SDCC資料番号 OWNサ開部 300-100-140-20230716-01

B解除済
会本部

SDCC ONW
マネジメント網設計
第３．３版

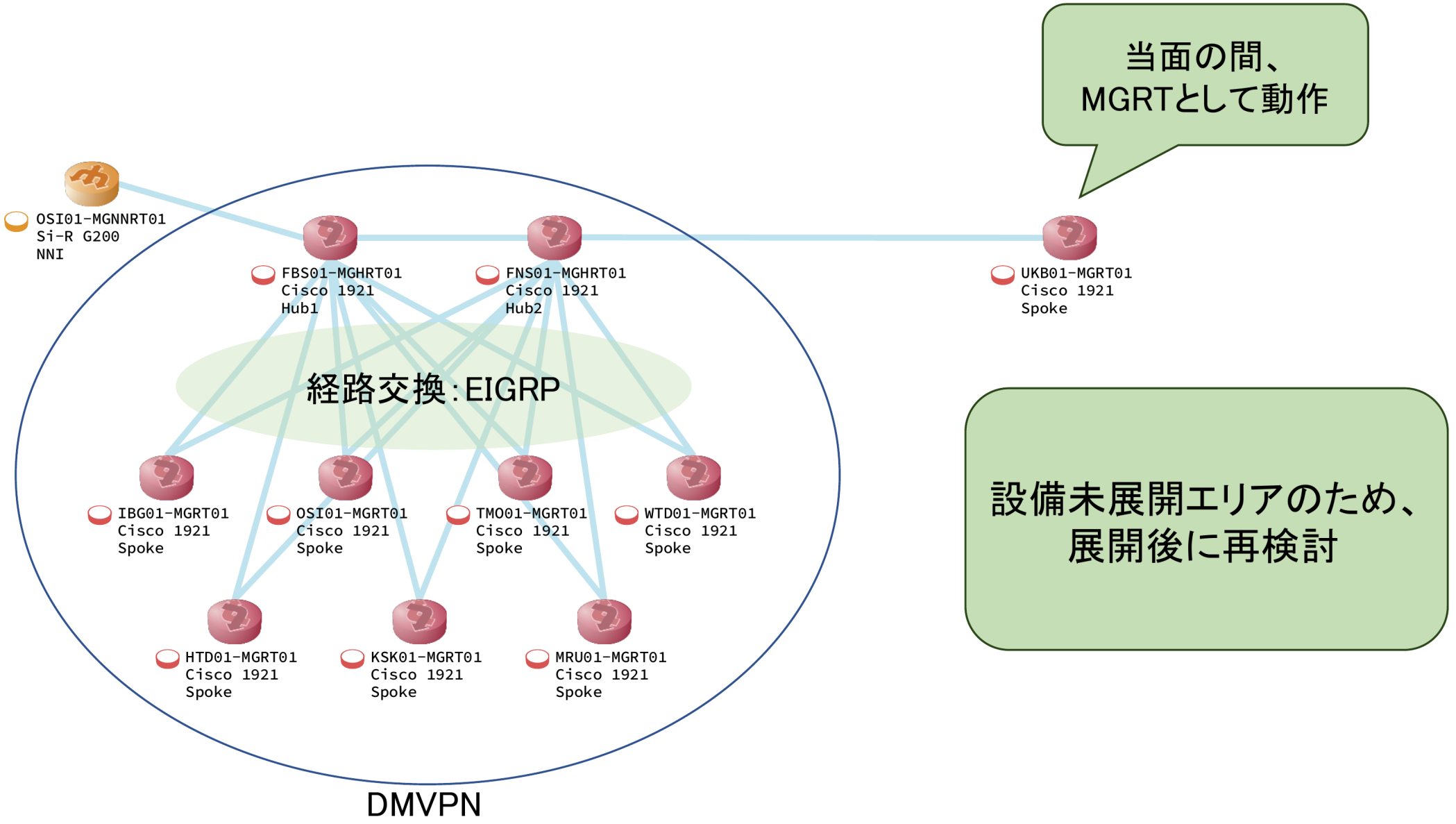
島根データセンター友の会
SDCC ONW本部
サービス開発部

更新履歴

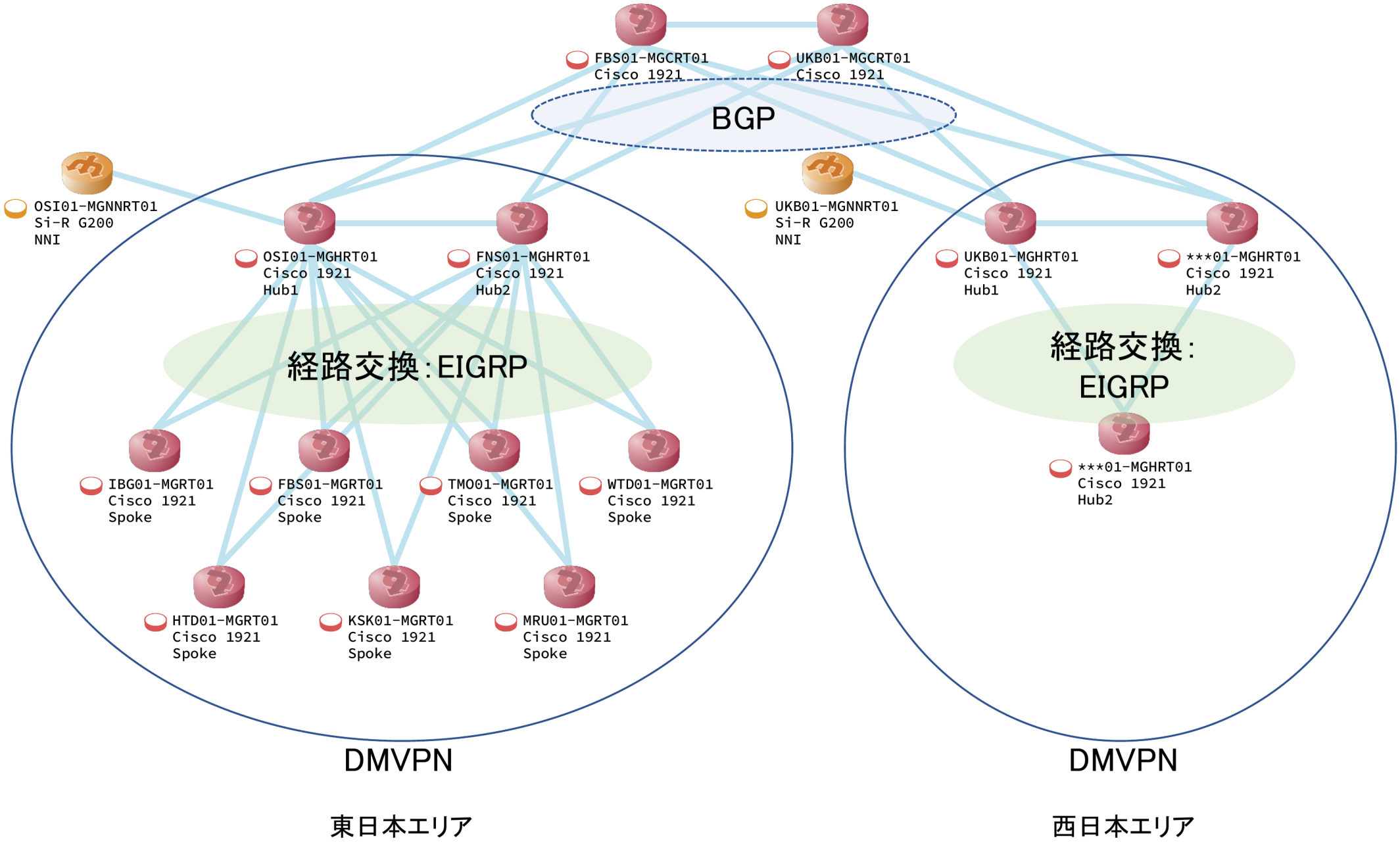
- ３．０版　　第二世代マネジメント網設計から引き継ぎ
- ３．１版　　L2スイッチ導入、MGRTの冗長化検討
- ３．２版　　網構成の変更、IPアドレッシングポリシの変更
- ３．３版　　網監視装置、アドレス解決サーバ等の構築

NW編

網構成概要（西日本エリア未展開時）



網構成概要(西日本エリア展開時)



