

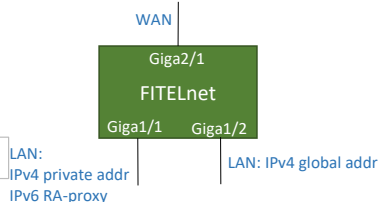
NTTコミュニケーションズ社「OCNバーチャルコネクトサービス (IPoE)」を利用するための設定例

対象装置：FITELnet F70/F71/F220/F221/F225/F310

ケース3：固定IP8

| 対応するMAP-E構成 |
|---------------|
| HGWあり/ひかり電話あり |
| HGWあり/ひかり電話なし |
| HGWなし/ひかり電話なし |

(光クロス非対応)



※ログインID/Passwordは“test”/“test”です。

| 設定例 | 補足 |
|--|---|
| 1 access-list 100 permit ip any host 192.0.2.2 | IPv4アクセスリスト (グローバルアドレス宛の通信を許可) ※お客様の環境に合わせて設定してください。 |
| 2 access-list 100 permit ip any host 192.0.2.3 | IPv4アクセスリスト (グローバルアドレス宛の通信を許可) ※お客様の環境に合わせて設定してください。 |
| 3 access-list 100 permit ip any host 192.0.2.4 | IPv4アクセスリスト (グローバルアドレス宛の通信を許可) ※お客様の環境に合わせて設定してください。 |
| 4 access-list 100 permit ip any host 192.0.2.5 | IPv4アクセスリスト (グローバルアドレス宛の通信を許可) ※お客様の環境に合わせて設定してください。 |
| 5 access-list 109 deny ip any any | IPv4アクセスリスト (全拒否) |
| 6 access-list 110 spi ip any any | IPv4アクセスリスト (SPI) |
| 7 access-list 4000 permit icmp6 any any neighbor-advertisement | IPv6アクセスリスト (NA許可) |
| 8 access-list 4000 permit icmp6 any any neighbor-solicitation | IPv6アクセスリスト (NS許可) |
| 9 access-list 4000 permit icmp6 any any router-advertisement | IPv6アクセスリスト (RA許可) |
| 10 access-list 4000 permit udp any any eq 546 | IPv6アクセスリスト (DHCPv6許可) |
| 11 access-list 4009 deny ipv6 any any | IPv6アクセスリスト (全拒否) |
| 12 access-list 4010 spi ipv6 any any | IPv6アクセスリスト (SPI) |
| 13 access-list 4100 permit tcp any any eq 53 | IPv6アクセスリスト (IPv6 TCP DNS/ポリシールーティング用) |
| 14 access-list 4100 permit udp any any eq 53 | IPv6アクセスリスト (IPv6 UDP DNS/ポリシールーティング用) |
| 15 access-list 4101 permit tcp any ::1/128 | IPv6アクセスリスト (IPv6 TCP loopback/ポリシールーティング用) |
| 16 access-list 4101 permit udp any ::1/128 | IPv6アクセスリスト (IPv6 UDP loopback/ポリシールーティング用) |
| 17 ! | |
| 18 ip route 0.0.0.0 0.0.0.0 tunnel 1 | IPv4デフォルトルート設定 (デフォルトルートをMAPトンネルに設定) |
