

アルテリア・ネットワークス社「クロスパス」を利用するための設定例

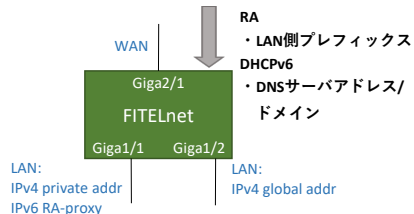
対象装置 : FITELnet F70/F71/F220/F221/F225/F310/F220 EX/F221 EX

固定IP8/IP16

- ・WANからLANへのIPv6プレフィックス
配布にRA-Proxyを利用

※本設定例は、「固定IP8」を使用する場合の例です。
「固定IP16」では、Giga 1/2 (Port-channel 12) に
マスク長28を設定かつ access-list 100 のエントリを
必要に応じて追加してください。
※ログインID/Passwordは“test”/“test”です。

○ : 対応する構成
○ HGWあり/ひかり電話あり
○ HGWあり/ひかり電話なし
○ HGWなし/ひかり電話あり
○ HGWなし/ひかり電話なし



設定例	補足
1 access-list 100 permit ip any host ##固定IP8アドレス-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 ##固定IP8アドレス-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 ##固定IP8アドレス-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 ##固定IP8アドレス-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 (学習フィルタ以外を拒否)
6 access-list 110 spi ip any any	IPv4アクセスリスト (学習フィルタ)
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 (access-list 4000と学習フィルタ以外を拒否)
12 access-list 4010 spi ipv6 any any	IPv6アクセスリスト (学習フィルタ)
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 default経路設定 (デフォルトルートをIPv4overIPv6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 LAN	DHCPv4サーバプロファイル
22 address 192.168.0.2 192.168.0.254	配布アドレス設定
23 lease-time 28800	DHCPリース期間設定
24 dns 192.168.0.1	配布DNSサーバアドレス設定
25 gateway 192.168.0.1	配布Gatewayアドレス設定
26 exit	
27 !	
28 ip nat list 1 192.168.0.0 0.0.0.255	NAT変換対象アドレス設定 (LAN側 192.168.0.0/24)
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します。
30 !	
31 ipv6 dhcp client-profile NGN	DHCPv6クライアントプロファイル
32 option-request dns-server	DNSサーバの情報取得要求の設定
33 retries infinity	DHCPメッセージの返信があるまで再送する設定
34 exit	
35 !	
36 ipv6 dhcp server-profile LANv6	DHCPv6サーバプロファイル
37 dns port-channel 1	DHCPv6クライアント機能で取得したDNSサーバアドレスを配布する設定
38 exit	
39 !	
40 ipinip tunnel-profile IPIPI	IPinIPトンネルプロファイル
41 profile-mode ipip	プロファイルモードをIPinIPに設定
42 source ipv6 port-channel 11	Outerの送信元アドレス : Port-channel11のIPv6アドレスを指定
43 destination address ##トンネル終端装置 IPv6アドレス##	Outerの宛先アドレス : トンネル終端装置のアドレスを設定 ★アルテリア・ネットワークス社の指定に合わせて設定ください。 例) destination address 2001:db8::1
44 ipinip fragment pre	ブリフラグメント設定
45 exit	
46 !	
47 logging buffer level informational	
48 !	
49 aaa authentication login default local	
50 aaa authorization exec default local	
51 !	
52 username test privilege 15 password 2 \$1\$LAruC04\$T3069M0hXaiNub6xoHnsG1	装置のログインID/Password (test /test)
53 !	
54 hostname FITELnet	
55 !	
56 interface GigaEthernet 1/1	物理インターフェース (LAN側)
57 vlan-id 11	
58 bridge-group 11	
59 channel-group 11	LAN側論理インターフェース (Port-channel) と紐付け
60 policy-route input DNS-POLICY	LAN側ポリシールーティング設定
61 exit	

