



Specifiche tecniche per la Connessione alla LAN di Peering MIX

CODICE DOCUMENTO : MIX-202
VERSIONE : 2.0
REPARTO : COMITATO TECNICO
STATO : DEFINITIVO
DATA DEL DOCUMENTO : 22/03/2011
NUMERO DI PAGINE : 7

RILASCIATO DA : VALERIA ROSSI

LISTA DELLE MODIFICHE

| VERSIONE | DATA | DESCRIZIONE |
|----------|----------|---|
| 1.0 | 15/07/06 | DOCUMENTO ORIGINARIO |
| 1.1 | 24/05/07 | 2.8: AGGIUNTA DI "MA PUÒ ESSERE REALIZZATO TRAMITE VLAN PRIVATE O CONNESSIONI BACK-TO-BACK [RIF. MIX-106]; 4.7: SOSTITUZIONE DI 217.29.67.1 CON 217.29.68.1 |
| 2.0 | 22/03/11 | REVISIONE COMPLETA |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |



| | | |
|----|---|---|
| 1. | Scopo..... | 4 |
| 2. | Norme generali..... | 4 |
| 3. | Norme di Livello 2..... | 4 |
| 4. | Norme di Livello 3..... | 5 |
| 5. | Traffico indesiderato sulla LAN di Peering..... | 6 |

1. Scopo

Nel presente documento vengono descritte le specifiche tecniche cui si atterranno gli ISP connessi al MIX per usufruire del servizio di peering sulla LAN pubblica del MIX. Le specifiche indicate, dettagliano e applicano le norme essenziali espresse nel “Regolamento di adesione al MIX” [Rif. MIX-101].

Si fa notare che le seguenti specifiche si applicano sia ai router di peering installati fisicamente nelle sale dati della MIX che ai router di peering connessi al MIX da una sede remota salvo che diversamente indicato (per le modalità di connessione al MIX si veda MIX-302).

2. Norme generali

- 2.1. gli apparati di peering sono installati fisicamente presso la MIX o sono installati in una sede remota; la scelta può essere vincolata al tipo di connessione geografica effettuata [Rif. MIX-302];
- 2.2. per le apparecchiature di peering installate nelle sale dati della MIX, si applicano i criteri espressi nel Regolamento e suoi Allegati;
- 2.3. nel caso, le apparecchiature sono installate dall'ISP che deve provvedere anche ai fissaggi delle stesse nei rack, il tutto eseguito a regola d'arte (per la lista del materiale necessario all'installazione fisica degli apparati nonché alla connessione degli stessi si rimanda a MIX-302);
- 2.4. ogni apparato installato è chiaramente identificato come appartenente all'ISP, tramite opportuna etichettatura ed è inventariato nell'apposito registro presso la MIX;
- 2.5. il collegamento geografico tra gli apparati di peering e la dorsale dell'ISP è effettuato solo tra apparati appartenenti allo stesso Autonomous System;
- 2.6. il transito verso Internet è preferibilmente realizzato tramite VLAN private o connessioni back-to-back [Rif. MIX-106];
- 2.7. le interfacce degli apparati di peering sulla LAN del MIX sono configurate in modalità “full-duplex” a velocità fissata e comunque non in modalità “autosensing”;
- 2.8. allo scopo di limitare i rischi derivanti da traffico non pertinente, ad ogni interfaccia degli apparati di peering connessi alla LAN del MIX viene staticamente assegnato da MIX un MAC address, utilizzato per l'applicazione di filtri a Liv.2.

