Zero Touch Configuration

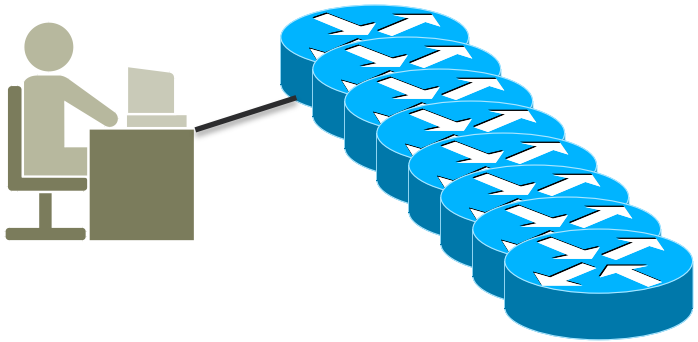
JANOG38 Meeting in Okinawa

Shishio Tsuchiya

shtsuchi@cisco.com

Zero Touch Configurationとは？

- ユーザが機器にログインする事をせず、設定を完了させる手法
- Zero Touch Provisioning(ZTP)

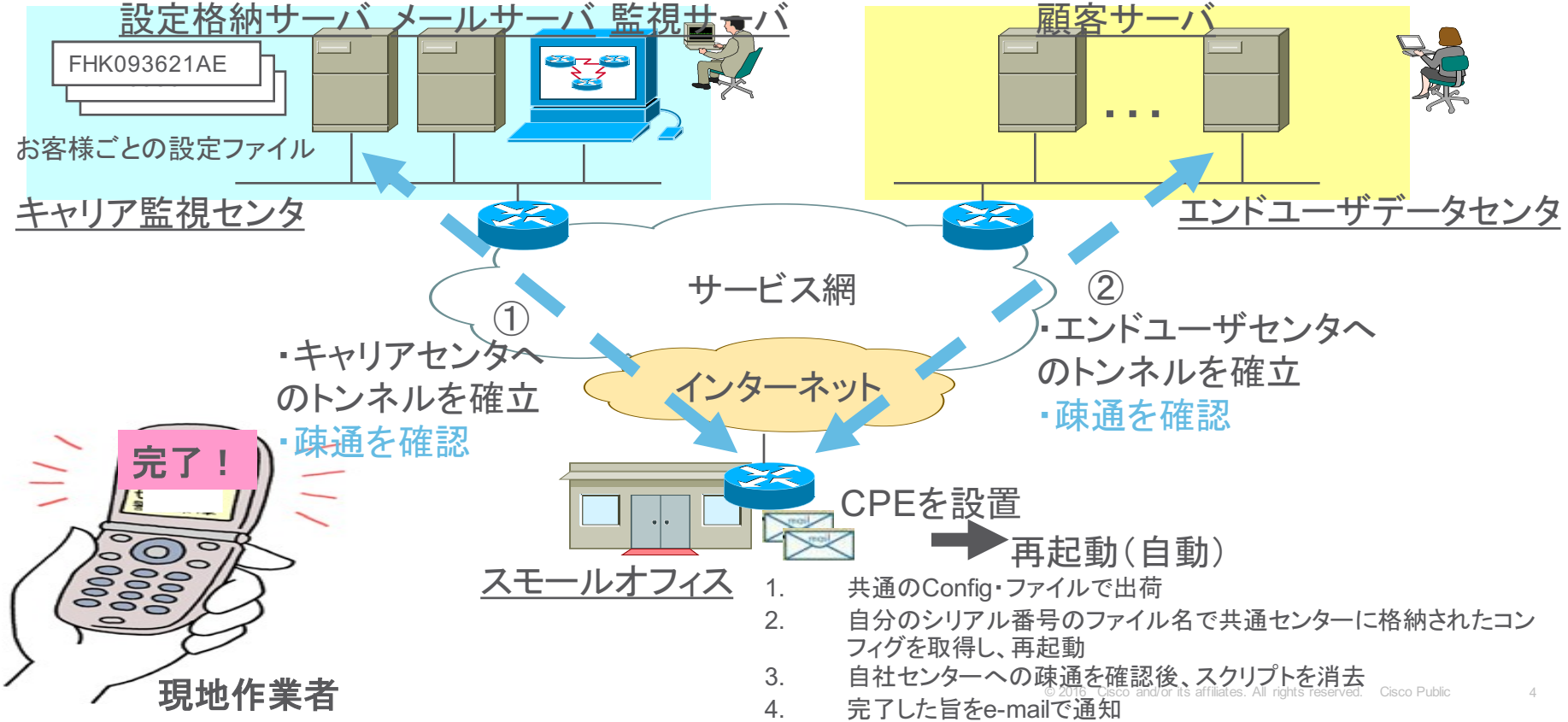


Agenda

- 今まであったZTPのアイディア
- データセンターのZTP
- ZTP over インバンドネットワーク

NTTPC Communications Inc.

事例紹介



1. 共通のConfig・ファイルで出荷
2. 自分のシリアル番号のファイル名で共通センターに格納されたコンフィグを取得し、再起動
3. 自社センターへの疎通を確認後、スクリプトを消去
4. 完了した旨をe-mailで通知

まとめ

- 複雑（PPPoE）な環境での現地でのZTPを実現
- ルータが持つスクリプト機能を活用
- シリアル番号を元にコンフィグをダウンロード

- 事前の共通コンフィグが必要

YAMAHAさん
リモートセットアップ

- 電話番号のみで機器に接続が出来る
- ISDN/専用線/モバイルに対応
- フレッツ光ネクストのデータコネクトにも対応

http://www.rtpro.yamaha.co.jp/RT/FAQ/Intro/remote-setup.html
http://www.rtpro.yamaha.co.jp/RT/docs/remote-setup/foma-remote-setup.html
http://www.rtpro.yamaha.co.jp/RT/docs/ngn/ngn_remote_setup.html

まとめ

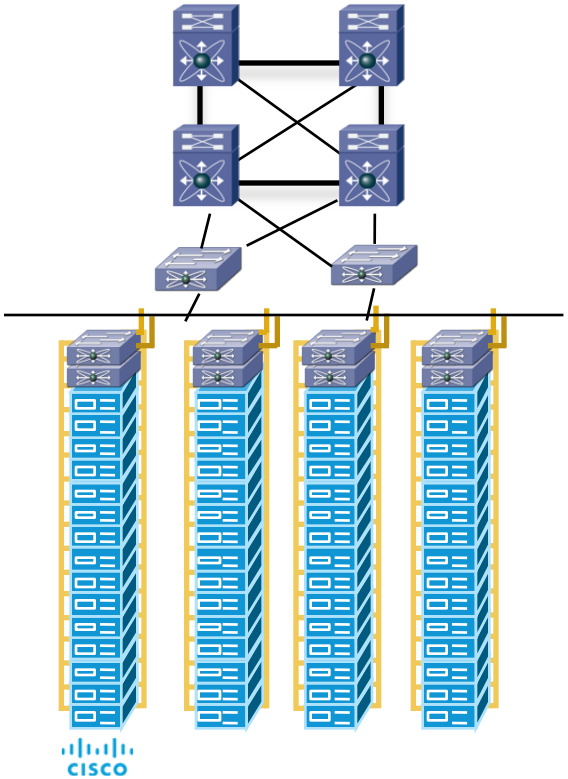
- IPを用いず電話番号だけで遠隔機器にログイン可能
- インバンド管理ネットワークを構築出来る
  - （既に出来てるネットワークを利用）