| 19 ip name-server ::1 | DNSサーバ設定 (自装置をサーバに設定) |
| 20 ! | |
| 21 ip dhcp server-profile DHCPv4_server | LAN側DHCPv4サーバ設定 (プライベートアドレスをLANに配布) |
| 22 address 192.168.100.2 192.168.100.254 | 配布アドレス設定 |
| 23 lease-time 259200 | DHCPリース期間設定 |
| 24 dns 192.168.100.1 | 配布DNSサーバアドレス設定 |
| 25 gateway 192.168.100.1 | 配布Gatewayアドレス設定 |
| 26 exit | |
| 27 ! | |
| 28 ip nat list 1 192.168.100.0 0.0.0.255 | NAT変換対象アドレス設定 (LAN側 192.168.100.0/24) |
| 29 ip nat default action pass | NAT対象外のパケットを中継する設定 * 送信元アドレス「192.0.2.2-192.0.2.6」を中継するために設定 |
| 30 ip nat port-sharing enable | NATポートシェアリング設定 * 宛先アドレス/ポートの異なる複数のトラフィックに対して同一のNATエントリを適用して、NATのリソースを節約します。 |
| 31 ! | |
| 32 ipv6 dhcp client-profile DHCPv6_client | WAN側DHCPv6クライアント設定 |
| 33 option-request dns-server | DNSサーバ要求設定 |
| 34 option-request dns-server-domain | DNSサーバドメイン要求設定 |
| 35 retries infinity | DHCPメッセージの応答があるまで再送する設定 |
| 36 exit | |
| 37 ! | |
| 38 ipv6 dhcp server-profile DHCPv6_server | LAN側DHCPv6サーバ設定 |
| 39 dns port-channel 20 | WAN側で受信したDNSサーバを配布する設定 |
| 40 domain port-channel 20 | WAN側で受信したドメイン名を配布する設定 |
| 41 exit | |
| 42 ! | |
| 43 event-action 1 | イベントアクション設定 (HGWのSPIフィルタエントリ対策用) |
| 44 event-condition match-all | イベント発生判定のマッチタイプを設定 * 本設定モードのイベントがすべて発生したときにアクションを実施します。 |
| 45 event interface tunnel 1 up | イベント監視 (interface tunnel 1 up) |
| 46 event timer countdown 180 replay | イベント監視 (180秒毎のカウントダウンタイマー) |
| 47 action 1.1 cli exec command ping ##宛先IPアドレス## source 192.168.100.1 repeat 1 | イベント発生時のアクション設定 : HGWのSPIエントリの除去を防ぐための設定 * BRから送信されたパケットのHGWでの破棄を防ぐために、本設定を推奨します。 * interface tunnel 1がupしている場合、180秒に1回、##宛先IPアドレス##に対して、192.168.100.1 (LAN側インタフェースのアドレス)を送信元アドレスとしてPingを送信します。 ※##宛先IPアドレス##はお客様の環境に合わせて設定ください。 |
| 48 exit | |
| 49 ! | |

