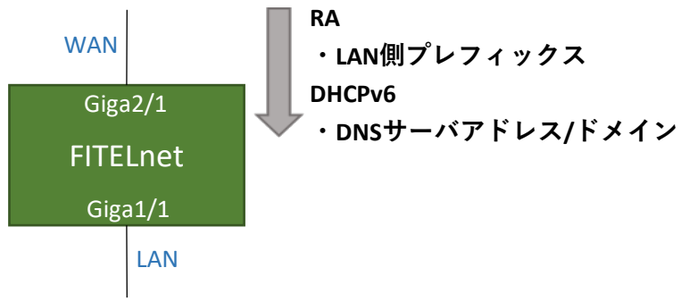
アルテリア・ネットワークス社「クロスパス」を利用するための設定例

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

可変IP（DS-Lite）

・WANからLANへのIPv6プレフィクス配布にRA-Proxy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	ipv6 dhcp client-profile NGN	DHCPv6クライアントプロファイル
48	option-request dns-server	DNSサーバの情報取得要求の設定
49	retries infinity	DHCPメッセージの返信があるまで再送する設定
50	exit	
51	!	
52	ipv6 dhcp server-profile LANv6	DHCPv6サーバープロファイル
53	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
54	exit	
55	!	
56	ipinip tunnel-profile IPIP1	IPinIPトンネルプロファイル
57	profile-mode ipip	プロファイルモードをIPinIPに設定
58	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
59	destination ipv6 fqdn ##トンネル終端装置 FQDN##	トンネル終端装置のFQDN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 ipv6 fqdn example.com ※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するコマンドです。
60	ipinip fragment pre	プリフラグメント設定
61	exit	
62	!	
63	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。
64	!	

	設定例	補足
65	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）
66	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）
67	!	
68	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
69	!	
70	hostname FITELnet	hostname設定
71	!	
72	interface GigaEthernet 1/1	物理インターフェース（LAN側）
73	vlan-id 11	
74	bridge-group 11	
75	channel-group 11	LAN側論理インタフェース（Port-channel）と紐付け
76	policy-route input DNS-POLICY	LAN側ポリシールーティング設定
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側論理インタフェース（Port-channel）と紐付け
83	ipv6 access-group 4000 in	IPv6アクセスリスト紐づけ（NS/NA/RA/DHCPv6）
84	ipv6 access-group 4009 in	IPv6アクセスリスト紐づけ（deny）
85	ipv6 access-group 4010 out	IPv6アクセスリスト紐づけ（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 nd receive-ra prefix-delegation port-channel 11	RA-proxy設定
91	ipv6 router-lifetime-receive-enable	RA default経路登録設定
92	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。
93	ipv6 dhcp service client	DHCPv6クライアント設定
94	ipv6 dhcp client-profile NGN	DHCPv6クライアントプロファイル紐付け
95	exit	
96	!	
97	interface Port-channel 11	論理インターフェース（LAN側）
98	ip dhcp service server	DHCPv4サーバー設定
99	ip dhcp server-profile LAN	DHCPv4サーバープロファイル紐付け
100	ip address 192.168.0.1 255.255.255.0	IPv4アドレス設定
101	ipv6 enable	IPv6リンクローカルアドレス設定
102	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。
103	ipv6 nd other-config-flag	RA Oフラグセット
104	ipv6 nd send-ra	RA送信設定
105	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。
106	ipv6 dhcp service server	DHCPv6サーバー設定
107	ipv6 dhcp server-profile LANv6	DHCPv6サーバープロファイル紐付け
108	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。）
109	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
110	exit	
111	!	
112	interface Tunnel 1	トンネルインタフェース設定
113	ip access-group 111 out	IPv4アクセスリスト紐づけ
114	ip access-group 112 in	IPv4アクセスリスト紐づけ
115	ip access-group 113 out	IPv4アクセスリスト紐づけ
116	ip access-group 114 out	IPv4アクセスリスト紐づけ
117	ip access-group 115 in	IPv4アクセスリスト紐づけ
118	ip access-group spi ftp-data enable	学習フィルタ追加
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	class-map DNS6	ポリシールーティング用class-map
132	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）
133	exit	
134	!	
135	class-map DNS6_LO	ポリシールーティング用class-map
136	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）
137	exit	
138	!	

	設定例	補足
139	policy-route-map DNS-POLICY	ポリシールーティング用のポリシー設定
140	!	
141	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）
142	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）
143	count	クラスにマッチしたパケット数をカウントする設定
144	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。
145	exit	
146	!	
147	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）
148	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）
149	count	クラスにマッチしたパケット数をカウントする設定
150	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
151	exit	
152	!	
153	exit	
154	!	
155	local policy-route DNS-POLICY	自発パケットのポリシールーティング設定
156	!	
157	dns-server ip enable	DNSサーバ機能およびProxyDNS機能を有効化（IPv4）
158	dns-server ipv6 enable	DNSサーバ機能およびProxyDNS機能を有効化（IPv6）
159	!	
160	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）
161	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）
162	!	
163	end	