設備名称



Management Core Router

ブロックごとのMGHRTの通信を集約し、MGHRT間の転送を担う集約ルーター。
本ルーターが最も上位。



Management Hub Router

ブロック内のルーター間を動的に経路制御するルーター。
MGRTとセッション確立後は、配下のルーター間の経路を自動構築する。



Management Router

各拠点に配備するルーター。
拠点内の通信を集約し、EIGRPにて経路広報する。



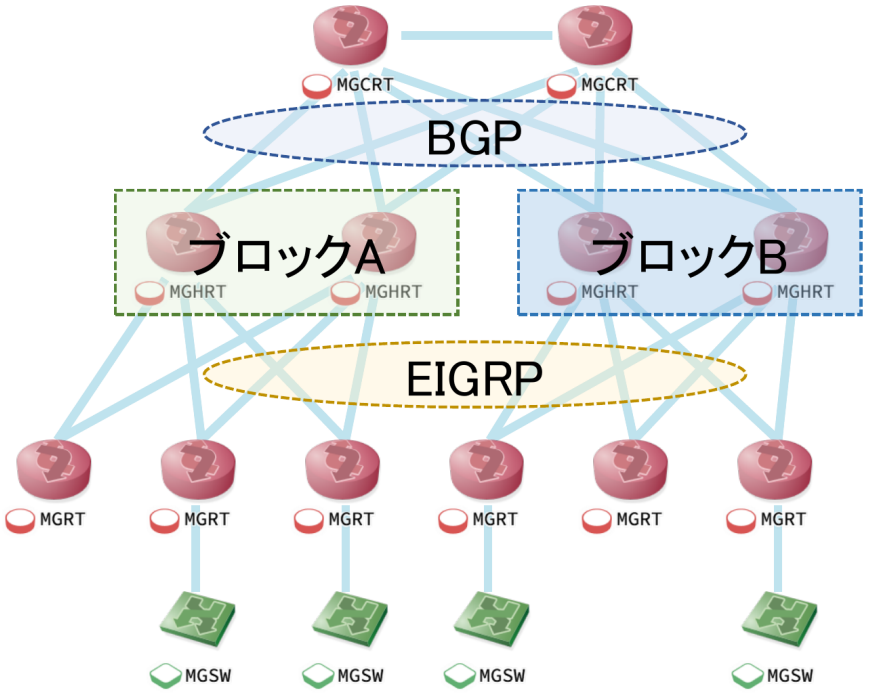
Management Switch

拠点内の通信を集約するスイッチ。



Management NNI※ Router

マネジメント網と外部の網を相互接続する際に設置するルーター。
主なものとして、インターネットへのNATを実施するルーターなどがある。



※Network-Network Interfaceのこと。ネットワーク間を相互接続する。

マネジメント網概要

- SDCCが所有する設備の管理ネットワークを既設NWと独立して構築することで、障害発生時等における迅速な対応を可能にする。
- 本ネットワークは物理NW設備の管理を専らの目的とし、それ以外の通信を可能な限り行わない。また、接続する機器は慎重に選定する。
- Cisco 1921を採用し、HubをFQDNで指定するDMVPNにより構築を行い、EIGRPにより網内の経路交換を行う。新規拠点を構築する場合は、DMVPN/EIGRPに参加するのみで集約拠点等の変更作業を不要とした。
- 利用者が本NWに接続する際は設定を導入したC1921を送付する形をとる。

命名規則等

- VPN装置名称
  - 削除）
  - ドメインサフィックスは 削除
- トンネル終端IF DDNSアドレス
  - NGN接続IF：削除
    - （例：削除）
  - MCS（移動体通信）接続IF：削除
    - （例：削除）

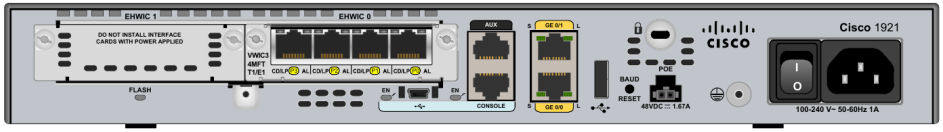
拠点名	拠点符号	拠点番号
削除		

【参考】拠点名、符号、管理番号

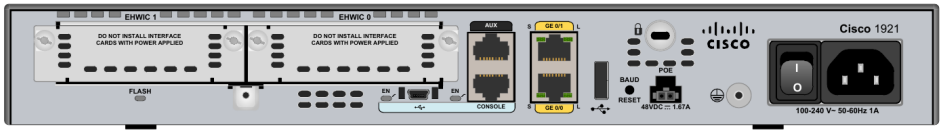
概要 –物理装置–

MGCRT　MGHRT　MGRT

- SDCC物理設備がある拠点向け装置
  - 装置概要図を右に示す。



  - すべての拠点に共通し、C1921を配布するが、SDCC物理設備を有する拠点にはスイッチポートを最大4ポート搭載することができることを生かし、本装置を直接L2接続できるように構成する。
  - 下部MGSWへの渡りポートは共通して0/0/0を利用する。
  - ポートの設定等
    - GE0/0にフレッツNGNを接続（ひかり電話有無は問わない。）。NGN以外の場合は応相談。IPv6の接続性があればどこでも利用可能。クロス品目については現状非対応。
    - GE0/1は利用しない。
- SDCC物理設備がない拠点向け設備
  - 装置概要図を右に示す。