- 正確には…ZTPという話では無い
- セキュリティとの問題
  - 電話番号認証などが必要

Agenda

- 今まであったZTPのアイディア
- データセンターのZTP
- ZTP over インバンドネットワーク

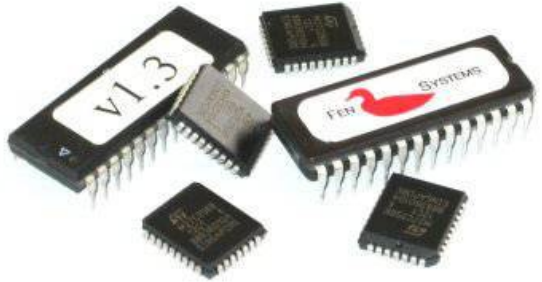
ネットワークブートの必要性



- 複数のサーバーが存在するデータセンターでは下記の理由でのネットワークブートが有効
  - 物理的に移動する必要が無い
  - HDDが壊れた時のリカバリー
  - 一度に大量にインストールしたい
  - 複数のOSを同じ環境にインストールする

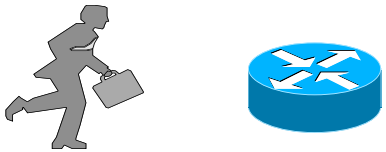
iPXEとは？

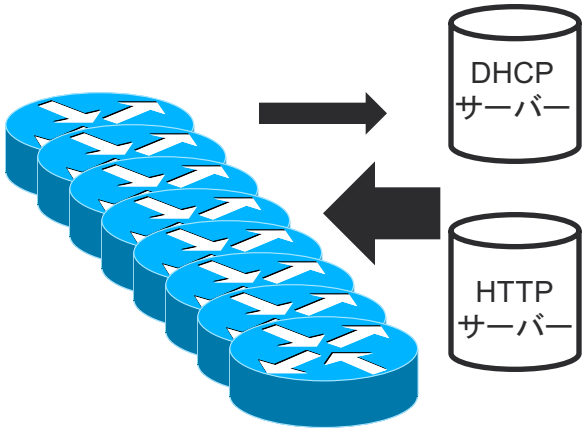
- PXE(Preboot eXecution Environment)はDHCP/TFTPなどの標準的なプロトコルを使ったイーサネットブートの仕組み
- ROMに書き込み可能な非常に小さいオープンソースブートローダー
- gPXEによりHTTP/iSCSI/ATAoE/Wifiなどに拡張
- iPXEは2010年に終了したgPXEの後継
- TFTPブートのみでは無く、HTTPやIPv6もサポート
- スクリプトと連動する事も可能
- CD-ROMやUSBにも収容可能



iPXEを使ったネットワークOSのブート

- サーバーで構築された環境をそのまま使える
- 大量キッティング時間の短縮や現地作業も可能か!?
- 共有ラボでは必須？

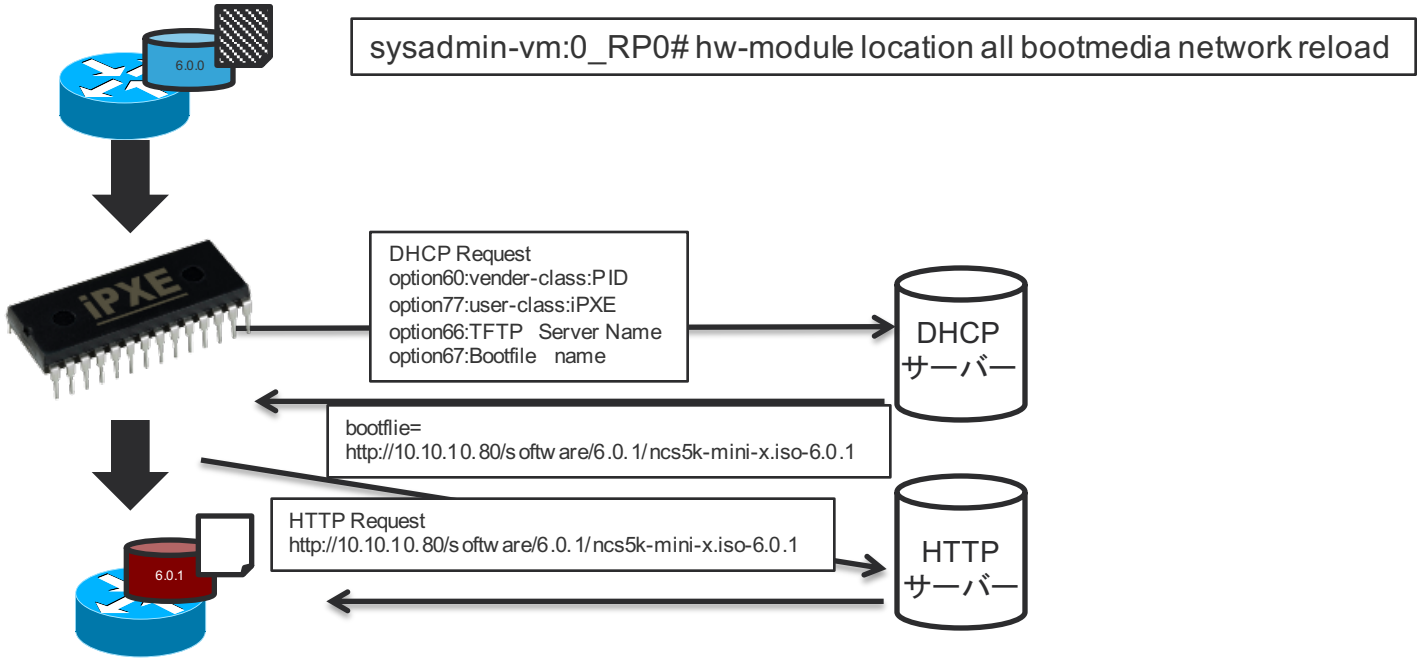




iPXEで使うDHCPv4オプション

- Option 60 “Vender-class-identifier”
  - タイプ：PXEClient　プロダクトID(PID)を表示
- Option 61 ″dhcp-client-identifier”
  - システムのシリアルナンバー
- Option 66 “TFTP Server name”
- Option 67 “Boot File name”
- Option 77 “user-class”
  - iPXEと表示される
- Option 97 “uuid” 世界で唯一の識別子(RFC4122)

