



IPv4 EXHAUSTION

IPv6オペレータ育成プログラム

本資料は2009年12月3-4日に開催されたIPv4アドレス枯渇対応タスクフォース主催の
IPv6ハンズオンセミナー
「iDC ネットワーク編」(講師:井上一清氏)を元に
し、公開用に資料を編集したものである。

IPv4アドレス枯渇対応タスクフォース
<http://www.kokatsu.jp/>



IPv4
EXHAUSTION

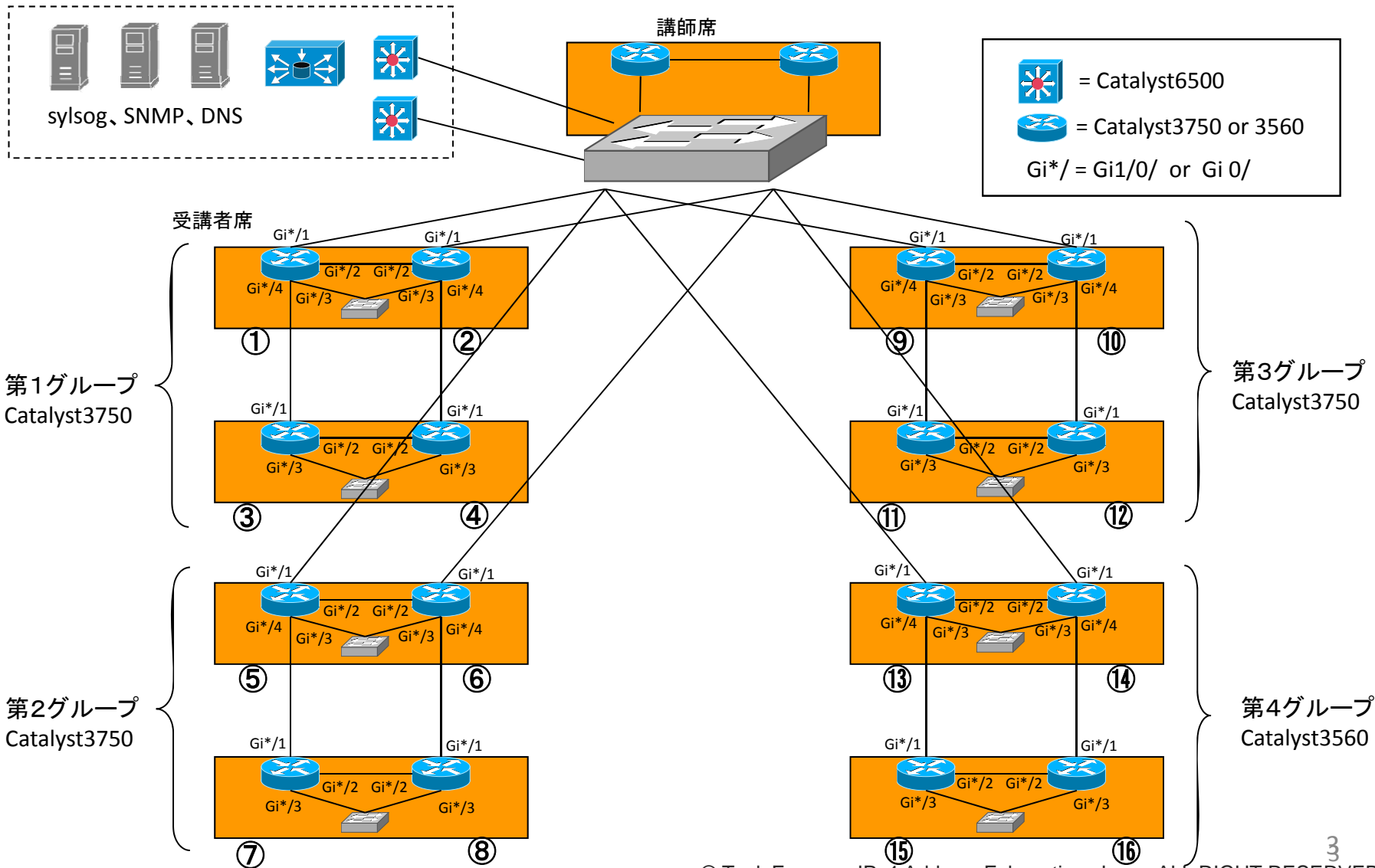
IPv6オペレータ育成プログラム

iDCネットワーク編ハンズオン用資料

株式会社iDCフロンティア

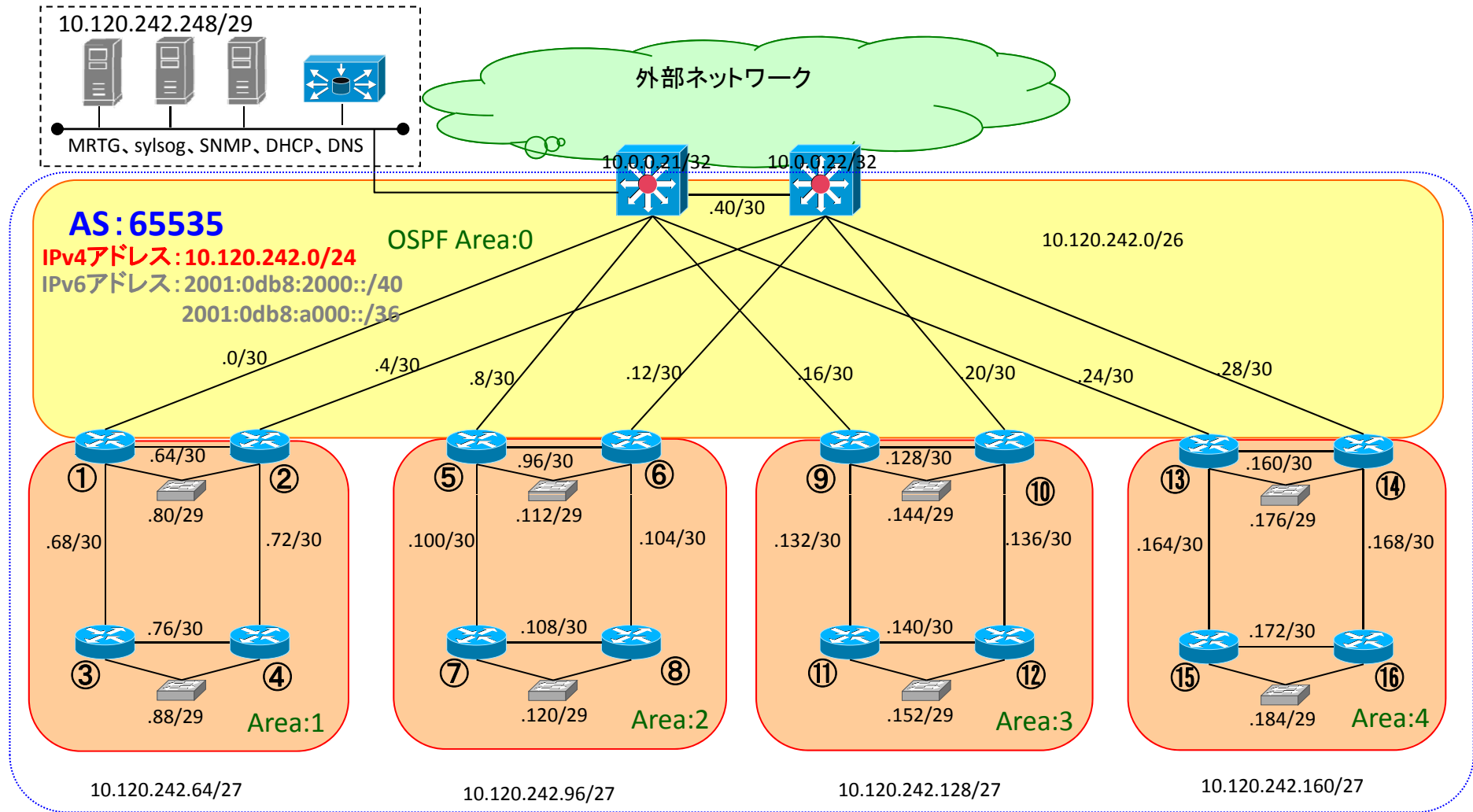
井上 一清

IPv6ハンズオン物理構成図





ハンズオン論理構成図 (IPv4)