| | 設定例 | 補足 |
|-----|---|---|
| 50 | ipinip tunnel-profile MAPCE | MAPトンネルプロファイル |
| 51 | profile-mode map-encap option-c | トンネルのプロファイルモードを指定 |
| 52 | map rule-get | MAPルール取得設定 |
| 53 | ipinip fragment pre | ブリフラグメント指定 |
| 54 | exit | |
| 55 | ! | |
| 56 | logging buffer level informational | 装置内部バッファへ出力するログレベルを設定 * show logging bufferで確認出来ます。 |
| 57 | ! | |
| 58 | aaa authentication login default local | ログイン認証方式を指定 local: usernameコマンドで設定したID/パスワードで認証 ※お客様の環境に合わせて設定ください。 |
| 59 | aaa authorization exec default local | Telnetログイン時の許可方式を指定 local: usernameコマンドで設定した特権レベルでログイン許可 ※お客様の環境に合わせて設定ください。 |
| 60 | ! | |
| 61 | username test privilege 15 password 2 \$1\$LAruCQ4A\$T3069M0hXaiNub6xoHNsG1 | 装置のログインID/Password(test /test) ※お客様の環境に合わせて設定ください。 |
| 62 | ! | |
| 63 | hostname FITElnet | hostname設定 |
| 64 | ! | |
| 65 | interface GigaEthernet 1/1 | 物理インターフェース (LAN側) |
| 66 | vlan-id 11 | vlan-id設定 (ポートVLAN) |
| 67 | bridge-group 11 | ブリッジグループ設定 |
| 68 | channel-group 11 | LAN側論理インタフェース (Port-channel) と紐付け |
| 69 | policy-route input DNS-POLICY | LAN側ポリシーリング設定 |
| 70 | exit | |
| 71 | ! | |
| 72 | interface GigaEthernet 1/2 | 物理インターフェース (LAN側) |
| 73 | vlan-id 12 | vlan-id設定 (ポートVLAN) |
| 74 | bridge-group 12 | ブリッジグループ設定 |
| 75 | channel-group 12 | LAN側論理インタフェース (Port-channel) と紐付け |
| 76 | exit | |
| 77 | ! | |
| 78 | interface GigaEthernet 2/1 | 物理インターフェース (WAN側) |
| 79 | vlan-id 20 | vlan-id設定 (ポートVLAN) |
| 80 | bridge-group 20 | ブリッジグループ設定 |
| 81 | channel-group 20 | WAN側論理インタフェース (Port-channel) と紐付け |
| 82 | ipv6 access-group 4000 in | IPv6アクセスリスト紐付け (NS/NA/RA/DHCPv6) |
| 83 | ipv6 access-group 4009 in | IPv6アクセスリスト紐付け (deny) |
| 84 | ipv6 access-group 4010 out | IPv6アクセスリスト紐付け (SPI) |
| 85 | ipv6 access-group spi ftp-data enable | ダイナミックフィルタリング (FTP) |
| 86 | exit | |
| 87 | ! | |
| 88 | interface Port-channel 11 | 論理インターフェース (LAN側) IPv4: プライベートアドレスを設定 IPv6: RAで受信したプレフィックスを本IFに割り当て (RA-proxy機能) ※RA-proxy機能にて、RAで受信したプレフィックスを複数のLAN側 Port-channelに割り当てることはできません。 |
| 89 | ip dhcp service server | DHCPv4サーバ設定 |
| 90 | ip dhcp server-profile DHCPv4_server | DHCPv4サーバプロファイル紐付け |
| 91 | ip address 192.168.100.1 255.255.255.0 | IPv4アドレス設定 |
| 92 | ipv6 enable | IPv6リンクローカルアドレス設定 |
| 93 | ipv6 address autoconfig | IPv6アドレス設定 (RAからアドレス生成) |
| 94 | ipv6 address autoconfig-map-encap MAPCE | IPv6アドレス設定 (RAからMAP-E用アドレス生成) |
| 95 | ipv6 nd other-config-flag | RA 0フラグセット |
| 96 | ipv6 nd send-ra | RA送信設定 |
| 97 | ipv6 trust-ra-prefix-lifetime | RAで通知されたprefix valid lifetimeをそのままアドレスのlifetimeに反映する設定 * RA送信側でプレフィックスの削除(lifetime=0)が行われた場合に、端末側に即時反映させるための設定です。端末側のプレフィックス残留により通信ができなくなるケースを回避するために、本設定を推奨します。デフォルトでは、サービス否認攻撃を受ける環境を想定して、2時間よりも短い値はlifetimeに反映しません。 ※本設定はLAN側/WAN側の両方の論理インタフェースにて必要です。 |
| 98 | ipv6 dhcp service server | DHCPv6サーバ設定 |
| 99 | ipv6 dhcp server-profile DHCPv6_server | DHCPv6サーバプロファイル紐付け |
| 100 | mss 1420 | MSS設定 (1420byte: MAPトンネルから送信するIPv4overIPv6パケットのinner最大長に合わせた値です。) |
| 101 | link-state always-up | 本論理インタフェースを常にリンクアップさせる設定 * 装置起動時にリンクダウンしているとMAPルール取得に失敗するため、本設定を推奨します。 |
| 102 | exit | |
| 103 | ! | |
| 104 | interface Port-channel 12 | 論理インターフェース (LAN側) IPv4: 固定IP8のグローバルアドレスを設定 |
| 105 | ip address 192.0.2.6 255.255.255.248 | IPv4アドレス設定 ※固定IP8で払い出されたアドレスを、お客様の環境に合わせて設定してください。 |
| 106 | mss 1420 | MSS設定 (1420byte: MAPトンネルから送信するIPv4overIPv6パケットのinner最大長に合わせた値です。) |
| 107 | exit | |