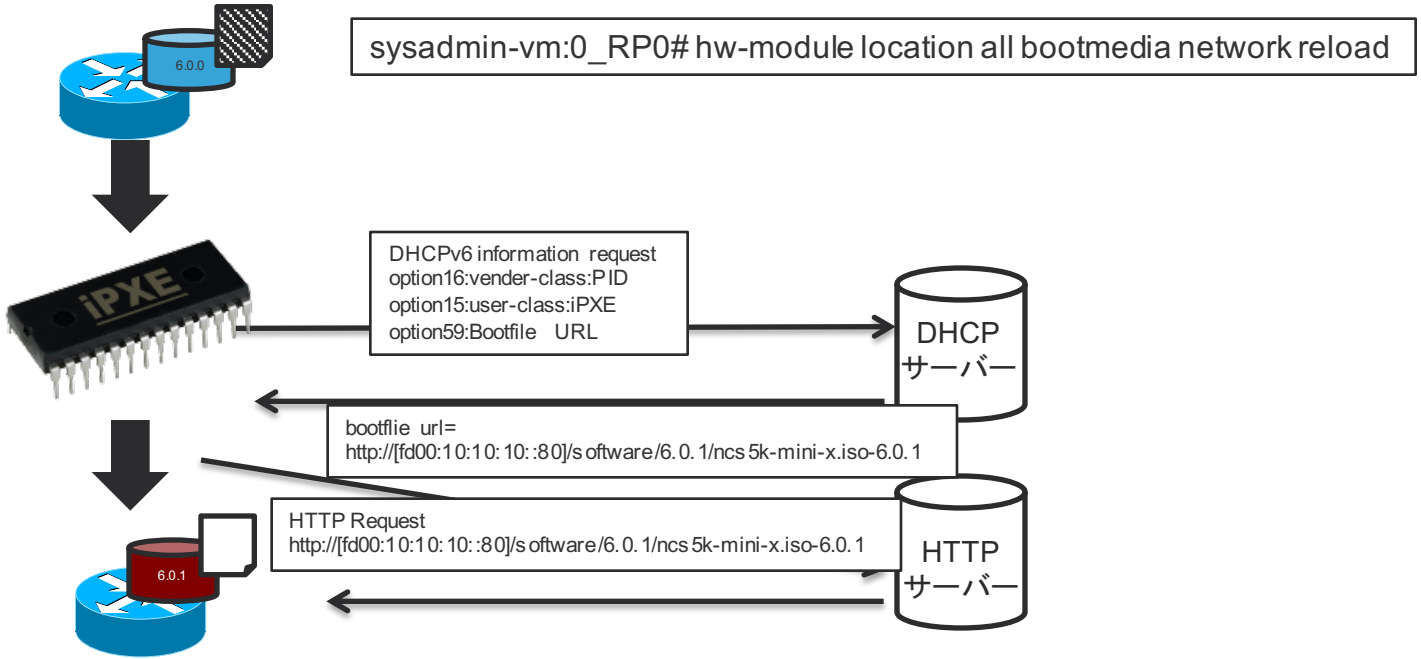
iPXEブートシーケンス DHCPv4



iPXEで使うDHCPv6オプション

- Option 1 “client-identifier”
  - DHCPv6クライアントのID
    - *DHCPv6ではクライアントMACアドレスは送られない
- Option 15 “dhcp6.user-class”
  - DHCPv4 Option77と同様 iPXEと表示
- Option 16 “vendor-class-identifier”
  - DHCPv4 Option60と同様 “PXEClient” PID/企業名を表示
- Option 59 “dhcp6.bootfile-url”
  - DHCPv4 Option67と同様

iPXEブートシーケンス DHCPv6



iPXEブート画面

```
sysadmin-vm:0_RP0# hw-module location all bootmedia network reload
Sat May  28 22:13:32.119 UTC
Reload hardware module ? [no,yes] yes
--snip--
iPXE 1.0.0+ (72b21) -- Open Source Network Boot Firmware -- http://ipxe.org
Features: DNS HTTP TFTP VLAN EFI ISO9660 NBI Menu
Trying net0...
net0: dc:eb:94:56:42:e0  using dh8900cc on PCI01:00.1 (open)
  [Link:up, TX:0 TXE:0 RX:0 RXE:0]
Configuring (net0 dc:eb:94:56:42:e0).....  ok
net0: 10.10.10.101/255.255.255.0  gw 10.10.10.80
net0: fe80::deeb:94ff:fe56:42e0/64
net1: fe80::deeb:94ff:fe56:42e1/64 (inaccessible)
Next server: 10.10.10.67
Filename: http://10.10.10.80/software/6.0.1/ncs5k-mini-x.iso-6.0.1
http://10.10.10.80/software/6.0.1/ncs5k-mini-x.iso-6.0.1... ok
Booting iso-image@0x4311a2000(786817024), bzImage@0x4311cf000(4473998)
**** PASS: secure boot verification of iamge: bzImage****
[    5.298722] i8042: No controller found
mkdir: cannot create directory '/run': File exists
--snip--
```

ダウンロード%を表示

ISC DHCPの設定例
/etc/dhcp/dhcpd.conf

```
default-lease-time 600;
max-lease-time 7200;
log-facility local7;
###iPXE demo###
subnet 10.10.10.0 netmask 255.255.255.0 {
   option subnet-mask 255.255.255.0;
   option broadcast-address 10.10.10.255;
   option routers 10.10.10.80;
   option domain-name-servers 8.8.8.8;
   option domain-name "cisco.com";
   range 10.10.10.100 10.10.10.250;
  class "ncs-5k" {
     match if substring (option vendor-class-identifier, 0, 9) = "PXEClient";
          filename = "http://10.10.10.80/software/6.0.0/ncs5k-mini-x.iso-6.0.0";
     }
}
```