3. Norme di Livello 2

- 3.1. Sono permesse sulla LAN di peering MIX trame Ethernet basate sullo standard Ethernet II (802.3) o ‘DIX Ethernet. L'incapsulamento LLC/SNAP non è quindi permesso
- 3.2. A livello di pacchetti Ethernet sono ammessi i seguenti Ethertypes:
 - 0x0800 IPv4
 - 0x0806 ARP
 - 0x086dd IPv6
- 3.3. Il MAC address assegnato alle interfacce del router dell'ISP avrà la seguente struttura logica:

00:17:A3:<id-cliente>:<mix code>

dove :

| Campo | Descrizione |
|---------------------|--------------------------------------|
| 00:17:A3 (24 bit) | Prefisso OUI assegnato da IEEE a MIX |
| Id cliente (16 bit) | AS Number del cliente |
| mix code (8 bit) | Identificativo dell'interfaccia |

- 3.4. Le trame indirizzate da/verso una porta degli switch del MIX hanno esclusivamente gli indirizzi MAC autorizzati a transitare su quella porta.
- 3.5. Le trame indirizzate da/verso una porta degli switch del MIX non indirizzano destinazioni MAC broadcast o multicast, tranne che per il protocollo ARP. MIX comunque applica un meccanismo di limitazione del traffico broadcast per porta.
- 3.6. Le interfacce dei router collegate agli switch del MIX non possono essere configurate all'uso del proxy ARP.
- 3.7. E' raccomandabile configurare ARP timeouts di almeno due ore sulle porte connesse a MIX, preferibilmente di quattro ore, per limitare il quantitativo di traffico di broadcast sulla LAN di peering dovuto al protocollo ARP. I meccanismi di restart delle sessioni BGP basati su TCP fanno sì che Timeout lunghi sulla persistenza delle informazioni nella ARP cache dei router di peering non influenzino i tempi di down delle sessioni stesse, in seguito al down di porte di Peering.
- 3.8. I protocolli di tipo 'link-local (ad eccezione di ARP e IPv6ND) non sono ammessi sulla LAN di Peering MIX. Appartengono alla famiglia dei protocolli Link-Local (la lista non è esaustiva)
 - o IRDP
 - o ICMP Redirects
 - o Protocolli proprietari come
 - Protocolli di Discovery: CDP, EDP etc.
 - Protocolli di Gestione VLAN come VTP e DTP
 - o Protocolli di Boot o assegnazione indirizzi IP come BOOTP o DHCP
 - o Protocolli OAM come UDLD e L2 Keepalives.

4. Norme di Livello 3

- 4.1. Le interfacce collegate alla LAN del MIX devono esplicitamente essere configurate per non permettere il directed broadcast sulla LAN di Peering;
- 4.2. gli indirizzi IP e le netmask associate, configurati sulle interfacce collegate agli apparati del MIX, sono esclusivamente forniti dalla MIX all'interno del proprio spazio di indirizzi pubblici.
- 4.3. le apparecchiature di peering sono configurate con protocollo BGP-4, unico protocollo utilizzabile per lo scambio di traffico tra gli ISP afferenti al MIX;
- 4.4. le apparecchiature di peering non hanno protocolli IGP attivi (come OSPF, ISIS, IGRP, EIGRP, RIP) verso la LAN del MIX;
- 4.5. le reti IP annunciate verso la LAN del MIX sono reti pubblicamente registrate presso RIPE o un registro equivalente, appartenenti all'Autonomous System dell'ISP o di suoi clienti a lui connessi;
- 4.6. le reti annunciate sono aggregate in modo ottimale per garantire il minor numero possibile di prefissi annunciati;
- 4.7. le apparecchiature di peering hanno una sessione di peering con i router del MIX di cui di seguito i dettagli:

AS: 16004

IPv4 addresses: 217.29.66.1 e 217.29.68.1

Reti Ipv4 annunciate: 217.29.72.0/21

IPv6 addresses: 2001:7F8:B:100:1D1:A5D1:6004:1/64

Reti IPv6 annunciate: 2001:1AC0::/32

- 4.8. le sessioni di peering con i router del MIX sono sessioni di peering locale e gli ISP non dovranno annunciare all'esterno le reti appartenenti all' AS 16004, salvo diversamente concordato con la MIX.
- 4.9. le apparecchiature di peering non annunciano come proprie le reti della LAN del MIX.

5. Traffico indesiderato sulla LAN di Peering

Tutto il traffico che non è esplicitamente premesso in base all'elenco visibile nel Capitolo 3 è da considerarsi traffico illegale sulla LAN di Peering MIX. Nel seguito viene presentata una lista delle violazioni più comuni e delle motivazioni per cui tale traffico è vietato.