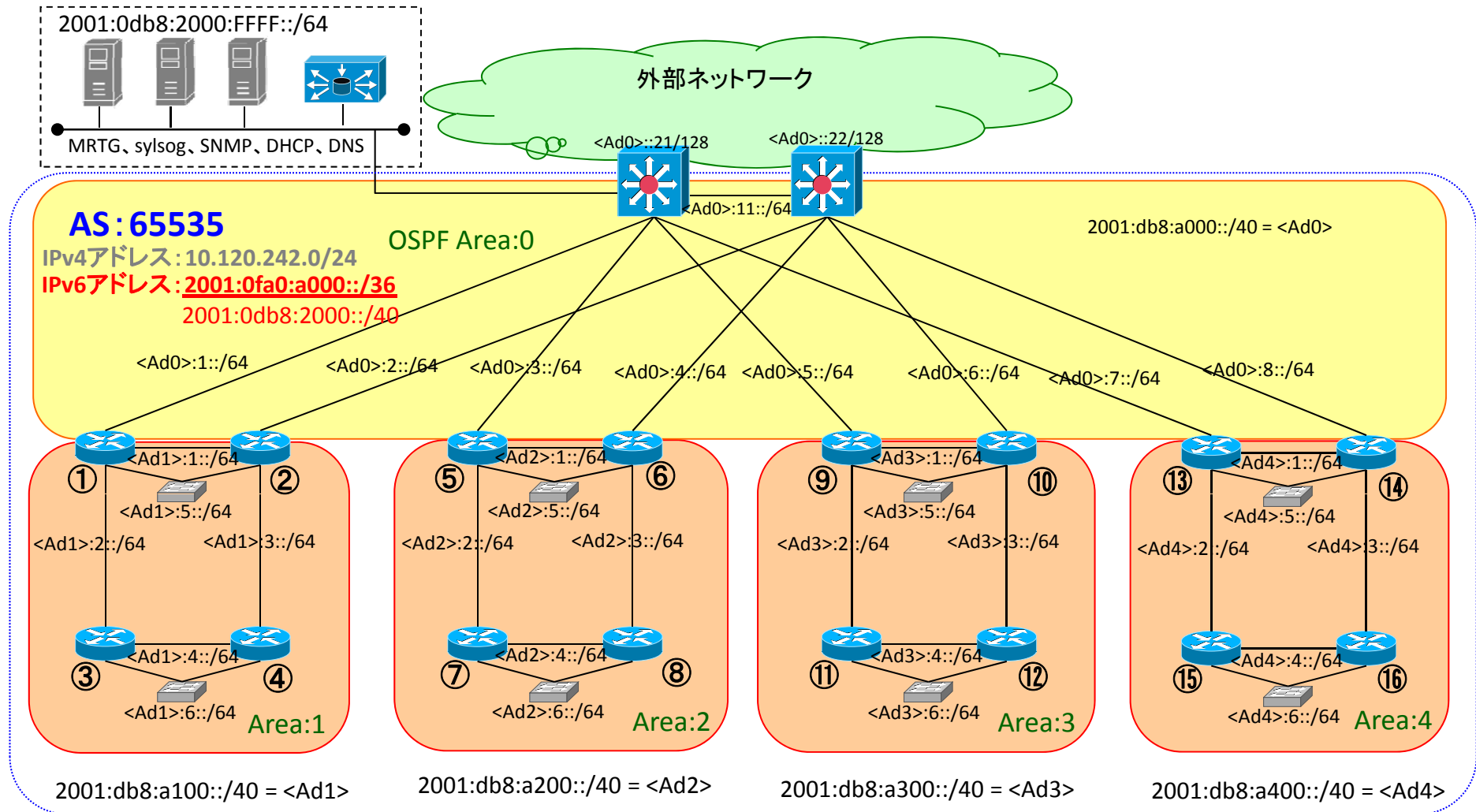


上位NW側に若番のIPをアサイン
 若番の機器側に若番のIPをアサイン

Loopbackアドレスは10.0.0.x/32 (xは座席番号)



ハンズオン論理構成図 (IPv6)