ISC DHCPの設定例 /etc/dhcp/dhcpd6.conf

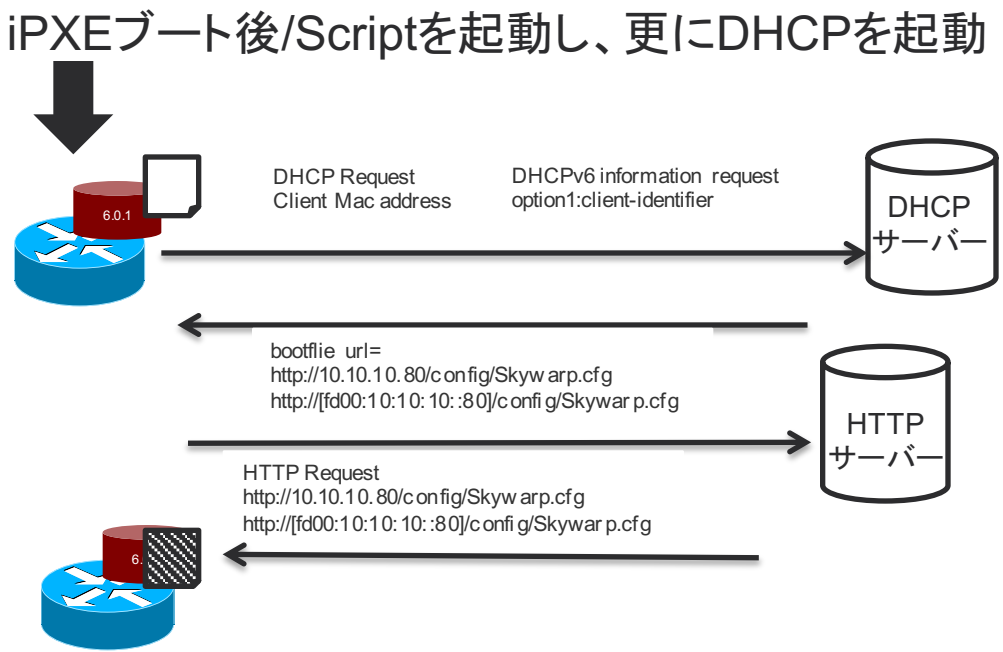
```
option dhcp6.user-class code 15 = string;
option dhcp6.bootfile-url code 59 = string;
default-lease-time 600;
max-lease-time 72000;
log-facility local7;
   subnet6 fd00:10:10:10::/64 {
      range6 fd00:10:10:10::0100 fd00:10:10:10::FFFD;
      range6 fd00:10:10:10::/64 temporary;
   class "ncs5k" {
      match if substring (option dhcp6.user-class, 2, 4) = "iPXE";
    option dhcp6.bootfile-url "http://[fd00:10:10:10::80]/software/6.0.1/ncs5k-mini-x.iso-6.0.1";
}
}
```

iPXE

- DHCP/HTTPを使用
- 標準的なやり方で簡単に大量のOSのインストールを実現
- コンフィグも初期状態に

- ん？ZTP・・・
- iPXEはスクリプト連携が可能
  - http://ipxe.org/scripting

ZTP(Zero Touch Provisioning)



ISC DHCPの設定例
/etc/dhcp/dhcpd.conf

```
default-lease-time 600;
max-lease-time 7200;
log-facility local7;
###iPXE demo###
subnet 10.10.10.0 netmask 255.255.255.0 {
   option subnet-mask 255.255.255.0;
   option broadcast-address 10.10.10.255;
   option routers 10.10.10.80;
   option domain-name-servers 8.8.8.8;
   option domain-name "cisco.com";
   range 10.10.10.100 10.10.10.250;
  host Skywarp {
     hardware ethernet dc:eb:94:56:42:e0;
     if exists user-class and option user-class = "iPXE" {
          filename = "http://10.10.10.80/software/6.0.1/ncs5k-mini-x.iso-6.0.1";
           }
      else { filename = "http://10.10.10.80/config/Skywarp.cfg";
          }
              }
}
```

ISC DHCPの設定例
/etc/dhcp/dhcpd6.conf

```
option dhcp6.user-class code 15 = string;
option dhcp6.bootfile-url code 59 = string;
default-lease-time 600;
max-lease-time 72000;
log-facility local7;
   subnet6 fd00:10:10:10::/64 {
      range6 fd00:10:10:10::0100 fd00:10:10:10::FFFD;
      range6 fd00:10:10:10::/64 temporary;
  host Skywarp {
      host-identifier option dhcp6.client-id 00:02:00:00:00:09:46:4f:43:32:30:30:33:52:30:4b:47:00;
      fixed-address6 fd00:10:10:10::10;
      if option dhcp6.user-class  = 00:04:69:50:58:45 {
           option  dhcp6.bootfile-url "http://[fd00:10:10:10::80]/software/6.0.1/ncs5k-mini-x.iso-6.0.1";
            }
       else { option dhcp6.bootfile-url "http://[fd00:10:10:10::80]/config/Skywarp.cfg";
            }
}
}
```

ztp.log

```
xr-vm_node0_RP0_CPU0:~]$cat ztp/ztp.log
Wed Jun 1 13:09:16 UTC 2016:ztp-main:ZTP initializing
Wed Jun 1 13:09:17 UTC 2016:ztp-main:Start dhclient
Wed Jun 1 13:09:17 UTC 2016:ztp-main:Exit
Wed Jun 1 13:09:20 UTC 2016:ztp-hook: Entered exit-hook
Wed Jun 1 13:09:20 UTC 2016:ztp-hook: Using DHCPv6 bootfile option
Wed Jun 1 13:09:20 UTC 2016:ztp-hook: Download target=http://[fd00:10:10:10::80]/config/Skywarp.cfg
Wed Jun 1 13:09:20 UTC 2016:ztp-hook: Check if startup configuration has completed
Wed Jun 1 13:09:25 UTC 2016:ztp-hook: Entered exit-hook
Wed Jun 1 13:09:30 UTC 2016:ztp-hook: Startup configuration has completed
Wed Jun 1 13:09:31 UTC 2016:ztp-hook: Requesting suggested URL
http://[fd00:10:10:10::80]/config/Skywarp.cfg with http_header [-H X-cisco-serial:FOC2003R0KG -H X-
cisco-arch:x86_64 -H X-cisco-uuid: -H X-cisco-oper:exr-config -H X-cisco-platform:skywarp ]
Wed Jun 1 13:09:31 UTC 2016:ztp-hook: We've got config file, first, revert configuration
Wed Jun 1 13:09:31 UTC 2016:ztp-hook: Applying config...
Wed Jun 1 13:09:40 UTC 2016:ztp-hook: Config applied, please check configuration
Wed Jun 1 13:09:40 UTC 2016:ztp-hook: Configuration file will be saved at /disk0:/ztp/ztp_config_done
Wed Jun 1 13:09:40 UTC 2016:ztp-hook: Shutting down dhclient - eth0 eth1
Wed Jun 1 13:09:40 UTC 2016:ztp-hook: ZTP complete
```

まとめ

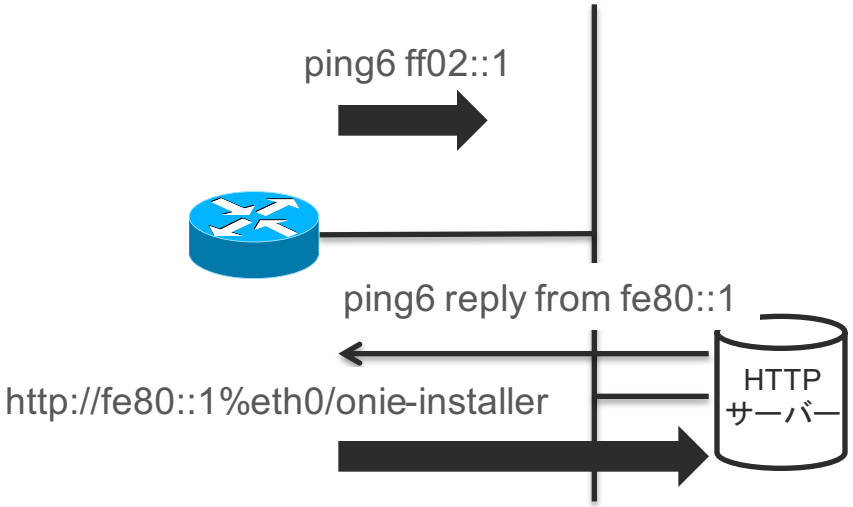
- iPXEを使ってソフトウェアのバージョン入れ替え作業が簡単に
- 大量のインストールにも対応可能
- スクリプト機能を使ってZTPも可能に