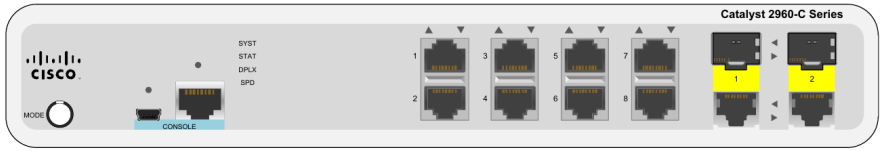


  - ポートの設定等
    - GE0/0にフレッツNGNを接続（ひかり電話有無は問わない。）。NGN以外の場合は応相談。IPv6の接続性があればどこでも利用可能。クロス品目については現状非対応。
    - GE0/1にPC等を接続する。DHCP/RA/DHCPv6等によりアドレスを配布する。
    - スイッチポートが付属する設備はGE0/1ではなくスイッチポートに当該設定を割り当てる。

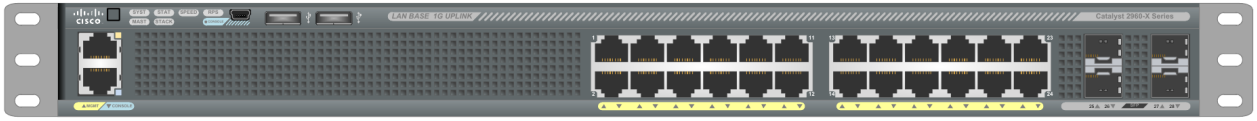
概要 –物理装置–

MGSW

- MGRT下部スイッチ構成（小規模拠点向け）
  - 装置概要図を右に示す。
  - FE0/1～8ポートはPoE対応Fast Ethernet（100Mbps）
  - GE0/1ポートがMGRTに接続される。



- MGRT下部スイッチ構成（大規模拠点向け）
  - 装置概要図を右に示す。



  - GE1/0/23ポートがMGRTに接続される。

採番等

- VLAN ID

削除

採番等

- 拠点番号
  - SDCC BBが設置してる拠点は1～20。
  - SDCC BB未設置拠点は21～50。
- IPv4/IPv6の払い出しの際は下記表を参考に読み替える。

SDCC管理拠点

拠点番号	v4拠点番号	v6拠点番号
1	削除	
2		
3		
4		
5		
6		
7		
8		
9		
10		

拠点番号	v4拠点番号	v6拠点番号
11	削除	
12		
13		
14		
15		
16		
17		
18		
19		
20		

SDCC管理外拠点

拠点番号	v4拠点番号	v6拠点番号
21	削除	
22		
23		
24		
25		
26		
27		
28		
29		
30		

採番等

- VLAN ID
  - SDCC設備がある拠点
    - MGMT
    - INT

削除

- IPv4アドレス
  - 管理網全体
    - 10.250.0.0/16
  - 装置/利用者用アドレス 削除.<v4拠点番号>.0/22
    - DHCP払出しは第4 /24ブロックから。
  - SDCC管理外拠点は 削除.<v4拠点番号>.0/24
  - DMVPN内部用 172.16.20.<拠点番号>
- IPv6アドレス
  - 装置/利用者用アドレス 2001:削除:<v6拠点番号>::/58
    - DHCPv6払い出しは2001:削除:<v6拠点番号>+3::/64
    - SDCC設備がない拠点は/64
  - DMVPN内部用 2001:削除::<IPv4拠点番号>::/64

例

ルーター	削除	.0.0	2001	/64
スイッチ		.1.0	2001	/64
その他		.2.0	2001	/64
DHCP		.3.0	2001	/64

削除

終端アドレス変更への追従

- Hubサイトについて
  - i.open.ad.jpのDDNSに登録
- Spokeサイトについて
  - FQDNによりNBMAアドレスの追従が可能。
  - （ただしバグあり）

IPv6 DMVPN構築の注意点

- IOS15以降、DMVPNのHUB、NBMAアドレスをFQDN指定できるようになった。
  - https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-conf-using-fqdn.html
- FQDN対象がIPv6アドレスの場合、バグがあるので注意。
  - FQDNのアドレスがIPv6の場合、名前解決に失敗する。
  - Cisco 1921 Version 15.8(3)M5 にて再現を確認。TACに確認中。
- 対策方法
  - その他のプロセスで名前解決できた場合、そのキャッシュを利用している？様子で、トンネルが開通する。
  - 下記設定を投入、1分ごとにHubサイトのアドレスを名前解決する。
  - （一度名前解決できれば問題ないが、変更に追従するため。）

コマンド例　ipv6 nhrp nhs [hub ipv6 address(2001::1)] nbma ipv6.example.com multicast

修正設定例：

```
event manager applet DMVPN-NBMA-Address-Resolver
 event timer cron name DMVPN_NBMA_ADDRESS_RESOLVE_PING cron-entry "*
* * * * *" maxrun 30
 action 10 cli command "enable"
 action 15 cli command "ping ipv6                                    "
 action 20 cli command "ping ipv6                                    "
 action 90 cli command "end"
 action 91 cli command "exit"
```