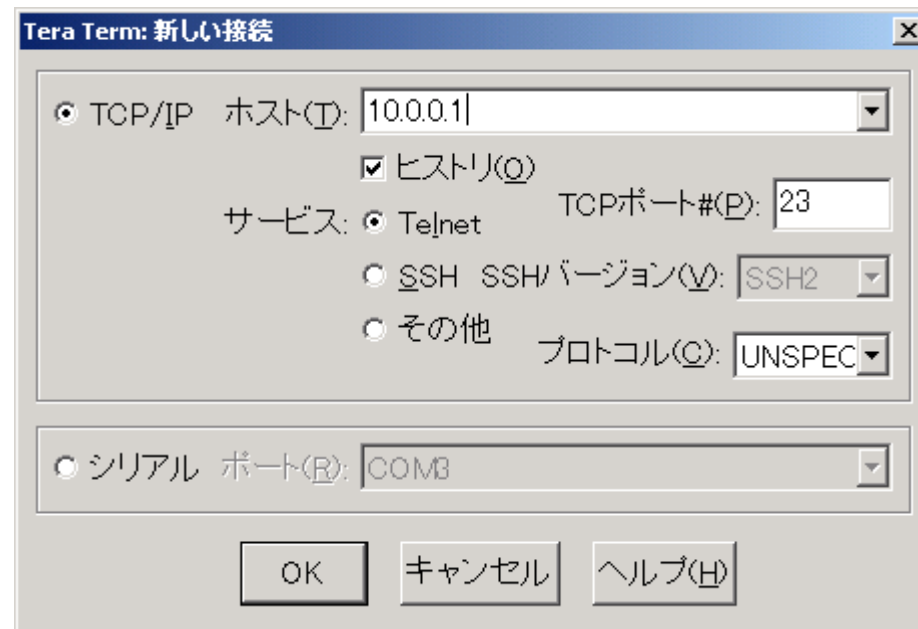


$\langle Adx \rangle :: 1 \sim \langle Adx \rangle :: 4/128$ をLoopback 0にアサインする



ルータへのログイン

- デスクトップにあるショートカットのTeraTermを使用してtelnetログインを行う
- ルータのIPアドレスは10.0.0.X
 - Xは座席番号
- Passwordは”ipv6”



※login、enable後はterminal monitorを有効にしておいて下さい。



(参考)SDMの設定と確認

SDMの設定

```
Cat3k(config)#sdm prefer ?
access      Access bias
default     Default bias
dual-ipv4-and-ipv6 Support both IPv4 and IPv6
ipe         IPe bias
routing     Unicast bias
vlan        VLAN bias
Cat3k(config)#sdm prefer dual-ipv4-and-ipv6 ?
default     Default bias
routing     Unicast bias
vlan        VLAN bias
Cat3k-13(config)#sdm prefer dual-ipv4-and-ipv6 routing
Changes to the running SDM preferences have been stored, but cannot take effect
until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
Cat3k(config)#
```

参考:

http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/sw/cat30/3750escg/chapter08/9775_01_8.shtml



(参考)SDMの設定と確認

SDMの確認 – 変更前

```
└Cat3k#sh sdm prefer
```

The current template is "desktop default" template.

The selected template optimizes the resources in the switch to support this level of features for 8 routed interfaces and 1024 VLANs.

number of unicast mac addresses:	6K
number of IPv4 IGMP groups + multicast routes:	1K
number of IPv4 unicast routes:	8K
number of directly-connected IPv4 hosts:	6K
number of indirect IPv4 routes:	2K
number of IPv4 policy based routing aces:	0
number of IPv4/MAC qos aces:	0.5K
number of IPv4/MAC security aces:	1K

On next reload, template will be "desktop IPv4 and IPv6 routing" template.

```
Cat3k#
```




(参考)SDMの設定と確認

SDMの確認 – 変更後

```
Cat3k#sh sdm prefer
```

The current template is "desktop IPv4 and IPv6 routing" template.

The selected template optimizes the resources in the switch to support this level of features for 8 routed interfaces and 1024 VLANs.

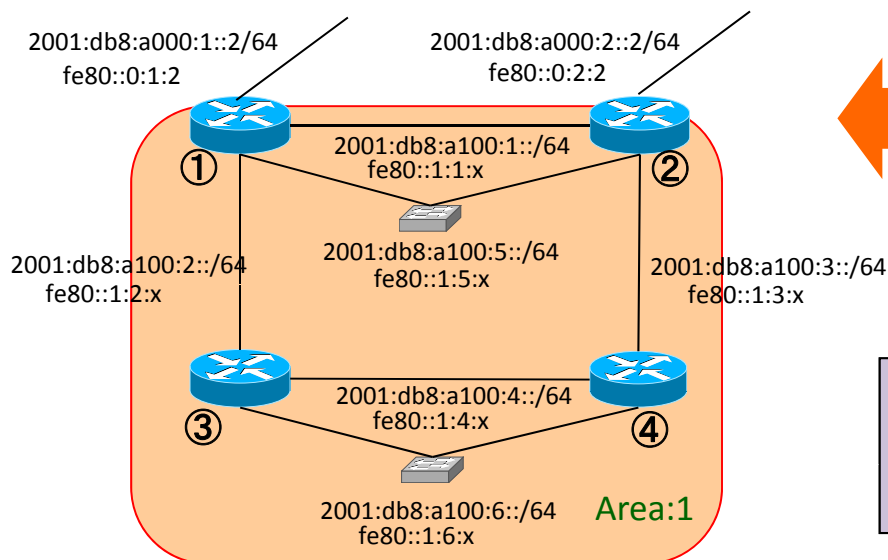
```
number of unicast mac addresses:          1.5K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes:           2.75K
  number of directly-connected IPv4 hosts: 1.5K
  number of indirect IPv4 routes:         1.25K
number of IPv6 multicast groups:          1.125k
number of directly-connected IPv6 addresses: 1.5K
number of indirect IPv6 unicast routes:    1.25K
number of IPv4 policy based routing aces: 0.25K
number of IPv4/MAC qos aces:              0.5K
number of IPv4/MAC security aces:         0.5K
number of IPv6 policy based routing aces: 0.25K
number of IPv6 qos aces:                  0.5K
number of IPv6 security aces:             0.5K
```

```
Cat3k#
```

