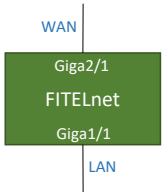
NTTコミュニケーションズ社「OCNバーチャルコネクトサービス（IPoE）」を利用するための設定例

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

ケース1：動的IP

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 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 wellknown 1 1 65535 off	NAT+変換にて全ポート番号を変換対象とする設定 ＊動的IPの場合は、wellknownポートも含めて、送信元ポート番号を本装置に割り当てられたポート番号に変換することが必要です。
49	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。
50	!	
51	ipv6 dhcp client-profile DHCPv6_client	WAN側DHCPv6クライアント設定
52	option-request dns-server	DNSサーバ要求設定
53	option-request dns-server-domain	DNSサーバドメイン要求設定
54	retries infinity	DHCPメッセージの応答があるまで再送する設定
55	exit	
56	!	
57	ipv6 dhcp server-profile DHCPv6_server	LAN側DHCPv6サーバ設定
58	dns port-channel 2	WAN側で受信したDNSサーバを配布する設定
59	domain port-channel 2	WAN側で受信したドメイン名を配布する設定
60	exit	

	設定例	補足
61	!	
62	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）
63	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。
64	event interface tunnel 1 up	イベント監視（interface tunnel 1 up）
65	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）
66	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。
67	exit	
68	!	
69	ipinip tunnel-profile MAPCE	MAPトンネルプロファイル
70	profile-mode map-encap option-c	トンネルのプロファイルモードを指定
71	map rule-get	MAPルール取得設定
72	ipinip fragment pre	プリフラグメント指定
73	exit	
74	!	
75	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。
76	!	
77	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）
78	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）
79	!	
80	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
81	!	
82	hostname FITELnet	hostname設定
83	!	
84	interface GigaEthernet 1/1	物理インターフェース（LAN側）
85	vlan-id 1	vlan-id設定（ポートVLAN）
86	bridge-group 1	ブリッジグループ設定
87	channel-group 1	LAN側論理インタフェース（Port-channel）と紐付け
88	policy-route input DNS-POLICY	LAN側ポリシールーティング設定
89	exit	
90	!	
91	interface GigaEthernet 2/1	物理インターフェース（WAN側）
92	vlan-id 2	vlan-id設定（ポートVLAN）
93	bridge-group 2	ブリッジグループ設定
94	channel-group 2	WAN側論理インタフェース（Port-channel）と紐付け
95	ipv6 access-group 4000 in	IPv6アクセスリスト紐付け（NS/NA/RA/DHCPv6）
96	ipv6 access-group 4009 in	IPv6アクセスリスト紐付け（deny）
97	ipv6 access-group 4010 out	IPv6アクセスリスト紐付け（SPI）
98	ipv6 access-group spi ftp-data enable	ダイナミックフィルタリング（FTP）
99	exit	
100	!	
101	interface Port-channel 1	論理インターフェース（LAN側）
102	ip dhcp service server	DHCPv4サーバ設定
103	ip dhcp server-profile DHCPv4_server	DHCPv4サーバプロファイル紐付け
104	ip address 192.168.100.1 255.255.255.0	IPv4アドレス設定
105	ipv6 enable	IPv6リンクローカルアドレス設定
106	ipv6 address autoconfig	IPv6アドレス設定（RAからアドレス生成）
107	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）
108	ipv6 nd other-config-flag	RA Oフラグセット
109	ipv6 nd send-ra	RA送信設定
110	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。
111	ipv6 dhcp service server	DHCPv6サーバ設定
112	ipv6 dhcp server-profile DHCPv6_server	DHCPv6サーバプロファイル紐付け
113	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。）
114	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。
115	exit	

	設定例	補足
116	!	
117	interface Port-channel 2	論理インターフェース（WAN側）
118	ipv6 enable	IPv6リンクローカルアドレス設定
119	ipv6 nd receive-ra prefix-delegation port-channel 1	RA-proxy設定
120	ipv6 router-lifetime-receive-enable	RA default経路登録設定
121	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。
122	ipv6 dhcp service client	DHCPv6クライアント設定
123	ipv6 dhcp client-profile DHCPv6_client	DHCPv6クライアントプロファイル紐付け
124	exit	
125	!	
126	interface Tunnel 1	MAPトンネルインターフェース
127	ip access-group 111 out	IPv4アクセスリスト紐づけ
128	ip access-group 112 in	IPv4アクセスリスト紐づけ
129	ip access-group 113 out	IPv4アクセスリスト紐づけ
130	ip access-group 114 out	IPv4アクセスリスト紐づけ
131	ip access-group 115 in	IPv4アクセスリスト紐づけ
132	ip access-group spi ftp-data enable	学習フィルタ追加
133	ip access-group spi ftp-data enable	ダイナミックフィルタリング(FTP)
134	ip nat inside source list 1 map-encap overload	MAP用NAT+設定
135	tunnel mode ipinip tunnel-profile MAPCE	MAP用プロファイルと紐付け
136	exit	
137	!	
138	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。
139	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。
140	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
141	exit	
142	!	
143	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。
144	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。
145	exit	
146	!	
147	class-map DNS6	ポリシールーティング用class-map
148	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）
149	exit	
150	!	
151	class-map DNS6_LO	ポリシールーティング用class-map
152	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）
153	exit	
154	!	
155	policy-route-map DNS-POLICY	ポリシールーティング用のポリシー設定
156	!	
157	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）
158	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）
159	count	クラスにマッチしたパケット数をカウントする設定
160	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。
161	exit	
162	!	
163	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）
164	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）
165	count	クラスにマッチしたパケット数をカウントする設定
166	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
167	exit	
168	!	
169	exit	
170	!	
171	local policy-route DNS-POLICY	自発パケットのポリシールーティング設定
172	!	
173	dns-server ip enable	DNSv4サーバ設定
174	dns-server ipv6 enable	DNSv6サーバ設定
175	!	
176	proxydns domain 1 any * any dhcp ipv6 port-channel 2 source-interface port-channel 1	proxyDNS 順引き設定（any）
177	proxydns address 1 any dhcp ipv6 port-channel 2 source-interface port-channel 1	proxyDNS 逆引き設定（any）
178	!	
179	end	