削除

IPv4/v6 over IPv6 のDMVPN構築例

- Hubサイト

```
interface Tunnel0
 ip address 172.16.20.x 255.255.255.0
 no ip redirects
 ip mtu 1360
 no ip split-horizon eigrp 1000
 ip nhrp authentication <auth-key>
 ip nhrp network-id 削除
 ip nhrp holdtime 15
 ip nhrp nhs 172.16.20.y nbma huby.fqdn.example.com multicast
 ip nhrp redirect
 ip tcp adjust-mss 1320
 ipv6 address FE80::A00x link-local
 ipv6 address 2001 削除 ::x/64
 ipv6 eigrp 1000
 no ipv6 split-horizon eigrp 1000
 ipv6 nhrp authentication <auth-key>
 ipv6 nhrp network-id 削除
 ipv6 nhrp holdtime 15
 ipv6 nhrp nhs 2001: 削除 :y nbma huby.fqdn.example.com multicast
 ipv6 nhrp redirect
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint ipv6
 tunnel protection ipsec profile mgvpnfnt
```

- Spokeサイト

```
interface Tunnel0
 ip address 172.16.20.z 255.255.255.0
 no ip redirects
 ip mtu 1360
 ip nhrp authentication <auth-key>
 ip nhrp network-id 削除
 ip nhrp holdtime 15
 ip nhrp nhs 172.16.20.x nbma hubx.fqdn.example.com multicast
 ip nhrp nhs 172.16.20.y nbma huby.fqdn.example.com multicast
 ip tcp adjust-mss 1320
 ipv6 address FE80::A00z link-local
 ipv6 address 2001 削除 ::z/64
 ipv6 eigrp 1000
 ipv6 nhrp authentication <aut-key>
 ipv6 nhrp network-id 削除
 ipv6 nhrp holdtime 15
 ipv6 nhrp nhs 2001:DF4:1780:F00::x nbma hubx.fqdn.example.com multicast
 ipv6 nhrp nhs 2001:DF4:1780:F00::y nbma huby.fqdn.example.com multicast
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint ipv6
 tunnel protection ipsec profile mgvpnfnt
```

- 共通設定（IPsec）

```
crypto isakmp policy 100
 encr aes 256
 hash sha512
 authentication pre-share
 group 24
crypto isakmp key <pre-shared-key> address ipv6 ::/0
crypto isakmp invalid-spi-recovery
!
crypto ipsec transform-set dmvpnts001 esp-aes esp-sha512-hmac
 mode transport
!
crypto ipsec profile mgvpnfnt
 set transform-set dmvpnts001
!
crypto identity 削除
```

利用者/装置用 IFのアドレス設定

- スイッチポート有りの場合

```
ip dhcp pool SDCC-MGMT-Local-Pool0
 network 削除
 default-router 削除
 domain-name
 dns-server 1 削除

ip dhcp excluded-address 削除

ipv6 dhcp pool SDCC-MGMT-Localv6-Pool0
 address prefix 削除 x::/64 lifetime 604800 86400
 domain-name 削除

interface range GigabitEthernet0/0/0-4
 switchport access vlan 100
 switchport mode access
 no ip address

interface Vlan100
 ip address 削除
 ipv6 address FE80::1 link-local
 ipv6 address 削除 ::1/58
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 eigrp 1000
 ipv6 dhcp server SDCC-MGMT-Localv6-Pool0
```

EIGRPの設定

- Hub側（その他のTunnel設定は導入済みとする。）

```
interface Tunnel0
 no ip redirects
 no ip next-hop-self eigrp 1000
 no ip split-horizon eigrp
 no ipv6 split-horizon eigrp 1000
```

- 共通設定

```
router eigrp 1000
 network
 network

ipv6 router eigrp 1000
 eigrp router-id

interface Tunnel0
 ipv6 eigrp 1000

interface Vlan103
 ipv6 eigrp 1000
```

削除

削除

DDNS向け設定

- Hub拠点は必須、Spoke拠点は任意。

```
ip name-server 2001:4860:4860::8888
ip name-server 2606:4700:4700::1111

event manager applet OPEN-DDNS-GE0-INTF-Updater
 event timer cron name OPEN_DDNS_ADDRESS_UPDATER_PING cron-entry "* * * * *"
 action 1.0 cli command "enable"
 action 2.0 cli command “ping ipv6 <update専用識別子>.i.open.ad.jp"

event manager applet OPEN-DDNS-GE1-INTF-Updater
 event timer cron name OPEN_DDNS_ADDRESS_UPDATER_PING cron-entry "* * * * *"
 action 1.0 cli command "enable"
 action 2.0 cli command "ping vrf mcs-intf ipv6 <update専用識別子>.i.open.ad.jp"
```

