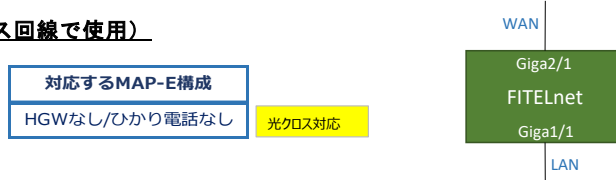


NTTコミュニケーションズ社「OCNバーチャルコネクサービス (IPoE)」を利用するための設定例

対象装置：FITELnet F310

ケース2：固定IP1 (光クロス回線で使用)



※ログインID/Passwordは"test"/"test"です。

設定例	補足
1 access-list 109 deny ip any any	IPv4アクセスリスト (全拒否)
2 access-list 110 spi ip any any	IPv4アクセスリスト (SPI)
3 access-list 4000 permit icmp6 any any neighbor-advertisement	IPv6アクセスリスト (NA許可)
4 access-list 4000 permit icmp6 any any neighbor-solicitation	IPv6アクセスリスト (NS許可)
5 access-list 4000 permit icmp6 any any router-advertisement	IPv6アクセスリスト (RA許可)
6 access-list 4000 permit udp any any eq 546	IPv6アクセスリスト (DHCPv6許可)
7 access-list 4009 deny ipv6 any any	IPv6アクセスリスト (全拒否)
8 access-list 4010 spi ipv6 any any	IPv6アクセスリスト (SPI)
9 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)
10 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)
11 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)
12 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)
13 !	
14 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)
15 ip name-server ::1	DNSサーバ設定 (自装置をサーバに設定)
16 !	
17 ip dhcp server-profile DHCPv4_server	LAN側DHCPv4サーバ設定
18 address 192.168.100.2 192.168.100.254	配布アドレス設定
19 lease-time 259200	DHCPリース期間設定
20 dns 192.168.100.1	配布DNSサーバアドレス設定
21 gateway 192.168.100.1	配布Gatewayアドレス設定
22 exit	
23 !	
24 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)
25 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。
26 !	
27 ipv6 route ::/0 dhcp port-channel 2	IPv6デフォルトルート設定
28 !	
29 ipv6 dhcp client-profile DHCPv6_client	WAN側DHCPv6クライアント設定
30 option-request prefix-delegation	アドレスプレフィックス要求設定
31 option-request dns-server	DNSサーバ要求設定
32 option-request dns-server-domain	DNSサーバドメイン要求設定
33 retries infinity	DHCPメッセージの応答があるまで再送する設定
34 exit	
35 !	
36 ipv6 dhcp server-profile DHCPv6_server	LAN側DHCPv6サーバ設定
37 dns port-channel 2	WAN側で受信したDNSサーバを配布する設定
38 domain port-channel 2	WAN側で受信したドメイン名を配布する設定
39 exit	
40 !	
41 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)
42 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。
43 event interface tunnel 1 up	イベント監視 (interface tunnel 1 up)
44 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)
45 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。
46 exit	
47 !	
48 ipinip tunnel-profile MAPCE	MAPトンネルプロファイル
49 profile-mode map-encap option-c	トンネルのプロファイルモードを指定
50 map rule-get	MAPルール取得設定
51 ipinip fragment pre	プリフラグメント指定
52 exit	
53 !	
54 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。
55 !	