ONIEとは

- ONIE(Open Network Install Environment)
- ホワイトボックス環境などでの異なるOSの入れ替えを容易にする為の取り組み
- サービス発見はDHCPだけでは無く、mDNS/DNS-SDやIPv6 Link Localにも対応可能
- デフォルト名前検索順がある

```
onie-installer-x86_64-VENDOR_MACHINE-r0
onie-installer-x86_64-VENDOR_MACHINE
onie-installer-VENDOR_MACHINE
onie-installer-x86_64-SWITCH_SILICON_VENDOR
onie-installer-x86_64
onie-installer
```

HTTP IPv6 Neighbors



1. リンクローカルマルチキャストPing実施
2. 戻ってきた相手に対して、デフォルト名前検索をURLにし、ダウンロードを実施
   - 自動でアドレスを作成するIPv6の特徴を上手く使用

まとめ

- DHCPだけではなく、mDNS/DNS-SDを使う
- IPv6を上手（？）に使う

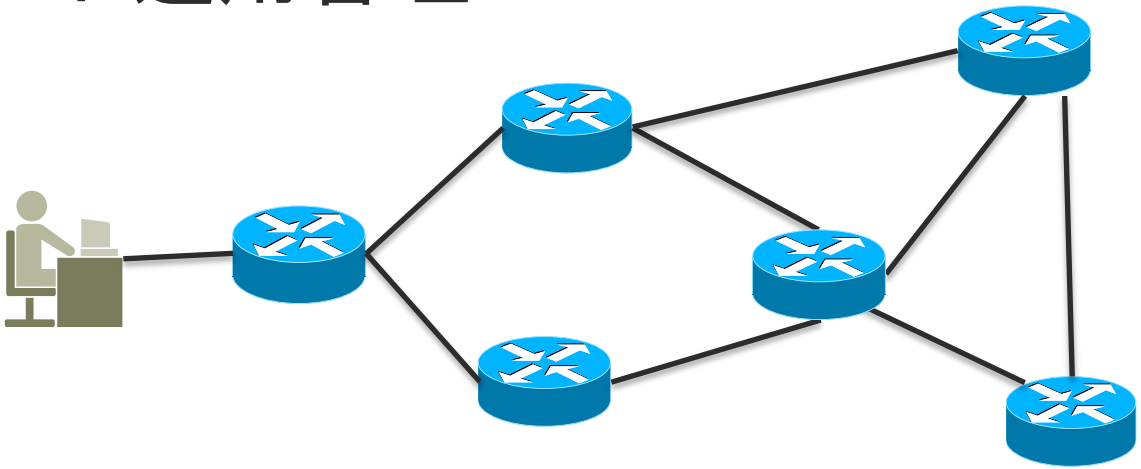
Agenda

- 今まであったZTPのアイディア
- データセンターのZTP
- ZTP over インバンドネットワーク

今までのソリューションから必要なもの

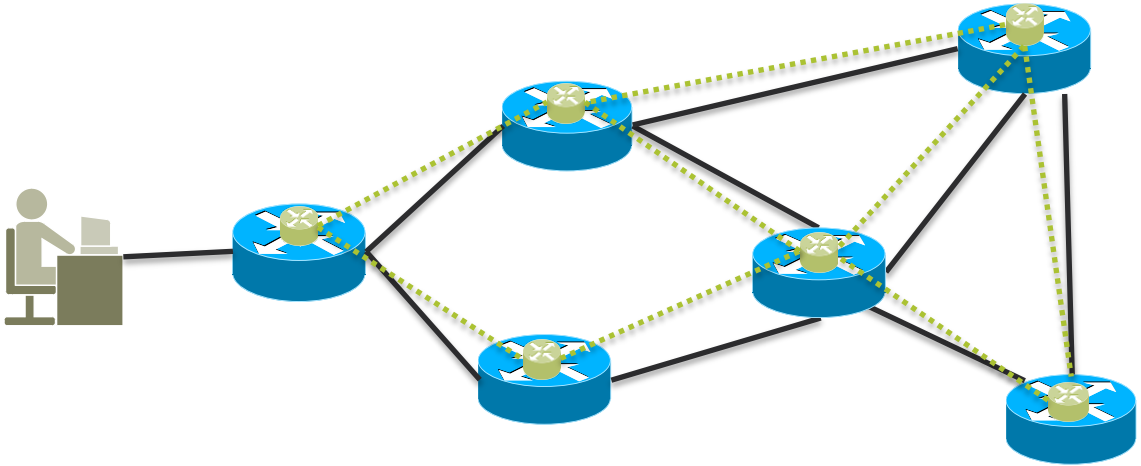
- ノードが自動的/自発的に動く
- セキュリティの担保
- 識別子（シリアルナンバー/MACアドレス/電話番号/UUID)
- 通常運用に依存しない管理ネットワーク/チャネルの構築
  - SDH/SONETのDCC(Data Communication Channel)
  - リモートセットアップでの電話番号
- IPv6の上手な使い方

リモート運用管理



- 運用コスト：アウトバンドネットワーク>インバンドネットワーク
- ネットワークマネージメントに影響がある様な運用が多い
  - アクセスリストの設定
  - スクリプト実施によるユーザ追加/削除
  - ルーティングコスト変更

