

## 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3 : 固定IP8 (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 100 permit ip any host 192.0.2.2	IPv4アクセリスト (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 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。
6	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。
7	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。
8	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。
9	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。
10	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。
11	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。
12	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。
13	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。
14	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。
15	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。
16	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。
17	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。
18	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。
19	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。
20	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。
21	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。
22	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。
23	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。
24	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。
25	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。
26	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。
27	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。
28	access-list 114 permit ip any any	全てのIPトラフィックを許可します。
29	access-list 115 deny ip any any	全てのIPトラフィックを拒否します。
30	access-list 4000 permit icmp6 any any neighbor-advertisement	IPv6アクセリスト (NA許可)
31	access-list 4000 permit icmp6 any any neighbor-solicitation	IPv6アクセリスト (NS許可)
32	access-list 4000 permit icmp6 any any router-advertisement	IPv6アクセリスト (RA許可)
33	access-list 4000 permit udp any any eq 546	IPv6アクセリスト (DHCPv6許可)
34	access-list 4009 deny ipv6 any any	IPv6アクセリスト (全拒否)
35	access-list 4010 spi ipv6 any any	IPv6アクセリスト (SPI)
36	access-list 4100 permit tcp any any eq 53	IPv6アクセリスト (IPv6 TCP DNS/ポリシールーティング用)
37	access-list 4100 permit udp any any eq 53	IPv6アクセリスト (IPv6 UDP DNS/ポリシールーティング用)
38	access-list 4101 permit tcp any ::1/128	IPv6アクセリスト (IPv6 TCP loopback/ポリシールーティング用)
39	access-list 4101 permit udp any ::1/128	IPv6アクセリスト (IPv6 UDP loopback/ポリシールーティング用)
40	!	
41	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)
42	ip name-server ::1	DNSサーバ設定 (自装置をサーバに設定)
43	!	
44	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)
45	address 192.168.100.2 192.168.100.254	配布アドレス設定
46	lease-time 259200	DHCPリース期間設定
47	dns 192.168.100.1	配布DNSサーバアドレス設定
48	gateway 192.168.100.1	配布Gatewayアドレス設定
49	exit	
50	!	
51	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)
52	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」を中継するための設定
53	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。

	設定例	補足
54 !		
55 ipv6 route ::/0 dhcp port-channel 20	IPv6デフォルトルート設定	
56 !		
57 ipv6 dhcp client-profile DHCPv6_client	WAN側DHCPv6クライアント設定	
58 option-request prefix-delegation	アドレスプレフィックス要求設定	
59 option-request dns-server	DNSサーバ要求設定	
60 option-request dns-server-domain	DNSサーバドメイン要求設定	
61 retries infinity	DHCPメッセージの応答があるまで再送する設定	
62 exit		
63 !		
64 ipv6 dhcp server-profile DHCPv6_server	LAN側DHCPv6サーバ設定	
65 dns port-channel 20	WAN側で受信したDNSサーバを配布する設定	
66 domain port-channel 20	WAN側で受信したドメイン名を配布する設定	
67 exit		
68 !		
69 event-action 1	イベントアクション設定 (HGWのSPIフィルタエンタリ対策用)	
70 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。	
71 event interface tunnel 1 up	イベント監視 (interface tunnel 1 up)	
72 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)	
73 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エンタ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側インター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。	
74 exit		
75 !		
76 ipipip_tunnel-profile MAPCE	MAPトンネルプロファイル	
77 profile-mode map-encap option-c	トンネルのプロファイルモードを指定	
78 map rule-get	MAPルール取得設定	
79 ipipip fragment pre	ブリッジメント指定	
80 exit		
81 !		
82 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。	
83 !		
84 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)	
85 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)	
86 !		
87 username guest password guest-secret	ログインユーザID名 (guest) とパスワード (guest-secret) の登録	
88 !		
89 hostname FITELnet	hostname設定	
90 !		
91 interface GigaEthernet 1/1	物理インターフェース (LAN側)	
92 vlan-id 11	vlan-id設定 (ポートVLAN)	
93 bridge-group 11	ブリッジグループ設定	
94 channel-group 11	LAN側論理インターフェース (Port-channel) と紐付け	
95 policy-route input DNS-POLICY	LAN側ポリシールーティング設定	
96 exit		
97 !		
98 interface GigaEthernet 1/2	物理インターフェース (LAN側)	
99 vlan-id 12	vlan-id設定 (ポートVLAN)	
100 bridge-group 12	ブリッジグループ設定	
101 channel-group 12	LAN側論理インターフェース (Port-channel) と紐付け	
102 exit		
103 !		
104 interface GigaEthernet 2/1	物理インターフェース (WAN側)	
105 vlan-id 20	vlan-id設定 (ポートVLAN)	
106 bridge-group 20	ブリッジグループ設定	
107 channel-group 20	WAN側論理インターフェース (Port-channel) と紐付け	
108 ipv6 access-group 4000 in	IPv6アクセリスト紐付け (NS/NA/RA/DHCPv6)	
109 ipv6 access-group 4009 in	IPv6アクセリスト紐付け (deny)	
110 ipv6 access-group 4010 out	IPv6アクセリスト紐付け (SPI)	
111 ipv6 access-group spi ftp-data enable	ダイナミックフィルタリング (FTP)	
112 exit		
113 !		