1st day

IPv6アドレス設定

- 構成図をもとにIPv6アドレスを設定
 - 2001:db8:a<area>00:<num>::1(or2)/64
 - fe80::<area>:<num>:1(or2)
 - 上位NW側、若番の機器側に XXXX::1/64 をアサイン、
 - 下位NW側、老番の機器側に XXXX::2/64 をアサイン
 - Gi*/3以外のI/FではRAを止める
 - Loopback 0に 2001:db8:a<area>00::1~4/128をアサイン (例:2001:db8:a100::1/128)



(例) 受講番号①~④の場合

※グループ毎にArea番号が異なっているため、2001:db8:a<X>00 のXの数字を変える

設定例

```
interface GigabitEthernet 1/2
ipv6 address FE80::1:1:1 link-local
ipv6 address 2001:db8:a100:1::1
ipv6 nd ra suppress
```

IPv6アドレス設定

IPv6基本設定

```
(config)# ipv6 unicast-routing
```

IPv6ルーティングを行うために必要

IPv6 I/F設定

```
(config)# interface GigabitEthernet */*  
(config-if)# ipv6 enable  
(config-if)# ipv6 address FE80:::<num>:1(2) link-local  
(config-if)# ipv6 address 2001:db8:a<area>00:<num>::1(2)/64  
(config-if)# ipv6 nd ra suppress
```

IPv6を有効にする(明示的なアドレス設定があれば不要)
リンクローカルアドレスを手動で設定
グローバルアドレスを設定
RAを抑制(Gi*/3では不要)

IPv6 Loopback I/F設定

```
(config)# interface Loopback 0  
(config-if)# ipv6 enable  
(config-if)# ipv6 address 2001:db8:a<area>00::1~4/128
```

IPv6を有効にする(明示的なアドレス設定があれば不要)
Loopbackにグローバルアドレスを設定

NDPの動作確認

- 対向のアドレスにPingが通ることを確認
 - (例) ping ipv6 2001:db8:a100:1::1
- show コマンドでの確認
 - show ipv6 neighbor

```
IPv6 Address                               Age Link-layer Addr State Interface
2001:db8:0:12::2                           0 0012.f29a.8360 REACH Po12
2001:db8:0:11::2                           0 0012.f29a.b350 REACH Po11
FE80::12:2                                  0 0012.f29a.8360 REACH Po12
FE80::11:2                                  0 0012.f29a.b350 STALE Po11
```

- show ipv6 interface brief
 - インタフェースに割り当てられているIPv6アドレスを確認



IPv6アドレス設定の確認

- RAによりPCに2001:db8:a<area>00:5(6)::/64がアサインされていることを確認
 - ipconfig
- IPv6アドレスでもtelnetログインできることを確認
 - TeraTermにルータのGi*/3のIPv6アドレスを入力
 - IPv6アドレスは”[]”で囲む必要があります
- (参考)キャプチャによる確認
 - WireSharkを使い、Gi*/3上でやり取りされるIPv6トラフィックを確認
 - 他の特定I/FのトラフィックをGi*/3に吐き出させる方法
 - monitor session 1 source int gi x/x both
 - monitor session 1 destination int gi */3



パケットフィルタの設定

- 下記を始点アドレスとするIPv6パケットをフィルタする
 - 予約済みアドレス ::/8
 - サイトローカルアドレス fec0::/10
 - ユニークローカルアドレス fc00::/7
 - ドキュメントアドレス 2001:db8::/32