理想



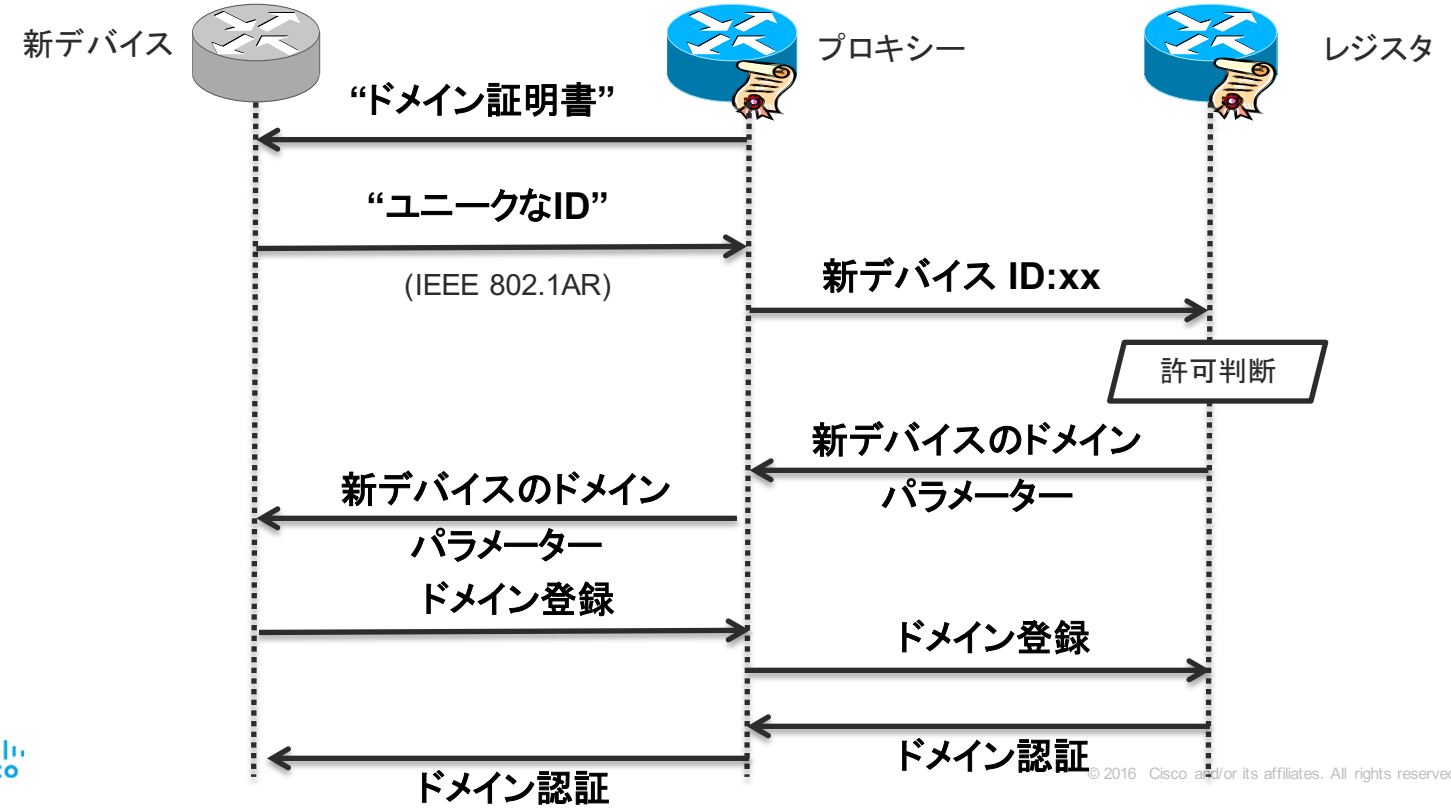
- インバンドネットワーク
- リモートの機器には触らずにセキュアに出来上がる
- 運用には依存しないネットワーク

IETF ANIMA WG

- ANIMA(Autonomic Networking Integrated Model and Approach)
- 自律型ネットワークの統合モデルとアプローチ
- IRTF NWRGでは自律ネットワークに関して議論しゴールをまとめた(RFC7575)
- またRFC7576では現時点でのギャップを解析した
- ANIMA WGは下記の様なプロトコルを定義する為のWG
  - 自律ノードの発見
  - 自律ノード間のネゴシエーション
  - 信頼できるインフラの構築
  - 自律コントロールプレーンの分離

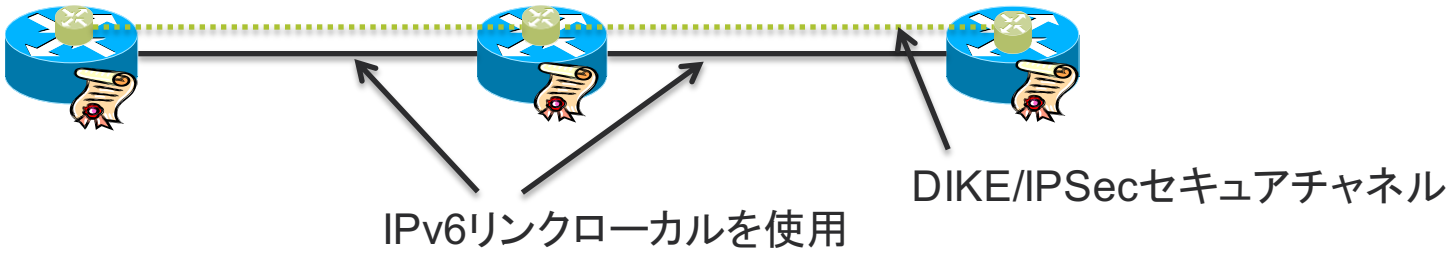
セキュアドメイン認証登録

draft-ietf-anima-bootstrapping-keyinfra



Autonomic Control Place

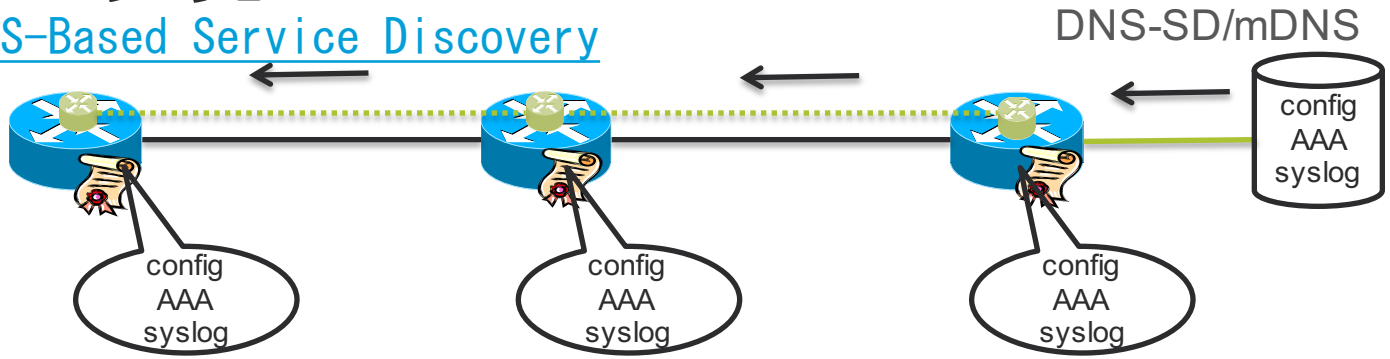
draft-ietf-anima-autonomic-control-plane



- IPアドレスを持っていない初期状態のノードでどうやり取りするのか？
- IPv6リンクローカルの使用をし、IPSec/DIKEなどのセキュアチャネルを構築
- loopbackはULAアドレスで自動的に生成され、RPL(IPv6 Routing Protocol for Low power and Lossy Networks)でルーティング
- 全てのインターフェースはVRFに属する為、ユーザデータの影響をうけない