	設定例	補足
56	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。
57	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。
58	!	
59	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。
60	!	
61	hostname F1TELnet	hostname設定
62	!	
63	interface GigaEthernet 1/1	物理インターフェース (LAN側)
64	vlan-id 1	vlan-id設定 (ポートVLAN)
65	bridge-group 1	ブリッジグループ設定
66	channel-group 1	LAN側論理インターフェース (Port-channel) と紐付け
67	policy-route input DNS-POLICY	LAN側ポリシールーティング設定
68	exit	
69	!	
70	interface GigaEthernet 2/1	物理インターフェース (WAN側)
71	vlan-id 2	vlan-id設定 (ポートVLAN)
72	bridge-group 2	ブリッジグループ設定
73	channel-group 2	WAN側論理インターフェース (Port-channel) と紐付け
74	ipv6 access-group 4000 in	IPv6アクセスリスト紐付け (NS/NA/RA/DHCPv6)
75	ipv6 access-group 4009 in	IPv6アクセスリスト紐付け (deny)
76	ipv6 access-group 4010 out	IPv6アクセスリスト紐付け (SPI)
77	ipv6 access-group spi ftp-data enable	ダイナミックフィルタリング (FTP)
78	exit	
79	!	
80	interface Port-channel 1	論理インターフェース (LAN側)
81	ip dhcp service server	DHCPv4サーバ設定
82	ip dhcp server-profile DHCPv4_server	DHCPv4サーバプロファイル紐付け
83	ip address 192.168.100.1 255.255.255.0	IPv4アドレス設定
84	ipv6 enable	IPv6リンクローカルアドレス設定
85	ipv6 address dhcp port-channel 2 ::2/64	IPv6アドレス設定 (DHCPv6-PDから上位64bit+下位64bitアドレス生成)
86	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)
87	ipv6 nd other-config-flag	RA 0フラグセット
88	ipv6 nd send-ra	RA送信設定
89	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ーフェースにて必要です。
90	ipv6 dhcp service server	DHCPv6サーバ設定
91	ipv6 dhcp server-profile DHCPv6_server	DHCPv6サーバプロファイル紐付け
92	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。)
93	link-state always-up	本論理インター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。
94	exit	
95	!	
96	interface Port-channel 2	論理インターフェース (WAN側)
97	ipv6 enable	IPv6リンクローカルアドレス設定
98	ipv6 nd receive-ra prefix-delegation port-channel 1	RA-proxy設定
99	ipv6 router-lifetime-receive-enable	RA default経路登録設定
100	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。
101	ipv6 dhcp service client	DHCPv6クライアント設定
102	ipv6 dhcp client-profile DHCPv6_client	DHCPv6クライアントプロファイル紐付け
103	exit	
104	!	
105	interface Tunnel 1	MAPトンネルインターフェース
106	ip access-group 109 in	IPv4アクセスリスト紐付け (deny)
107	ip access-group 110 out	IPv4アクセスリスト紐付け (SPI)
108	ip access-group spi ftp-data enable	ダイナミックフィルタリング (FTP)
109	ip nat inside source list 1 map-encap overload	MAP用NAT+設定
110	tunnel mode ipinip tunnel-profile MAPCE	MAP用プロファイルと紐付け
111	exit	
112	!	

	設定例	補足
113	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。
114	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。
115	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
116	exit	
117	!	
118	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。
119	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。
120	exit	
121	!	
122	class-map DNS6	ポリシールーティング用class-map
123	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)
124	exit	
125	!	
126	class-map DNS6_LO	ポリシールーティング用class-map
127	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)
128	exit	
129	!	
130	policy-route-map DNS-POLICY	ポリシールーティング用のポリシー設定
131	!	
132	class DNS6	ポリシールーティング用のクラス設定 (IPv6 DNSアクセス)
133	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)
134	count	クラスにマッチしたパケット数をカウントする設定
135	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。
136	exit	
137	!	
138	class DNS6_LO	ポリシールーティング用のクラス設定 (IPv6 loopbackアクセス)
139	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)
140	count	クラスにマッチしたパケット数をカウントする設定
141	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
142	exit	
143	!	
144	exit	
145	!	
146	local policy-route DNS-POLICY	自発パケットのポリシールーティング設定
147	!	
148	dns-server ip enable	DNSv4サーバ設定
149	dns-server ipv6 enable	DNSv6サーバ設定
150	!	
151	proxydns domain 1 any * any dhcp ipv6 port-channel 2 source-interface port-channel 1	proxyDNS 順引き設定 (any)
152	proxydns address 1 any dhcp ipv6 port-channel 2 source-interface port-channel 1	proxyDNS 逆引き設定 (any)
153	!	
154	end	