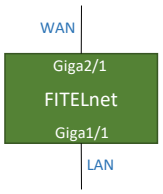
NTTコミュニケーションズ社「OCNバーチャルコネクトサービス（IPoE）」を利用するための設定例

対象装置：FITELnet F310

ケース2：固定IP1（光クロス回線で使用）

対応するMAP-E構成
HGWなし/ひかり電話なし
光クロス対応



※ログインID/Passwordは"test"/"test"です。

	設定例	補足
1	access-list 111 deny udp any eq 135 any	UDPポート135（MS DCOM / RPC）からの全てのトラフィックを拒否します。
2	access-list 111 deny udp any any eq 135	UDPポート135（MS DCOM / RPC）への全てのトラフィックを拒否します。
3	access-list 111 deny tcp any eq 135 any	TCPポート135（MS DCOM / RPC）からの全てのトラフィックを拒否します。
4	access-list 111 deny tcp any any eq 135	TCPポート135（MS DCOM / RPC）への全てのトラフィックを拒否します。
5	access-list 111 deny udp any range 137 139 any	UDPポート137-139（NetBIOS関連）からの全てのトラフィックを拒否します。
6	access-list 111 deny udp any any range 137 139	UDPポート137-139（NetBIOS関連）への全てのトラフィックを拒否します。
7	access-list 111 deny tcp any range 137 139 any	TCPポート137-139（NetBIOS関連）からの全てのトラフィックを拒否します。
8	access-list 111 deny tcp any any range 137 139	TCPポート137-139（NetBIOS関連）への全てのトラフィックを拒否します。
9	access-list 111 deny udp any eq 445 any	UDPポート445（Microsoft-DS / SMB）からの全てのトラフィックを拒否します。
10	access-list 111 deny udp any any eq 445	UDPポート445（Microsoft-DS / SMB）への全てのトラフィックを拒否します。
11	access-list 111 deny tcp any eq 445 any	TCPポート445（Microsoft-DS / SMB）からの全てのトラフィックを拒否します。
12	access-list 111 deny tcp any any eq 445	TCPポート445（Microsoft-DS / SMB）への全てのトラフィックを拒否します。
13	access-list 112 deny ip 192.168.100.0 0.0.0.255 any	IPアドレス範囲192.168.100.0/24からの全てのトラフィックを拒否します。
14	access-list 112 permit icmp any 192.168.100.0 0.0.0.255	192.168.100.0/24へのICMPトラフィックを許可します。
15	access-list 113 spi tcp any any eq ftp	TCPポート21（FTP）への全てのトラフィックを許可します。応答パケットも許可されます。
16	access-list 113 spi tcp any any eq ftp-data	TCPポート20（FTPデータ）への全てのトラフィックを許可します。応答パケットも許可されます。
17	access-list 113 spi tcp any any eq www	TCPポート80（HTTP）への全てのトラフィックを許可します。応答パケットも許可されます。
18	access-list 113 spi udp any any eq domain	UDPポート53（DNS）への全てのトラフィックを許可します。応答パケットも許可されます。
19	access-list 113 spi tcp any any eq smtp	TCPポート25（SMTP）への全てのトラフィックを許可します。応答パケットも許可されます。
20	access-list 113 spi tcp any any eq pop3	TCPポート110（POP3）への全てのトラフィックを許可します。応答パケットも許可されます。
21	access-list 113 spi tcp any any eq 587	TCPポート587（SMTPサブミッション）への全てのトラフィックを許可します。応答パケットも許可されます。
22	access-list 113 spi tcp any any	全てのTCPトラフィックを許可します。応答パケットも許可されます。
23	access-list 113 spi udp any any	全てのUDPトラフィックを許可します。応答パケットも許可されます。
24	access-list 114 permit ip any any	全てのIPトラフィックを許可します。
25	access-list 115 deny ip any any	全てのIPトラフィックを拒否します。
26	access-list 4000 permit icmp6 any any neighbor-advertisement	IPv6アクセスリスト（NA許可）
27	access-list 4000 permit icmp6 any any neighbor-solicitation	IPv6アクセスリスト（NS許可）
28	access-list 4000 permit icmp6 any any router-advertisement	IPv6アクセスリスト（RA許可）
29	access-list 4000 permit udp any any eq 546	IPv6アクセスリスト（DHCPv6許可）
30	access-list 4009 deny ipv6 any any	IPv6アクセスリスト（全拒否）
31	access-list 4010 spi ipv6 any any	IPv6アクセスリスト（SPI）
32	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）
33	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）
34	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）
35	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）
36	!	
37	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）
38	ip name-server ::1	DNSサーバ設定（自装置をサーバに設定）
39	!	
40	ip dhcp server-profile DHCPv4_server	LAN側DHCPv4サーバ設定
41	address 192.168.100.2 192.168.100.254	配布アドレス設定
42	lease-time 259200	DHCPリース期間設定
43	dns 192.168.100.1	配布DNSサーバアドレス設定
44	gateway 192.168.100.1	配布Gatewayアドレス設定
45	exit	
46	!	
47	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）
48	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。
49	!	
50	ipv6 route ::/0 dhcp port-channel 2	IPv6デフォルトルート設定
51	!	
52	ipv6 dhcp client-profile DHCPv6_client	WAN側DHCPv6クライアント設定
53	option-request prefix-delegation	アドレスプレフィックス要求設定
54	option-request dns-server	DNSサーバ要求設定
55	option-request dns-server-domain	DNSサーバドメイン要求設定
56	retries infinity	DHCPメッセージの応答があるまで再送する設定
57	exit	
58	!	

