

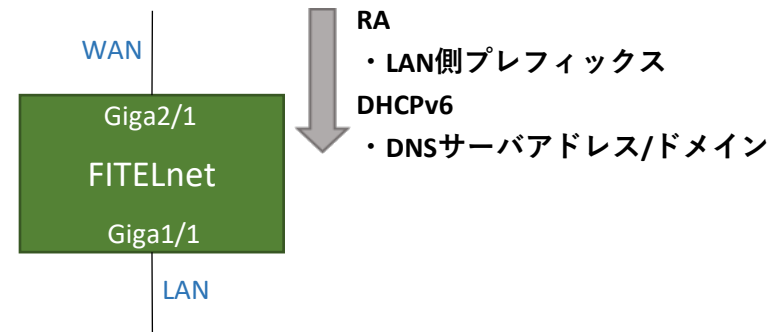
アルテリア・ネットワークス社「クロスパス」を利用するための設定例

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

固定IP1

- ・WANからLANへのIPv6プレフィクス配布にRA-Proxyを利用

<input type="radio"/> ：対応する構成
<input type="radio"/> HGWあり/ひかり電話あり
<input type="radio"/> HGWあり/ひかり電話なし
<input type="radio"/> HGWなし/ひかり電話あり
<input type="radio"/> HGWなし/ひかり電話なし



	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（access-list 4000と学習フィルタ以外を拒否）
31	access-list 4010 spi ipv6 any any	IPv6アクセスリスト（学習フィルタ）
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 default経路設定（デフォルトルートをIPv4overIPv6トンネルに設定）
38	ip name-server ::1	DNSサーバー設定（自装置をサーバーに設定）
39	!	
40	ip dhcp server-profile LAN	DHCPv4サーバープロファイル
41	address 192.168.0.2 192.168.0.254	配布アドレス設定
42	lease-time 28800	DHCPリース期間設定
43	dns 192.168.0.1	配布DNSサーバーアドレス設定
44	gateway 192.168.0.1	配布Gatewayアドレス設定
45	exit	
46	!	
47	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）
48	!	
49	ipv6 dhcp client-profile NGN	DHCPv6クライアントプロファイル
50	option-request dns-server	DNSサーバの情報取得要求の設定
51	retries infinity	DHCPメッセージの返信があるまで再送する設定
52	exit	
53	!	
54	ipv6 dhcp server-profile LANv6	DHCPv6サーバープロファイル
55	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
56	exit	
57	!	
58	ipinip tunnel-profile IPIP1	IPinIPトンネルプロファイル
59	profile-mode ipip	プロファイルモードをIPinIPに設定
60	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
61	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
62	ipinip fragment pre	プリフラグメント設定
63	exit	
64	!	
65	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。
66	!	

	設定例	補足
67	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）
68	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口許可方式を指定（username コマンドで登録した特権レベルとする）
69	!	
70	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
71	!	
72	hostname FITELnet	hostname設定
73	!	
74	interface GigaEthernet 1/1	物理インターフェース（LAN側）
75	vlan-id 11	
76	bridge-group 11	
77	channel-group 11	LAN側論理インタフェース（Port-channel）と紐付け
78	policy-route input DNS-POLICY	LAN側ポリシールーティング設定
79	exit	
80	!	
81	interface GigaEthernet 2/1	物理インターフェース（WAN側）
82	vlan-id 1	
83	bridge-group 1	
84	channel-group 1	WAN側論理インタフェース（Port-channel）と紐付け
85	ipv6 access-group 4000 in	IPv6アクセスリスト紐づけ（NS/NA/RA/DHCPv6）
86	ipv6 access-group 4009 in	IPv6アクセスリスト紐づけ（deny）
87	ipv6 access-group 4010 out	IPv6アクセスリスト紐づけ（学習フィルタ）
88	exit	
89	!	
90	interface Port-channel 1	論理インターフェース（WAN側）
91	ipv6 enable	IPv6リンクローカルアドレス設定
92	ipv6 nd receive-ra prefix-delegation port-channel 11	RA-proxy設定
93	ipv6 router-lifetime-receive-enable	RA default経路登録設定
94	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。
95	ipv6 dhcp service client	DHCPv6クライアント設定
96	ipv6 dhcp client-profile NGN	DHCPv6クライアントプロファイル紐付け
97	exit	
98	!	
99	interface Port-channel 11	論理インターフェース（LAN側）
100	ip dhcp service server	DHCPv4サーバー設定
101	ip dhcp server-profile LAN	DHCPv4サーバープロファイル紐付け
102	ip address 192.168.0.1 255.255.255.0	IPv4アドレス設定
103	ipv6 enable	IPv6リンクローカルアドレス設定
104	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。
105	ipv6 nd other-config-flag	RA 0フラグセット
106	ipv6 nd send-ra	RA送信設定
107	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（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フェースにて必要です。
108	ipv6 dhcp service server	DHCPv6サーバー設定
109	ipv6 dhcp server-profile LANv6	DHCPv6サーバープロファイル紐付け
110	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。）
111	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
112	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
113	exit	
114	!	
115	interface Tunnel 1	トンネルインタフェース設定
116	ip address ##固定IPv4グローバルアドレス## 255.255.255.255	IPv4グローバルアドレス設定 ★固定IPv4グローバルアドレスはアルテリア・ネットワークス社の指定に合わせて設定ください。
117	ip access-group 111 out	IPv4アクセスリスト紐づけ
118	ip access-group 112 in	IPv4アクセスリスト紐づけ
119	ip access-group 113 out	IPv4アクセスリスト紐づけ
120	ip access-group 114 out	IPv4アクセスリスト紐づけ
121	ip access-group 115 in	IPv4アクセスリスト紐づけ
122	ip access-group spi ftp-data enable	学習フィルタ追加
123	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）
124	tunnel mode ipinip tunnel-profile IPIP1	トンネルプロファイル紐づけ
125	exit	
126	!	
127	class-map DNS6	ポリシールーティング用class-map
128	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）
129	exit	
130	!	
131	class-map DNS6_L0	ポリシールーティング用class-map
132	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）
133	exit	
134	!	

	設定例	補足
135	policy-route-map DNS-POLICY	ポリシールーティング用のポリシー設定
136	!	
137	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）
138	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）
139	count	クラスにマッチしたパケット数をカウントする設定
140	action nexthop 2001:db8::1	クラスにマッチしたパケットのnexthop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。
141	exit	
142	!	
143	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）
144	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）
145	count	クラスにマッチしたパケット数をカウントする設定
146	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
147	exit	
148	!	
149	exit	
150	!	
151	local policy-route DNS-POLICY	自発パケットのポリシールーティング設定
152	!	
153	line console	
154	exec-timeout 0	
155	authorization exec default local	
156	exit	
157	!	
158	line telnet	
159	exec-timeout 0	
160	exit	
161	!	
162	dns-server ip enable	DNSサーバ機能およびProxyDNS機能を有効化（IPv4）
163	dns-server ipv6 enable	DNSサーバ機能およびProxyDNS機能を有効化（IPv6）
164	!	
165	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）
166	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）
167	!	
168	http-client 1	ダイナミックDNSのHTTPクライアント設定
169	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
170	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。
171	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
172	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
173	logging on	HTTPクライアントのログ出力を行う設定
174	exit	
175	!	
176	end	