※ただしICMPv6パケットは全て許可する
対象I/FはGi*/1 (アップリンクI/F)

```
ipv6 access-list FILTER
  permit icmp any any
  deny ipv6 ::/8 any
  deny ipv6 FEC0::/10 any
  deny ipv6 FC00::/7 any
  deny ipv6 2001:DB8::/32 any
  permit ipv6 any any

interface GigabitEthernet 1/1
  ipv6 traffic-filter FILTER in
```



パケットフィルタ設定

IPv6 Access-list設定

```
(config)# ipv6 access-list FILTER
(config-ipv6-acl)# permit icmp any any
(config-ipv6-acl)# deny ipv6 ::/8 any
(config-ipv6-acl)# deny ipv6 FEC0::/10 any
(config-ipv6-acl)# deny ipv6 FC00::/7 any
(config-ipv6-acl)# deny ipv6 2001:DB8::/32 any
(config-ipv6-acl)# permit ipv6 any any
```

IPv6 Access-listの名前は”FILTER”
ICMPv6は全てpermit
予約済みアドレスのsrcパケットをdeny
サイトローカルアドレスのsrcパケットをdeny
ユニークローカルアドレスのsrcパケットをdeny
ドキュメントアドレスのsrcパケットをdeny
全IPv6パケットをpermit

IPv6 Access-list適用

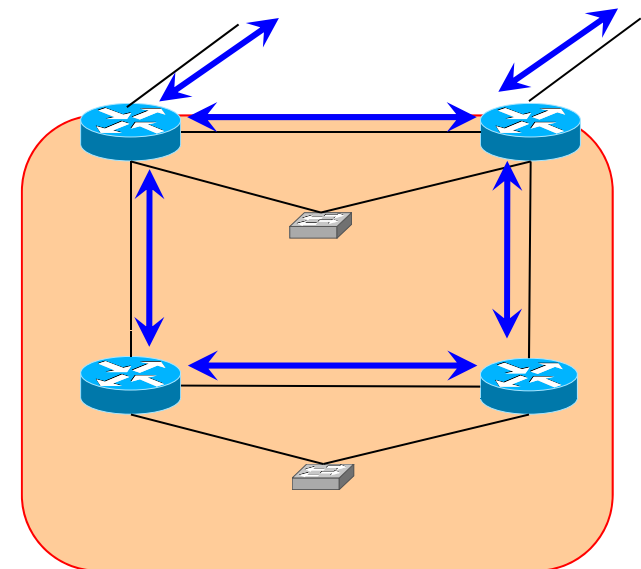
```
(config)# interface GigabitEthernet */1
(config-if)# ipv6 traffic-filter FILTER in
```

IPv6 Access-listをI/Fに適用

2nd day

OSPFv3設定

- 各機器同士でOSPFv3セッションを張る
- ネットワークタイプはPoint-to-Point
- costは500
- プロセスIDは1
- router-idは10.0.0.x (xは座席番号)





OSPFv3設定

OSPFv3基本設定

```
(config)# ipv6 router ospf 1  
(config-rtr)# router-id 10.0.0.x  
(config-rtr)# log-adjacency-changes detail
```

本実習ではプロセスIDは全て1とする
ルータIDを設定(xは席番号)
詳細なstate changeのlogを出力する

OSPFv3を有効にするI/Fに対して下記を設定

```
(config)# interface GigabitEthernet x/x  
(config-if)# ipv6 ospf network point-to-point  
(config-if)# ipv6 ospf cost 500  
(config-if)# ipv6 ospf 1 area x  
(config-if)# ipv6 ospf authentication ipsec spi xxx md5|sha1 xxx
```

ネットワークタイプをp-to-pにする
costを500に固定する
I/Fをエリアxに所属させる

Catalyst3750/3550は現時点でIPv6 OSPF
Authenticationをサポートしていない

Loopback0に対してもOSPFv3を有効化

```
(config)# interface Loopback 0  
(config-if)# ipv6 ospf 1 area x
```

Loopbackが所属するエリアを指定

OSPFv3設定確認

- show ipv6 ospf neighbor
- show ipv6 ospf database
- show ipv6 route ospf

対向のRouter-IDが見えていること

```
# show ipv6 ospf neighbor
Neighbor ID    Pri   State           Dead Time   Interface ID  Interface
a.a.a.a       1     FULL/-         00:00:34   97           GigabitEthernetx/x
b.b.b.b       1     FULL/-         00:00:34   41           GigabitEthernety/y
```