	設定例	補足
59	ipv6 dhcp server-profile DHCPv6_server	LAN側DHCPv6サーバ設定
60	dns port-channel 2	WAN側で受信したDNSサーバを配布する設定
61	domain port-channel 2	WAN側で受信したドメイン名を配布する設定
62	exit	
63	!	
64	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）
65	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。
66	event interface tunnel 1 up	イベント監視（interface tunnel 1 up）
67	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）
68	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エントリの消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。
69	exit	
70	!	
71	ipinip tunnel-profile MAPCE	MAPトンネルプロファイル
72	profile-mode map-encap option-c	トンネルのプロファイルモードを指定
73	map rule-get	MAPルール取得設定
74	ipinip fragment pre	プリフラグメント指定
75	exit	
76	!	
77	logging buffer level informational	装置内部バッファへ出力するログレベル（informational）を指定：指定したレベル名称以上（レベル番号以下）のログ情報を出力します。
78	!	
79	aaa authentication login default local	本装置にログインする場合の認証方式を指定（username コマンドで登録したID/パスワードとする）
80	aaa authorization exec default local	本装置でコマンド実行を許可するかどうかの許可方式を指定（username コマンドで登録した特権レベルとする）
81	!	
82	username guest password guest-secret	ログインユーザ名（guest）とパスワード(guest-secret）の登録
83	!	
84	hostname FITELnet	hostname設定
85	!	
86	interface GigaEthernet 1/1	物理インターフェース（LAN側）
87	vlan-id 1	vlan-id設定（ポートVLAN）
88	bridge-group 1	ブリッジグループ設定
89	channel-group 1	LAN側論理インタフェース（Port-channel）と紐付け
90	policy-route input DNS-POLICY	LAN側ポリシールーティング設定
91	exit	
92	!	
93	interface GigaEthernet 2/1	物理インターフェース（WAN側）
94	vlan-id 2	vlan-id設定（ポートVLAN）
95	bridge-group 2	ブリッジグループ設定
96	channel-group 2	WAN側論理インタフェース（Port-channel）と紐付け
97	ipv6 access-group 4000 in	IPv6アクセスリスト紐付け（NS/NA/RA/DHCPv6）
98	ipv6 access-group 4009 in	IPv6アクセスリスト紐付け（deny）
99	ipv6 access-group 4010 out	IPv6アクセスリスト紐付け（SPI）
100	ipv6 access-group spi ftp-data enable	ダイナミックフィルタリング（FTP）
101	exit	
102	!	
103	interface Port-channel 1	論理インターフェース（LAN側）
104	ip dhcp service server	DHCPv4サーバ設定
105	ip dhcp server-profile DHCPv4_server	DHCPv4サーバプロファイル紐付け
106	ip address 192.168.100.1 255.255.255.0	IPv4アドレス設定
107	ipv6 enable	IPv6リンクローカルアドレス設定
108	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）
109	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）
110	ipv6 nd other-config-flag	RA Oフラグセット
111	ipv6 nd send-ra	RA送信設定
112	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。
113	ipv6 dhcp service server	DHCPv6サーバ設定
114	ipv6 dhcp server-profile DHCPv6_server	DHCPv6サーバプロファイル紐付け
115	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。）
116	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。
117	exit	

	設定例	補足
118	!	
119	interface Port-channel 2	論理インターフェース（WAN側）
120	ipv6 enable	IPv6リンクローカルアドレス設定
121	ipv6 nd receive-ra prefix-delegation port-channel 1	RA-proxy設定
122	ipv6 router-lifetime-receive-enable	RA default経路登録設定
123	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フェースにて必要です。
124	ipv6 dhcp service client	DHCPv6クライアント設定
125	ipv6 dhcp client-profile DHCPv6_client	DHCPv6クライアントプロファイル紐付け
126	exit	
127	!	
128	interface Tunnel 1	MAPトンネルインターフェース
129	ip access-group 111 out	IPv4アクセスリスト紐づけ
130	ip access-group 112 in	IPv4アクセスリスト紐づけ
131	ip access-group 113 out	IPv4アクセスリスト紐づけ
132	ip access-group 114 out	IPv4アクセスリスト紐づけ
133	ip access-group 115 in	IPv4アクセスリスト紐づけ
134	ip access-group spi ftp-data enable	学習フィルタ追加
135	ip access-group spi ftp-data enable	ダイナミックフィルタリング（ FTP ）
136	ip nat inside source list 1 map-encap overload	MAP用NAT+設定
137	tunnel mode ipinip tunnel-profile MAPCE	MAP用プロファイルと紐付け
138	exit	
139	!	
140	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。
141	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。
142	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
143	exit	
144	!	
145	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。
146	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。
147	exit	
148	!	
149	class-map DNS6	ポリシールーティング用class-map
150	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）
151	exit	
152	!	
153	class-map DNS6_LO	ポリシールーティング用class-map
154	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）
155	exit	
156	!	
157	policy-route-map DNS-POLICY	ポリシールーティング用のポリシー設定
158	!	
159	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）
160	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）
161	count	クラスにマッチしたパケット数をカウントする設定
162	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包含される 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包含さ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）に包含されないアドレスであれば、 問題ありません。
163	exit	
164	!	
165	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）
166	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）
167	count	クラスにマッチしたパケット数をカウントする設定
168	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
169	exit	
170	!	
171	exit	
172	!	
173	local policy-route DNS-POLICY	自発パケットのポリシールーティング設定
174	!	
175	dns-server ip enable	DNSv4サーバ設定
176	dns-server ipv6 enable	DNSv6サーバ設定
177	!	
178	proxydns domain 1 any * any dhcp ipv6 port-channel 2 source-interface port-channel 1	proxyDNS 順引き設定（any）
179	proxydns address 1 any dhcp ipv6 port-channel 2 source-interface port-channel 1	proxyDNS 逆引き設定（any）
180	!	
181	end	