？
- BOOTPは無効にしてますか？
- DHCPリースクエリー・DHCPスヌーピング（使ったことありません）
- IPv6は？
- 冗長化・負荷分散
  - 高性能・高可用性プログラミング
  - 自社製品開発販売のメリット・デメリット
  - 本を書くのってどう？