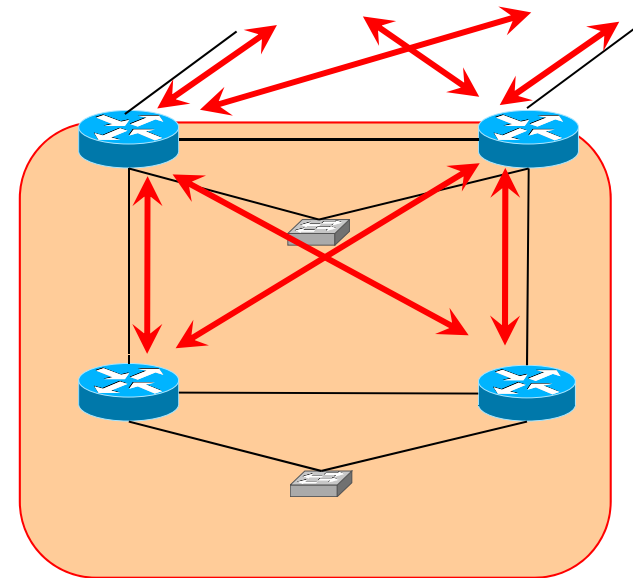
Next-hopがリンクローカルアドレスになっていること

```
# show ipv6 route ospf
IPv6 Routing Table - Default - 20 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001:db8:0:1::/64 [110/2]
    via FE80::11:2, Port-channel11
O   2001:db8:0:2::/64 [110/2]
    via FE80::12:2, Port-channel12
O   2001:db8:0:10::/64 [110/2]
    via FE80::12:2, Port-channel12
    via FE80::11:2, Port-channel11
```



BGP4+設定

- 上位ルータ、下位ルータのLoopbackアドレスでiBGPセッションを張る
- AS番号は65535
- update-sourceはLoopback0
- 上位ルータは下位ルータからのルートリフレクタになる
- send-communityをenableにする
- router-idは10.0.0.x(xは座席番号)
- PCセグメント(Gi*/3)のprefixをBGPで配送
- Passwordはipv6





BGP4+設定

BGP4+基本設定

```
(config)# router bgp 65535
(config-router)# bgp router-id 10.0.0.x
(config-router)# address-family ipv6 unicast
(config-router-af)# network 2001:db8:a<area>00:5(6)::/64
(config-router-af)# neighbor 2001:db8:a<area>00::x remote-as 65535
(config-router-af)# neighbor 2001:db8:a<area>00::x password ipv6
(config-router-af)# neighbor 2001:db8:a<area>00::x update-source Loopback0
(config-router-af)# neighbor 2001:db8:a<area>00::x send-community
```

AS番号は65535とする
ルータIDを設定(xは席番号)
IPv6 Address Familyを指定
PC向けprefixをBGPで配送
対向ASも65535
passwordを設定
update-srcをLoop0に設定
send-communityをenable

ルートリフレクタ設定

```
(config)# router bgp 65535
(config-router)# address-family ipv6 unicast
(config-router-af)# neighbor 2001:db8:a<area>00::x route-reflector-client 配下のルータに対して設定
```

Peer-groupを作成
する方法も勿論可能



BGP4+設定確認

- show bgp ipv6 unicast summary
- show bgp ipv6 unicast

```
# show bgp ipv6 unicast summary ルータID
BGP router identifier 10.0.0.1, local AS number 65535 自AS番号
BGP table version is 11, main routing table version 11
3 network entries using 423 bytes of memory
4 path entries using 304 bytes of memory
12/3 BGP path/bestpath attribute entries using 1920 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
1 BGP community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2695 total bytes of memory
BGP activity 33/10 prefixes, 135/94 paths, scan interval 60 secs
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
2001:db8:0:11::2	4	65535	217778	196026	11	0	0	2w5d	2
2001:db8:0:12::2	4	65535	216978	195375	11	0	0	3w1d	1

NeighborのIPv6アドレス

NeighborのAS番号



BGP4+経路制御

- 上位ルータからの最大受信prefix数を10000に制限する
- 下記の不要prefixの受信をrejectする
 - 予約済み Prefix `::/8` or longer
 - リンクローカルアドレス `fe80::/10` or longer
 - サイトローカルアドレス `fec0::/10` or longer
 - ユニークローカルアドレス `fc00::/7` or longer
 - マルチキャストアドレス `ff00::/8` or longer
 - ドキュメントアドレス `2001:db8::/32` or longer



BGP4+経路制御

IPv6 prefix-list