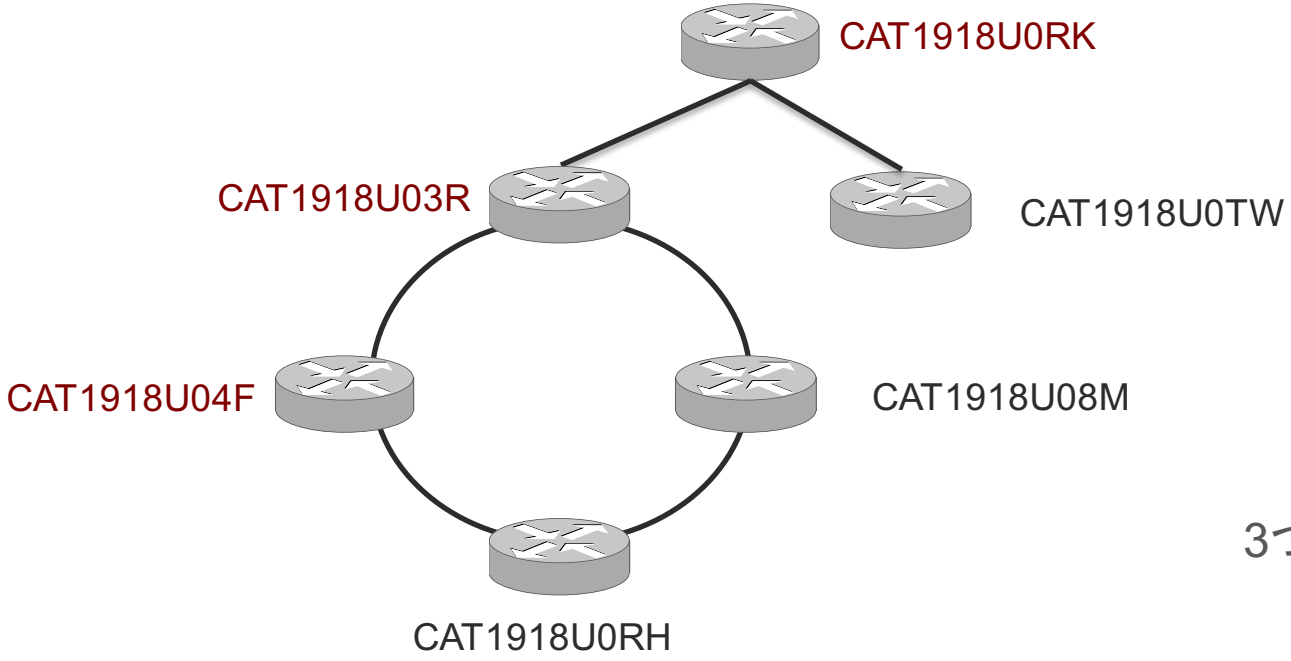
サービス発見

RFC6793 DNS-Based Service Discovery



- DNS-SD/mDNSを使ったサービスディスカバリー
- サーバーはアプリケーションをmDNSを使ってアナウンス
- サーバーはACPの中に属し、ANは自律的にサービスを発見する

ビデオトポロジー



3つのコンソールを表示

レジスタ設定

```
!
autonomic registrar
 domain-id cisco.com
 CA local
 whitelist bootflash:whitelist.txt
 no shut
autonomic
!
```

ドメインID

CAをルータ自身が行う。外部CAも可

ホワイトリスト
登録機器のPIDとシリアルナンバーを記載

デバイス認証確認

show autonomic device

```
R1#show autonomic device

      Status                        Enabled
      Type                          Autonomic Registrar
      UDI                           PID:ASR-920-4SZ-A SN:CAT1918U0RK
      Device ID                     e865.49a9.ff80-1
      Domain ID                     cisco.com
      Domain Certificate            (sub:) ou=cisco.com+serialNumber=PID:ASR-920-4SZ-A SN:CAT1918U0RK,cn=e865.49a9.ff80-1
      Certificate Serial Number     02
      Device Address                FD08:2EEF:C2EE:0:E865:49A9:FF80:1
      Domain Cert is Valid
```

```
R2#show autonomic device

      Status                        Enabled
      Type                          Autonomic Node
      UDI                           PID:ASR-920-4SZ-A SN:CAT1918U03R
      Device ID                     e865.49a9.ff80-3
      Domain ID                     cisco.com
      Domain Certificate            (sub:) ou=cisco.com+serialNumber=PID:ASR-920-4SZ-A SN:CAT1918U03R,cn=e865.49a9.ff80-3
      Certificate Serial Number     04
      Device Address                FD08:2EEF:C2EE:0:E865:49A9:FF80:3
      Domain Cert is Valid
```

ACP確認

show autonomic control-plane

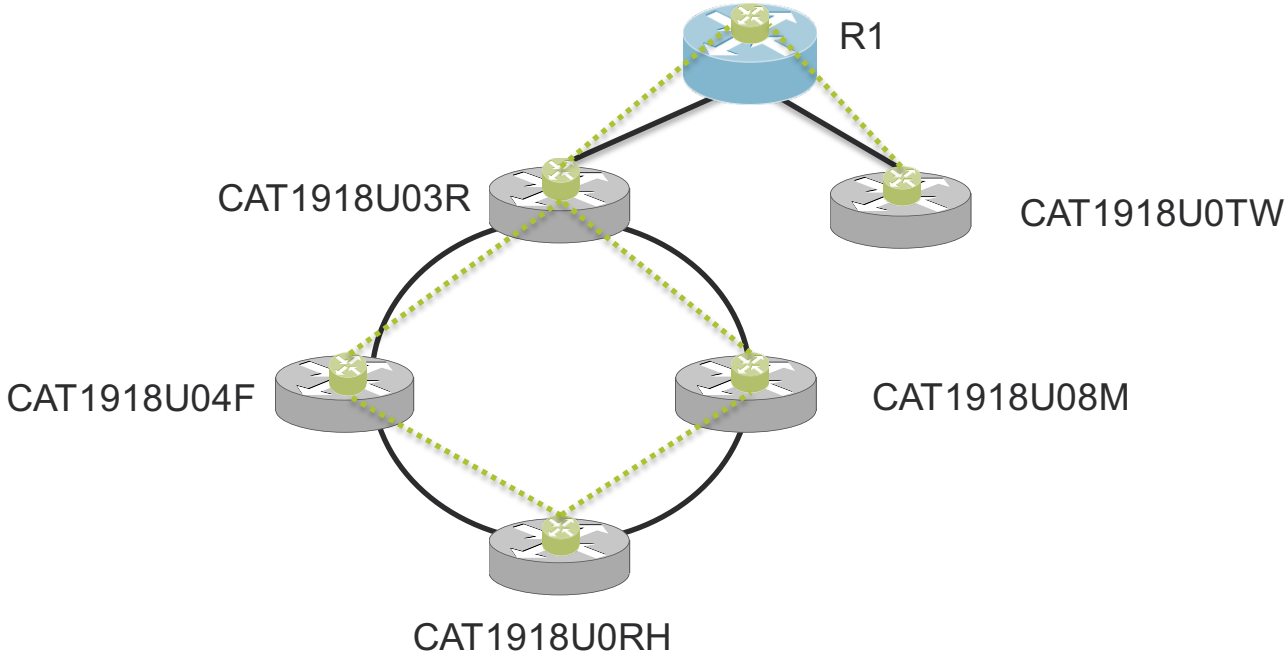
```
R1#show autonomic control-plane

VRF Name                        cisco_autonomic
Device Address                  FD08:2EEF:C2EE:0:E865:49A9:FF80:1
RPL                             Type = Root, Inst-Id = 0, OCP = 0, Mode = Storing

Neighbor                                              ACP Channel     ACP Security
-----------------------------------------------------------------------------------
PID:ASR-920-4SZ-A SN:CAT1918U03R                      Tunnel100005    DIKE
PID:ASR-920-4SZ-A SN:CAT1918U0TW                      Tunnel100004    DIKE
```