共通設定部分

```
!MGRT向け共通設定

no service pad
no service dhcp
no cdp run
no service config
no ip bootp server
no ip http server
no ip http secure-server
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service sequence-numbers
logging buffered 512000
clock timezone JST 9 0
ip domain retry 5
ip domain timeout 1
ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
```

削除

```
boot system flash flash:c1900-universalk9-mz.SPA.158-3.M5.bin

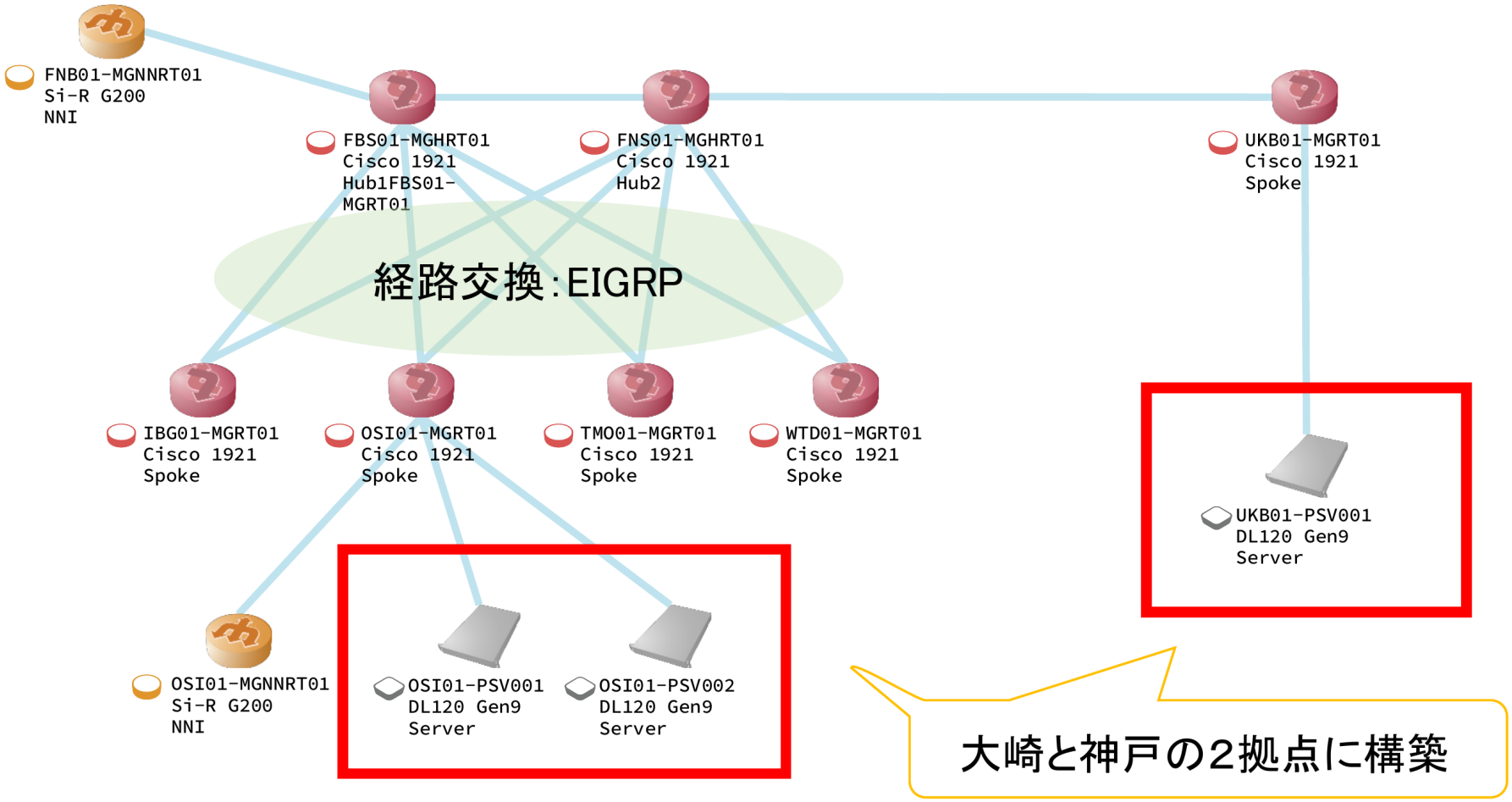
ip name-server 2001:4860:4860::8888
ip name-server 2606:4700:4700::1111
```

SSH接続・認証情報

```
line vty 0 4
 login
 transport input ssh
line vty 5 50
 login
 transport input none
```