| | 設定例 | 補足 |
|-----|--|---|
| 108 | ! | |
| 109 | interface Port-channel 20 | 論理インターフェース (WAN側) |
| 110 | ipv6 enable | IPv6リンクローカルアドレス設定 |
| 111 | ipv6 nd receive-ra prefix-delegation port-channel 11 | RA-proxy設定 |
| 112 | ipv6 router-lifetime-receive-enable | RA default経路登録設定 |
| 113 | ipv6 trust-ra-prefix-lifetime | RAで通知されたprefix valid lifetimeをそのままアドレスのlifetimeに反映する設定 * 論理インターフェース (LAN側) の補足欄に記載の通り、本設定を推奨します。 ※本設定はLAN側/WAN側の両方の論理インターフェースにて必要です。 |
| 114 | ipv6 dhcp service client | DHCPv6クライアント設定 |
| 115 | ipv6 dhcp client-profile DHCPv6_client | DHCPv6クライアントプロファイル紐付け |
| 116 | exit | |
| 117 | ! | |
| 118 | interface Tunnel 1 | MAPトンネルインターフェース |
| 119 | ip access-group 100 in | IPv4アクセスリスト紐付け (permit) |
| 120 | ip access-group 109 in | IPv4アクセスリスト紐付け (deny) |
| 121 | ip access-group 110 out | IPv4アクセスリスト紐付け (SPI) |
| 122 | ip access-group spi ftp-data enable | ダイナミックフィルタリング (FTP) |
| 123 | ip nat inside source list 1 map-encap overload | MAP用NAT+設定 |
| 124 | tunnel mode ipinip tunnel-profile MAPCE | MAP用プロファイルと紐付け |
| 125 | exit | |
| 126 | ! | |
| 127 | line console | Consoleアクセス設定 ※本設定モードは、お客様の環境に合わせて設定ください。 |
| 128 | exec-timeout 0 | 自動ログアウト時間 (分) * "0"指定時は自動ログアウトしません。 |
| 129 | authorization exec default local | Consoleログイン時の許可方式を指定 local: usernameコマンドで設定した特権レベルでログイン許可 |
| 130 | exit | |
| 131 | ! | |
| 132 | line telnet | Telnetアクセス設定 ※本設定モードは、お客様の環境に合わせて設定ください。 |
| 133 | exec-timeout 0 | 自動ログアウト時間 (分) * "0"指定時は自動ログアウトしません。 |
| 134 | exit | |
| 135 | ! | |
| 136 | class-map DNS6 | ポリシーラーティング用class-map |
| 137 | match ipv6 access-group 4100 | IPv6アクセスリスト紐付け (宛先ポート番号53: DNSサーバ宛) |
| 138 | exit | |
| 139 | ! | |
| 140 | class-map DNS6_LO | ポリシーラーティング用class-map |
| 141 | match ipv6 access-group 4101 | IPv6アクセスリスト紐付け (宛先アドレス [::1/128]: 自装置のloopback宛) |
| 142 | exit | |
| 143 | ! | |
| 144 | policy-route-map DNS-POLICY | ポリシーラーティング用のポリシー設定 |
| 145 | ! | |
| 146 | class DNS6 | ポリシーラーティング用のクラス設定 (IPv6 DNSアクセス) |
| 147 | search-sequence 10 | クラスの検索優先度を10に設定 (DNS6_LOより検索優先度が低い) |
| 148 | count | クラスにマッチしたパケット数をカウントする設定 |
| 149 | action nexthop ##ネクストホップアドレス (IPv6) ## | クラスにマッチしたパケットのnexthopを設定: HGWでproxyDNSが動作している場合など、DNSサーバアドレスがRAで受信したプレフィックスに含まれるような場合に、本装置が送信するDNSサーバ宛パケットがLAN方向に送信されて、名前解決が行われなくなることを防ぐための設定です。 ※IPv6デフォルトルートに含まれるアドレスを設定してください。 show ipv6 routeで表示される、デフォルトルート以外のプレフィックス (LAN側ネットワークアドレスなど) に含まれないアドレスであれば、問題ありません。 |
| 150 | exit | |
| 151 | ! | |
| 152 | class DNS6_LO | ポリシーラーティング用のクラス設定 (IPv6 loopbackアクセス) |
| 153 | search-sequence 1 | クラスの検索優先度を1に設定 (DNS6より検索優先度が高い) |
| 154 | count | クラスにマッチしたパケット数をカウントする設定 |
| 155 | action transmit | クラスにマッチしたパケットを経路表に従って送信する設定 |
| 156 | exit | |
| 157 | ! | |
| 158 | exit | |
| 159 | ! | |
| 160 | local policy-route DNS-POLICY | 自発パケットのポリシーラーティング設定 |
| 161 | ! | |
| 162 | dns-server ip enable | DNSv4サーバ設定 |
| 163 | dns-server ipv6 enable | DNSv6サーバ設定 |
| 164 | ! | |
| 165 | proxydns domain 1 any * any dhcp ipv6 port-channel 20 source-interface port-channel 11 | proxyDNS 順引き設定 (any) |
| 166 | proxydns address 1 any dhcp ipv6 port-channel 20 source-interface port-channel 11 | proxyDNS 逆引き設定 (any) |
| 167 | ! | |
| 168 | end | |