ACPルーティングテーブル確認

show ipv6 route vrf cisco_autnomic

```
R1#show ipv6 route vrf cisco_autonomic rpl
IPv6 Routing Table - cisco_autonomic - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, a - Application
RL  FD08:2EEF:C2EE:0:E865:49A9:FF80:2/128 [210/0]
     via FE80::EA65:49FF:FEA9:FC80%default, Tunnel100004%default
RL  FD08:2EEF:C2EE:0:E865:49A9:FF80:3/128 [210/0]
     via FE80::56A2:74FF:FE8C:AC80%default, Tunnel100005%default
RL  FD08:2EEF:C2EE:0:E865:49A9:FF80:4/128 [210/0]
     via FE80::56A2:74FF:FE8C:AC80%default, Tunnel100005%default
RL  FD08:2EEF:C2EE:0:E865:49A9:FF80:5/128 [210/0]
     via FE80::56A2:74FF:FE8C:AC80%default, Tunnel100005%default
```

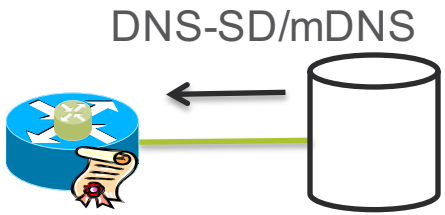
AN完成



サービスディスカバリー

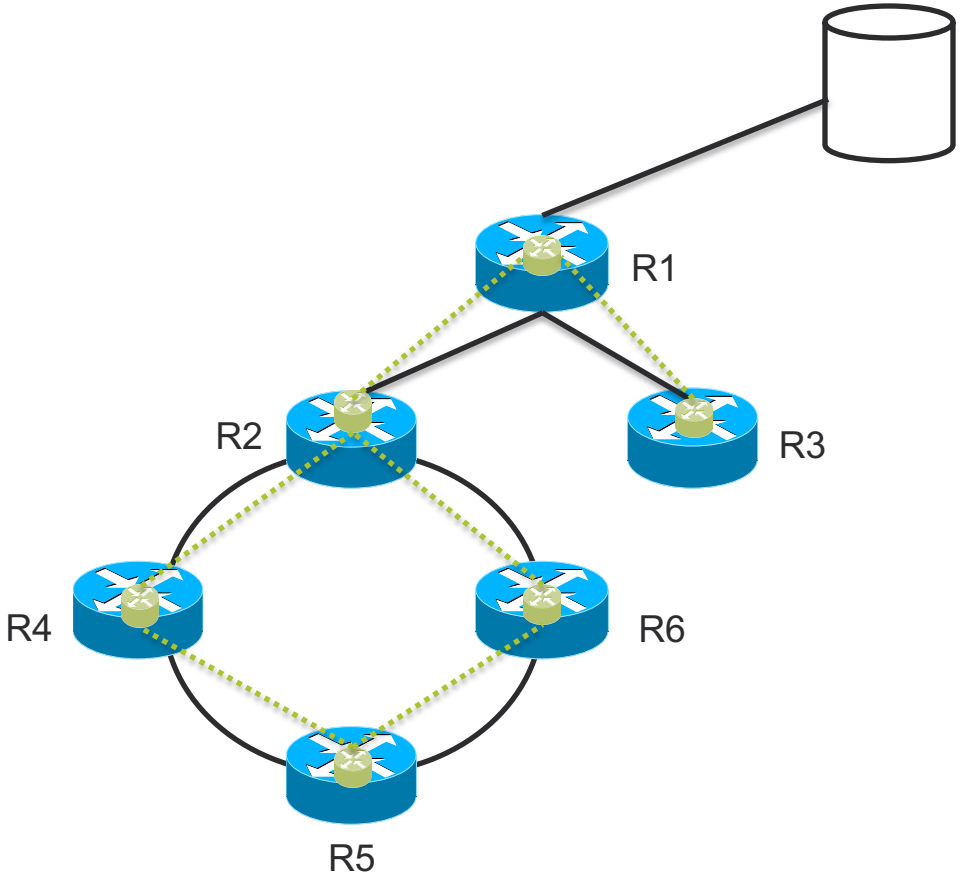
show autonomic service

```
!
interface GigabitEthernet0/0/1
 no ip address
 media-type rj45
 negotiation auto
 ipv6 address 2001:DB8:100::1/64
 ipv6 enable
 autonomic connect
!
```




```
R1#show autonomic service

Service                         IP-Addr
Syslog                          2001:DB8:100::100
AAA                             2001:DB8:100::100
 AAA Accounting Port            1813
 AAA Authorization Port         1812
Autonomic registrar             FD08:2EEF:C2EE:0:E865:49A9:FF80:1
 ANR type                       IOS CA
Config Server Address           2001:DB8:100::100
Auto IP Server                  UNKNOWN
```

ZTP



まとめ

- IETF ANIMAで定義されたAutonomic Networkはバーチャルインバンドを基本としたセキュアで自動的な仕組みである
- ODL SNBI(Secure Network Bootstrapping Infrastructure)でもプロジェクトとして、この仕組みを作成中
- ZTPのみでは無く、普段の運用に影響のないマネージメントプレーンを構築可能

議論

- どんな時、ZTPが欲しいですか？
- 今、どんな仕組みでキッティングや現地交換作業をしてますか？
- シリアル管理可能ですか？
- ONIEって必要？

デモ・ビデオ

- iPXE->ZTPを実施したデモ・ビデオ(12:19)

  iPXEでのダウンロード（2：26）が終わるとXRの解凍なので、10:31まで飛んで下さい

  https://cisco.box.com/s/6wpd94rfbe3dm3vsk5pz20s9lgxp4spo

- Autonomic Networkデモ・ビデオ（19:30)

  ASR920を6台使って、ANを構築します。

  初期設定状態からANの確立（-10:30)

  サービスディカバリーからコンフィグダウンロード(R1:-11:02,R2:-13:29,R4:-16:26)

  R6にログインし、ネットワーク切断から復旧(16:53-19:30)

  https://cisco.box.com/s/mi5q12jsw497y33sqo63iixxo6d8krdx


THERE'S NEVER BEEN A
BETTER TIME
to do something amazing
CISCO