サーバ編

監視用サーバー拠点


FNB01-MGNNRT01
Si-R G200
NNI
FBS01-MGHRT01
Cisco 1921
Hub1FBS01-
MGRT01
FNS01-MGHRT01
Cisco 1921
Hub2
UKB01-MGRT01
Cisco 1921
Spoke
経路交換：EIGRP
IBG01-MGRT01
Cisco 1921
Spoke
OSI01-MGRT01
Cisco 1921
Spoke
TMO01-MGRT01
Cisco 1921
Spoke
WTD01-MGRT01
Cisco 1921
Spoke
UKB01-PSV001
DL120 Gen9
Server
OSI01-MGNNRT01
Si-R G200
NNI
OSI01-PSV001
DL120 Gen9
Server
OSI01-PSV002
DL120 Gen9
Server
大崎と神戸の2拠点に構築

監視基盤向けサービス一覧

- DNSサーバ
- NTPサーバ
- IPAMサーバ
- SNMP/syslog情報収集サーバ（Zabbix）

仮想化基盤NWについて

既設仮想化基盤上に、管理用サーバを構築する。

SDCC資料番号300-100-130-20220912-01
サーバの展開計画と設備概要　より

大崎 削除

ビルの役割：東京エリア主系
サーバの種類：通常系、監視系

DL120 Gen9 通常系
DL120 Gen9 監視系（削除、Zabbix）

川崎 削除

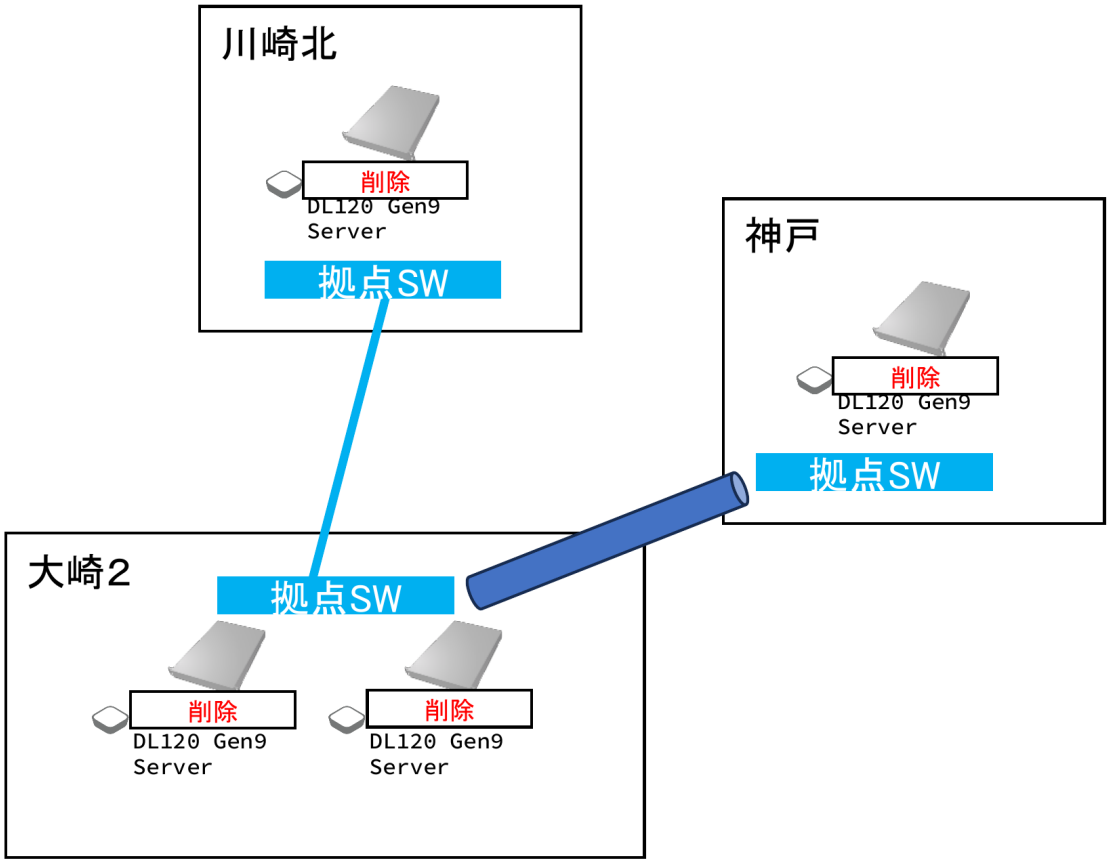
ビルの役割：東京エリア激甚対応
サーバの種類：待機系、監視系

DL120 Gen9 待機系
DL120 Gen9 監視系（削除）

神戸 削除

ビルの役割：大阪エリア主系
サーバの種類：待機系、監視系

DL120 Gen9 通常系



DNSサーバについて

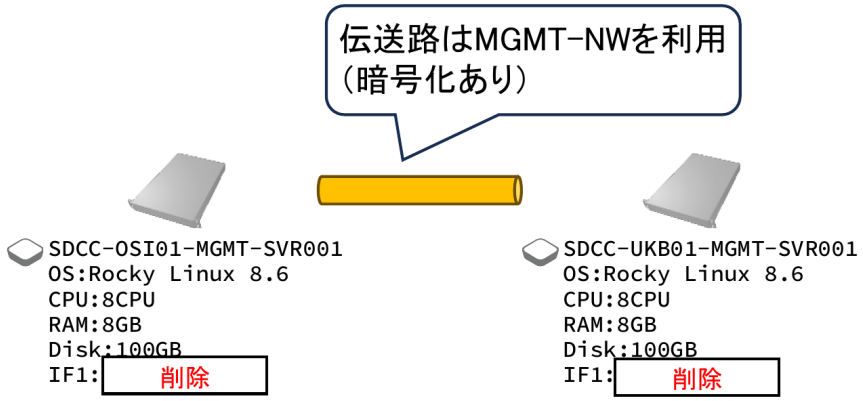
- 構成
  - OSI01とUKB01にそれぞれVMを展開
  - OSI01側をPrimary/UKB01側をSecondaryで同期
  - インターネット接続性：有

- RockyLinux 8.9
- PowerDNS 4.8.x
- MySQL（Backend） 8.x(latest)
- PowerDNS-Admin 0.4.1
- Nodejs 18.x
- Python 3.10

- 管理方法
  - ドメイン追加・確認 http://dns01.osi01.
  - 運用状況確認 http://dns01.osi01.
  - ドメイン追加・確認（UKB01） http://dns01.ukb01
  - 運用状況確認（UKB01） http://dns01.ukb01