	設定例	補足
62	!	
63	interface GigaEthernet 1/2	物理インターフェース (LAN側)
64	vlan-id 12	
65	bridge-group 12	
66	channel-group 12	LAN側論理インターフェース (Port-channel) と紐付け
67	exit	
68	!	
69	interface GigaEthernet 2/1	物理インターフェース (WAN側)
70	vlan-id 1	
71	bridge-group 1	
72	channel-group 1	WAN側論理インターフェース (Port-channel) と紐付け
73	ipv6 access-group 4000 in	IPv6アクセスリスト紐づけ (NS/NA/RA/DHCPv6)
74	ipv6 access-group 4009 in	IPv6アクセスリスト紐づけ (deny)
75	ipv6 access-group 4010 out	IPv6アクセスリスト紐づけ (学習フィルタ)
76	exit	
77	!	
78	interface Port-channel 1	論理インターフェース (WAN側)
79	ipv6 enable	IPv6リンクローカルアドレス設定
80	ipv6 nd receive-ra prefix-delegation port-channel 11	RA-proxy設定
81	ipv6 router-lifetime-receive-enable	RA default経路登録設定
82	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。
83	ipv6 dhcp service client	DHCPv6クライアント設定
84	ipv6 dhcp client-profile NGN	DHCPv6クライアントプロファイル紐付け
85	exit	
86	!	
87	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。
88	ip dhcp service server	DHCPv4サーバー設定
89	ip dhcp server-profile LAN	DHCPv4サーバープロファイル紐付け
90	ip address 192.168.0.1 255.255.255.0	IPv4アドレス設定
91	ipv6 enable	IPv6リンクローカルアドレス設定
92	ipv6 address autoconfig	IPv6アドレス設定 (RAから自動生成) ★クロスパスではインタフェースIDの指定は不要です。
93	ipv6 nd other-config-flag	RA 0フラグセット
94	ipv6 nd send-ra	RA送信設定
95	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 (WAN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。
96	ipv6 dhcp service server	DHCPv6サーバー設定
97	ipv6 dhcp server-profile LANv6	DHCPv6サーバープロファイル紐付け
98	mss 1420	MSS設定 (1420byte: Tunnel 1から送信するIPv4overIPv6パケットのinner最大長に合わせた値です。)
99	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
100	ddns-client address ipv6 action http-client 1 delay 10 interval 600	ダイナミックDNSクライアント設定
101	exit	
102	!	
103	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
104	ip address ##固定IP8アドレス-6## 255.255.255.248	IPv4グローバルアドレス設定 ★アルテリア・ネットワークス社より割り当てられた固定IP8アドレスをお客様の環境に合わせて設定してください。
105	mss 1420	MSS設定 (1420byte: Tunnel 1から送信するIPv4overIPv6パケットのinner最大長に合わせた値です。)
106	exit	
107	!	
108	interface Tunnel 1	トンネルインターフェース設定
109	ip address ##固定IP8アドレス-1## 255.255.255.255	IPv4グローバルアドレス設定 ★アルテリア・ネットワークス社より割り当てられた固定IP8アドレスをお客様の環境に合わせて設定してください。
110	ip access-group 100 in	IPv4アクセスリスト紐づけ (permit)
111	ip access-group 109 in	IPv4アクセスリスト紐づけ (deny)
112	ip access-group 110 out	IPv4アクセスリスト紐づけ (学習フィルタ)
113	ip nat inside source list 1 interface	NAT+設定 (送信元アドレスをLAN側アドレスからグローバルアドレスに変換)
114	tunnel mode ipinip tunnel-profile IPIP1	トンネルプロファイル紐づけ
115	exit	

	設定例	補足
116	!	
117	class-map DNS6	ポリシールーティング用class-map
118	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)
119	exit	
120	!	
121	class-map DNS6_L0	ポリシールーティング用class-map
122	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)
123	exit	
124	!	
125	policy-route-map DNS-POLICY	ポリシールーティング用のポリシー設定
126	!	
127	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)
128	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)
129	count	クラスにマッチしたパケット数をカウントする設定
130	action nextthop 2001:db8::1	クラスにマッチしたパケットのnextthopを設定 (2001:db8::1) : ★IPv6 Documentation Prefixの範囲 (2001:db8::/32) のアドレスを指定してください。 #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。このため、IPv6デフォルトルートに包含されるアドレスを指定する必要があります。
131	exit	
132	!	
133	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)
134	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)
135	count	クラスにマッチしたパケット数をカウントする設定
136	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
137	exit	
138	!	
139	exit	
140	!	
141	local policy-route DNS-POLICY	自発パケットのポリシールーティング設定
142	!	
143	line console	
144	exec-timeout 0	
145	authorization exec default local	
146	exit	
147	!	
148	line telnet	
149	exec-timeout 0	
150	exit	
151	!	
152	dns-server ip enable	DNSサーバ機能およびProxyDNS機能を有効化 (IPv4)
153	dns-server ipv6 enable	DNSサーバ機能およびProxyDNS機能を有効化 (IPv6)
154	!	
155	proxydns domain 1 any * any dhcp ipv6 port-channel 1 source-interface port-channel 11	ProxyDNSの正引き動作条件を指定 (DHCPクライアントが取得したDNSサーバアドレスをリレー先に指定)
156	proxydns address 1 any dhcp ipv6 port-channel 1 source-interface port-channel 11	ProxyDNSの逆引き動作条件を指定 (DHCPクライアントが取得したDNSサーバアドレスをリレー先に指定)
157	!	
158	http-client 1	ダイナミックDNSのHTTPクライアント設定
159	request-timeout 10 retry 5	登録要求メッセージの応答受信待ち許容時間とリトライ回数を設定
160	method 1 get url https://##Basic認証ID##:##Basic認証パスワード##@##アップデートサーバURL## d ##FQDN## p ##DDNSパスワード## u ##DDNS_ID## a \$i6	HTTPSのRequest-Lineの設定 ★Basic認証ID、Basic認証パスワード、アップデートサーバURL、DDNS_ID、DDNSパスワード、FQDNはアルテリア・ネットワークス社の指定に合わせて設定ください。 例) method 1 get url https://BID:diAC/Lag5iPe6@www.example.net d example.com p DPASS u DID a \$i6 ※HTTPS指定は、F70/F71はV01.03(00)以降、F220/F221はV01.05(00)以降のファームウェアにてサポートしています。
161	reference-interface port-channel 11	methodコマンドで参照するインタフェースを指定
162	source-interface port-channel 11	登録要求メッセージの送信元アドレスを指定
163	logging on	HTTPクライアントのログ出力を行う設定
164	exit	
165	!	
166	end	