```
(config)# ipv6 prefix-list DROP-LIST seq 5 deny ::/8 le 128
(config)# ipv6 prefix-list DROP-LIST seq 10 deny FE80::/10 le 128
(config)# ipv6 prefix-list DROP-LIST seq 15 deny FEC0::/10 le 128
(config)# ipv6 prefix-list DROP-LIST seq 20 deny FC00::/7 le 128
(config)# ipv6 prefix-list DROP-LIST seq 25 deny FF00::/8 le 128
(config)# ipv6 prefix-list DROP-LIST seq 30 deny 2001:DB8::/32 le 128
(config)# ipv6 prefix-list DROP-LIST seq 100 permit ::/0 le 128
```

不要prefixに対してprefix-listを作成

上記以外は全て許可するためpermit anyを設定

BGPの経路制御設定

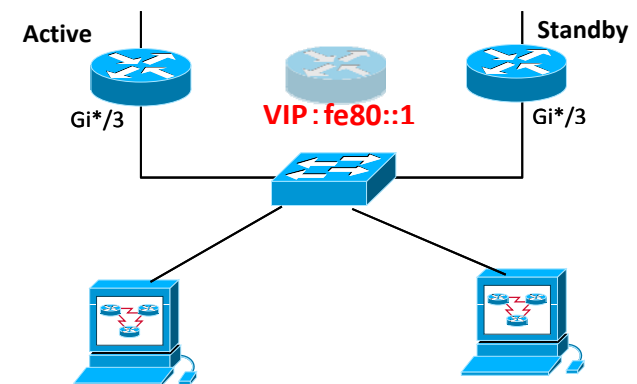
```
(config)# router-bgp 65535
(config-router)# address-family ipv6 unicast
(config-router-af)# neighbor 2001:db8:a<area>00::x maximum-prefix 10000 最大受信prefix数を10000に制限
(config-router-af)# neighbor 2001:db8:a<area>00::x prefix-list DROP-LIST in prefix-listを設定
(config-route-map)# end
# clear bgp ipv6 unicast X:X:X:X::X soft in
```

soft resetにより上記を適用



HSRPv2設定

- Gi*/3に対してHSRPv2設定を行う
- グループ番号は1
- VIPはfe80::1
- 若番がMasterとなるようにする
- 認証は平文で"ipv6"
- Timerはhelloが1秒、deadが3秒
- 自分より高いpriorityのルータが現れたらMasterを委譲する





HSRPv2設定

HSRPv2設定

```
(config)# interface GigabitEthernet */3
(config-if)# standby version 2
(config-if)# standby 1 ipv6 FE80::1
(config-if)# standby 1 timers 1 3
(config-if)# standby 1 priority 105
(config-if)# standby 1 preempt
(config-if)# standby 1 authentication text ipv6
```

HSRPv2を設定するためにversion 2を指定
VIP(リンクローカルアドレス)を設定
helloを1秒間隔、dead timerを3秒に設定
Master側のPriorityをdefaultの100から105に変更
自分より高いPriorityを持つルータが現れたらMasterを委譲
認証パスワードを平文で設定



HSRPv2設定確認

- show standby brief
- show standby

```
# show standby brief
                                P indicates configured to preempt.
                                |
Interface   Grp  Pri P State   Active      Standby      Virtual IP
Gi2/44      1    105 P Active  local       X:X:X:XX     FE80::1

# show standby
GigabitEthernet2/44 - Group 1 (version 2)
  State is Active
    2 state changes, last state change 00:00:45
  Virtual IP address is FE80::1
  Active virtual MAC address is 0005.73a0.0001
  Local virtual MAC address is 0005.73a0.0001 (v2 IPv6 default)
  Hello time 1 sec, hold time 3 sec
  Next hello sent in 0.672 secs
  Authentication text, string "ipv6"
  Preemption enabled
  Active router is local
  Standby router is X:X:X:XX
  Priority 105 (configured 105)
  Track interface GigabitEthernet2/1 state Up decrement 10
  Group name is "hsrp-Gi2/44-1" (default)
```



冗長試験

- OSPF、BGPの迂回確認
 - 片側のアップリンク回線(Gi*/1)を抜いても通信が途絶えないことを確認
 - ping 2001:db8:2000:FFFF::1
 - tracert 2001:db8:2000:FFFF::1
- HSRPv2の冗長確認
 - Master側のGi*/3を抜いても通信が途絶えないことを確認
 - ping 2001:db8:2000:FFFF::1
 - tracert 2001:db8:2000:FFFF::1
 - ipconfig



SNMP , Syslog確認

- 作業中に発生したSNMP Trap、Syslogを確認
- 前の画面をご覧ください。