	設定例	補足
114	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。
115	ip dhcp service server	DHCPv4サーバ設定
116	ip dhcp server-profile DHCPv4_server	DHCPv4サーバプロファイル紐付け
117	ip address 192.168.100.1 255.255.255.0	IPv4アドレス設定
118	ipv6 enable	IPv6リンクローカルアドレス設定
119	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)
120	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)
121	ipv6 nd other-config-flag	RA 0フラグセット
122	ipv6 nd send-ra	RA送信設定
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 * 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。
124	ipv6 dhcp service server	DHCPv6サーバ設定
125	ipv6 dhcp server-profile DHCPv6_server	DHCPv6サーバプロファイル紐付け
126	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。)
127	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。
128	exit	
129	!	
130	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
131	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。
132	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。)
133	exit	
134	!	
135	interface Port-channel 20	論理インターフェース (WAN側)
136	ipv6 enable	IPv6リンクローカルアドレス設定
137	ipv6 nd receive-ra prefix-delegation port-channel 11	RA-proxy設定
138	ipv6 router-lifetime-receive-enable	RA default経路登録設定
139	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。
140	ipv6 dhcp service client	DHCPv6クライアント設定
141	ipv6 dhcp client-profile DHCPv6_client	DHCPv6クライアントプロファイル紐付け
142	exit	
143	!	
144	interface Tunnel 1	MAPトンネルインターフェース
145	ip access-group 100 in	IPv4アクセリスト紐付け (permit)
146	ip access-group 111 out	IPv4アクセリスト紐づけ
147	ip access-group 112 in	IPv4アクセリスト紐づけ
148	ip access-group 113 out	IPv4アクセリスト紐づけ
149	ip access-group 114 out	IPv4アクセリスト紐づけ
150	ip access-group 115 in	IPv4アクセリスト紐づけ
151	ip access-group spi ftp-data enable	学習フィルタ追加
152	ip access-group spi ftp-data enable	ダイナミックフィルタリング(FTP)
153	ip nat inside source list 1 map-encap overload	MAP用NAT+設定
154	tunnel mode ipipip tunnel-profile MAPCE	MAP用プロファイルと紐付け
155	exit	
156	!	
157	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。
158	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。
159	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
160	exit	
161	!	
162	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。
163	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。
164	exit	
165	!	

	設定例	補足
166	class-map DNS6	ポリシールーティング用class-map
167	match ipv6 access-group 4100	IPv6アクセリスト紐付け（宛先ポート番号53：DNSサーバ宛）
168	exit	
169	!	
170	class-map DNS6_L0	ポリシールーティング用class-map
171	match ipv6 access-group 4101	IPv6アクセリスト紐付け（宛先アドレス[::1/128]：自装置のloopback宛）
172	exit	
173	!	
174	policy-route-map DNS-POLICY	ポリシールーティング用のポリシー設定
175	!	
176	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）
177	search-sequence 10	クラスの検索優先度を10に設定（DNS6_L0より検索優先度が低い）
178	count	クラスにマッチしたパケット数をカウントする設定
179	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。
180	exit	
181	!	
182	class DNS6_L0	ポリシールーティング用のクラス設定（IPv6 loopbackアクセス）
183	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）
184	count	クラスにマッチしたパケット数をカウントする設定
185	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
186	exit	
187	!	
188	exit	
189	!	
190	local policy-route DNS-POLICY	自発パケットのポリシールーティング設定
191	!	
192	dns-server ip enable	DNSv4サーバ設定
193	dns-server ipv6 enable	DNSv6サーバ設定
194	!	
195	proxydns domain 1 any * any dhcp ipv6 port-channel 20 source-interface port-channel 11	proxyDNS 順引き設定 (any)
196	proxydns address 1 any dhcp ipv6 port-channel 20 source-interface port-channel 11	proxyDNS 逆引き設定 (any)
197	!	
198	end	