- **Traffico da/per MAC address multipli su singola porta di Peering**

Salvo che nel caso del servizio "Pooling@MIX", MIX applica nella maggioranza dei casi il paradigma:

1 porta = 1 afferente = 1 MAC address attivo sulla LAN MIX

E' indispensabile che vi sia un solo MAC address visibile su ogni porta afferente. Essendo possibile la connessione agli switch MIX con uno switch Ethernet L2 come primo elemento di rete o con un dispositivo ibrido L2/L3, in caso di errori di configurazione o malfunzionamento degli stessi si possono verificare loop di instradamento instabilità legate a protocolli come lo Spanning Tree e in generale introduzione di traffico non voluto o non pertinente sul punto di Interscambio. Tale introduzione di traffico non pertinente non è in nessun modo giustificabile e non vi è alcuna ragione per mantenere attiva nello Spanning Tree la porta e/o la VLAN di connessione a MIX. I meccanismi di port security implementati da MIX permettono di identificare i sintomi di tali problematiche e vanno a proteggere l'integrità del punto di Interscambio, secondo una logica che ha impatto sia sul traffico generato dall'afferente, sia sullo stato attivo della porta di peering oggetto dell'anomalia.

Nel caso di configurazione di una porta in Pool le considerazioni lato afferente sono le medesime, anche se dalla prospettiva MIX l'equivalenza di cui sopra non è più univocamente verificata.

- **Spanning Tree (STP)**

Questa tipologia di traffico indesiderato è strettamente collegata a quella del punto precedente. Non vi è alcuna ragione per cui i dispositivi direttamente connessi a MIX siano visibili dagli switch di MIX come apparati attivi di Livello 2: quindi non vi è alcuna necessità di mantenere attivi verso MIX protocolli di controllo della tipologia L2 come Spanning Tree o simili

- **Protocolli di Routing Interno di Livello Tre**

Il traffico generato da protocolli di routing interno quali RIP, OSPF, EIGRP, IGRP o ISIS sia unicast che multicast non ha ragione di essere veicolato sulla LAN condivisa di MIX. L'unico protocollo di routing ammissibile su MIX è EBGP.

- **Protocolli di Auto Discovery**

Appartengono a questa famiglia protocolli come CDP e EDP. In generale vengono utilizzati per soluzioni di configurazione automatica di dispositivi di rete non pertinenti in uno scenario come MIX: il traffico unicast o multicast da essi generato è quindi indesiderato sul Punto di Interscambio.

- **Protocolli IPv4 non-unicast**

Appartengono a questa categoria protocolli come IGMP, DHCP e TFTP che generano traffico non unicast che, a differenza delle query ARP, non sono pertinenti sulla LAN di MIX.

- **Proxy ARP**

Essendo il traffico scambiato su MIX sotto il controllo esclusivo del protocollo BGP-4 non c'è alcuna ragione per uno qualsiasi dei router connessi alla LAN di Peering MIX di rendere disponibili funzionalità di Proxy ARP sulle LAN di peering. Purtroppo queste funzionalità sono spesso abilitate di default sulle porte Ethernet da parte di molti vendor. L'abilitazione di questa funzione non ha solo impatti negativi per l'Exchange Point ma sicuramente anche direttamente sulla rete dell'afferente che lo abilita, quindi è fondamentale il controllo che per nessun motivo il proxy ARP sia attivo sulle porte di Peering.

- **IPv6 ND-RA**

I router advertisement IPv6 non sono permessi sulle LAN di peering: essi generano molto traffico non necessario in quanto in sostanza non esiste un default router IPv6 sulla LAN di MIX

- **Traffico non IP**

Non è possibile far transitare altro traffico di rete su MIX che non utilizzi il protocollo IP. Anche in questo caso spesso i vendor abilitano le porte Ethernet alla gestione di default di altri protocolli (DEC MOP ad esempio) che devono essere inibite.