

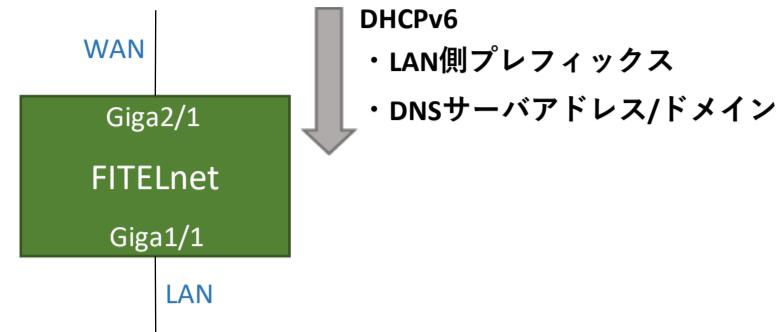
アルテリア・ネットワークス社「クロスパス」を利用するための設定例

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プレフィックス配布にDHCPv6-PDを利用

○ : 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 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アクセリスト (NA許可)
27	access-list 4000 permit icmp6 any any neighbor-solicitation	IPv6アクセリスト (NS許可)
28	access-list 4000 permit icmp6 any any router-advertisement	IPv6アクセリスト (RA許可)
29	access-list 4000 permit udp any any eq 546	IPv6アクセリスト (DHCPv6許可)
30	access-list 4009 deny ipv6 any any	IPv6アクセリスト (access-list 4000と学習フィルタ以外を拒否)
31	access-list 4010 spi ipv6 any any	IPv6アクセリスト (学習フィルタ)
32	!	
33	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)
34	ip name-server ::1	DNSサーバー設定 (自装置をサーバーに設定)
35	!	
36	ip dhcp server-profile LAN	DHCPv4サーバープロファイル
37	address 192.168.0.2 192.168.0.254	配布アドレス設定
38	lease-time 28800	DHCPリース期間設定
39	dns 192.168.0.1	配布DNSサーバーアドレス設定
40	gateway 192.168.0.1	配布Gatewayアドレス設定
41	exit	
42	!	
43	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)
44	!	
45	ipv6 route ::/0 dhcp port-channel 1	IPv6 default経路設定 (デフォルトルートをDHCPv6サーバとする設定)
46	!	
47	ipv6 dhcp client-profile NGN	DHCPv6クライアントプロファイル
48	option-request prefix-delegation	アドレスプレフィックス要求設定
49	option-request dns-server	DNSサーバの情報取得要求の設定
50	retries infinity	DHCPメッセージの返信があるまで再送する設定
51	exit	
52	!	
53	ipv6 dhcp server-profile LANv6	DHCPv6サーバープロファイル
54	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
55	exit	
56	!	
57	ipinip tunnel-profile IPIP1	IPinIPトンネルプロファイル
58	profile-mode ipip	プロファイルモードをIPinIPに設定
59	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
60	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
61	ipinip fragment pre	プリフラグメント設定
62	exit	
63	!	
64	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。
65	!	

	設定例	補足
66	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)
67	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)
68	!	
69	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
70	!	
71	hostname FITELnet	hostname設定
72	!	
73	interface GigaEthernet 1/1	物理インターフェース (LAN側)
74	vlan-id 11	
75	bridge-group 11	
76	channel-group 11	LAN側論理インターフェース (Port-channel) と紐付け
77	exit	
78	!	
79	interface GigaEthernet 2/1	物理インターフェース (WAN側)
80	vlan-id 1	
81	bridge-group 1	
82	channel-group 1	WAN側論理インターフェース (Port-channel) と紐付け
83	ipv6 access-group 4000 in	IPv6アクセリスト紐づけ (NS/NA/RA/DHCPv6)
84	ipv6 access-group 4009 in	IPv6アクセリスト紐づけ (deny)
85	ipv6 access-group 4010 out	IPv6アクセリスト紐づけ (学習フィルタ)
86	exit	
87	!	
88	interface Port-channel 1	論理インターフェース (WAN側)
89	ipv6 enable	IPv6リンクローカルアドレス設定
90	ipv6 dhcp service client	DHCPv6クライアント設定
91	ipv6 dhcp client-profile NGN	DHCPv6クライアントプロファイル紐づけ
92	exit	
93	!	
94	interface Port-channel 11	論理インターフェース (LAN側)
95	ip dhcp service server	DHCPv4サーバー設定
96	ip dhcp server-profile LAN	DHCPv4サーバープロファイル紐づけ
97	ip address 192.168.0.1 255.255.255.0	IPv4アドレス設定
98	ipv6 enable	IPv6リンクローカルアドレス設定
99	ipv6 address dhcp port-channel 1 ##インターフェースID##/64	IPv6アドレス設定 (RAから上位64bit+インターフェースIDから下位64bitによりアドレス生成) ★インターフェースIDはお客様の環境に合わせて設定してください。 例) ipv6 address dhcp port-channel 1 ::11/64
100	ipv6 nd other-config-flag	RA0フラグセット
101	ipv6 nd send-ra	RA送信設定 RA prefix lifetime の設定 * プレフィックスの削除が行われた場合に、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、prefix lifetime 0 を送信しません。 ※F70/F71はV01.02(00)以降、F220/F221はV01.04(00)以降のファームウェアにてサポートオプションです。
102	ipv6 trust-ra-prefix-lifetime	
103	ipv6 dhcp service server	DHCPv6サーバー設定
104	ipv6 dhcp server-profile LANv6	DHCPv6サーバープロファイル紐づけ
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	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
107	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
108	exit	
109	!	
110	interface Tunnel 1	トンネルインターフェース設定
111	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。
112	ip access-group 111 out	IPv4アクセリスト紐づけ
113	ip access-group 112 in	IPv4アクセリスト紐づけ
114	ip access-group 113 out	IPv4アクセリスト紐づけ
115	ip access-group 114 out	IPv4アクセリスト紐づけ
116	ip access-group 115 in	IPv4アクセリスト紐づけ
117	ip access-group spi ftp-data enable	学習フィルタ追加
118	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)
119	tunnel mode ipinip tunnel-profile IPIP1	トンネルプロファイル紐づけ
120	exit	
121	!	
122	line console	
123	exec-timeout 0	
124	authorization exec default local	
125	exit	
126	!	
127	line telnet	
128	exec-timeout 0	
129	exit	
130	!	
131	dns-server ip enable	DNSサーバ機能およびProxyDNS機能を有効化 (IPv4)
132	dns-server ipv6 enable	DNSサーバ機能およびProxyDNS機能を有効化 (IPv6)
133	!	
134	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)
135	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)
136	!	

	設定例	補足
137	http-client 1	ダイナミックDNSのHTTPクライアント設定
138	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
139	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.com 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。
140	reference-interface port-channel 11	methodコマンドで参照するインターフェースを指定
141	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
142	logging on	HTTPクライアントのログ出力を行う設定
143	exit	
144	!	
145	end	