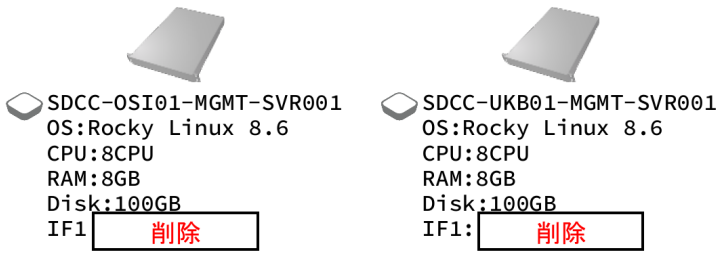
削除

  - IPアクセス制限あり、AXFR/notifyあり
  - ドメインの追加についてはPrimary側であるOSI01からのみ実施可能。



NTPサーバについて

- 構成
  - OSI01とUKB01にそれぞれVMを展開
  - chronyを使用。同期先は下記の通り
    - server ntp.nict.jp iburst
    - server ntp1.jst.mfeed.ad.jp iburst
    - server ntp2.jst.mfeed.ad.jp iburst
  - アクセス制限あり（削除）
  - インターネット接続性：有



IPAMサーバについて

- 構成
  - svr001.osi01[削除]上に構築
- アクセス方法
  - https://ipam01.[削除]/
- 備考
  - /var/www/html に直接配置
  - pingCheck discoveryCheckのcronは↓

```
vi /etc/cron.d/phpipam

*/15 *  *  *  * apache /bin/php /var/www/html/functions/scripts/pingCheck.php
*/15 *  *  *  * apache /bin/php /var/www/html/functions/scripts/discoveryCheck.php
```

- RockyLinux 8.9
- Apache 2.4.x(latest)
- PHP 8.3
- phpIPAM 1.6.0
- MySQL（Backend） 8.x(latest)



SDCC-OSI01-MGMT-SVR001
OS:Rocky Linux 8.6
CPU:8CPU
RAM:8GB
Disk:100GB
IF1:[削除]

SNMP情報収集サーバ(Zabbix)について

- 構成
  - zbx001.osi01[削除]上に構築
- アクセス方法
  - http://zbx001.osi01.[削除]/

- RockyLinux 8.9
- Zabbix 6.0.x(Stable)
- nginx 1.24.0
- MySQL(Backend) 8.x(latest)



Syslog情報収集サーバについて

- 構成
  - rsyslog：svr002.
  - Grafana：svr003
- アクセス方法
  - ssh://svr002.ukb01.
  - http://grfn001.osi01 （可視化済）
- 備考
  - NW機器はlocal4で区分
  - /var/log/rsyslog/ 配下にlog集積

