

## Videoconferenza su IP e attraverso INTERNET

La realizzazione di una videoconferenza su una rete IP (e più in generale su INTERNET) richiede alcune operazioni di verifica preliminari:

- I siti (o postazioni) coinvolti devono disporre di un collegamento Internet in grado di veicolare il flusso audio/video. A tal fine si consiglia di disporre di almeno 128Kbps di banda garantita per ognuno.
- Le postazioni da coinvolgere nella videoconferenza devono "vedersi", ovvero devono potersi raggiungere attraverso la rete IP (LAN/Internet). La verifica di questo requisito non è sempre semplice, ma a seconda della configurazione della propria rete, è possibile risolvere gli eventuali problemi di "visibilità" tra le postazioni.

Nel caso in cui le postazioni di videoconferenza siano installate:

1. Su rete pubblica
2. Su reti comunicanti all'interno delle quali non vi sono presenti firewall o apparati che effettuano la riscrittura degli indirizzi (NAT)
3. All'interno di una VPN

non sarà necessario prendere alcun provvedimento. Il protocollo H.323 utilizza infatti una combinazione conosciuta di porte statiche e dinamiche, e nel caso in cui non vi siano firewall, proxy e NAT, i flussi di videoconferenza transitano senza alcun problema. Nell'eventualità in cui sia invece presente un firewall a monte del sistema di videoconferenza, è necessario garantire il passaggio dei flussi di comunicazione mediante l'apertura di una gamma di porte comprese tra 1024 e 65535. Se il firewall non ne consente l'apertura limitatamente all'indirizzo del sistema di videoconferenza, l'operazione potrebbe compromettere la sicurezza e la difesa della rete, rendendo necessaria la valutazione di altri provvedimenti meno invasivi.

- **Firewall predisposto per il passaggio del protocollo H.323** – Una delle opzioni possibili è l'utilizzo di un firewall chiamato "snooping" ("ficcanaso"), in grado di controllare continuamente le porte H.323 e le richieste di autenticazione. Se autorizzati, la richiesta delle porte da utilizzare vengono aperte durante la conferenza. Al termine della conferenza, le porte sono immediatamente chiuse dal firewall.
- **VPN software** – I sistemi PC-based di Emblaze-VCON (vPointHD, HD4000, HD5000, xPoint) supportano la connessione su VPN fatta mediante software (ad es. client VPN Microsoft o Cisco). Tipicamente si hanno due indirizzi IP – uno fisico ed uno virtuale. Selezionando dall'applicazione l'indirizzo IP virtuale su cui la videoconferenza è veicolata, l'utente ha la possibilità di effettuare le chiamate verso gli altri utenti anche se questi sono dietro a firewall o NAT.

- **Configurazione di una gamma di porte** – Nel caso in cui i sistemi di videoconferenza in oggetto facciano parte di un'architettura MXM di Emblaze-VCON, attraverso il sistema di management possono essere configurate la gamma di porte RTP (Real Time Protocol), RTCP (Real Time Control Protocol) e H.245 utilizzate per i sistemi Emblaze-VCON e per il server di multiconferenza VCB di Emblaze-VCON. La riduzione della gamma di porte utilizzate permette una più facile gestione del firewall o la configurazione dell'H.323 "snooping".
- **Port Pinholing** – I sistemi Emblaze-VCON supportano il "port pinholing". Il protocollo H.323 non richiede necessariamente l'utilizzo della stessa porta dei flussi uscenti associata ai flussi entranti. Tale caratteristica di controllo permette l'associazione controllata sulle porte uscenti e sulle porte entranti. Ciò è particolarmente utile negli ambienti NAPT, in cui il firewall trasla le porte senza conoscere l'effettivo destinatario dell'applicazione. Poiché il sistema remoto rinverrà il flusso Video e Audio tramite la stessa porta controllata dal firewall, sarà più facile al firewall accettare tale flusso e trasferirlo verso la corretta destinazione.
- **Mascheramento dell'indirizzo IP via NAT** – I sistemi Emblaze-VCON permettono il mascheramento dell'indirizzo IP tramite NAT, in tal modo è possibile configurare manualmente l'indirizzo pubblico IP all'interno della applicazione. L'indirizzo pubblico sarà inserito nel pacchetto di segnalazione H.323 al posto dell'indirizzo IP interno. Questa soluzione funziona molto bene con IP NAT Statico ma non quando si utilizzano IP NAT dinamici. Con tale soluzione il sistema interno alla rete può effettuare chiamate verso sistemi su rete pubblica ma non può ricevere alcuna chiamata.

Nel caso in cui nessuna delle soluzioni fosse percorribile, Emblaze-VCON mette a disposizione l'architettura AES: una piattaforma client/server in grado di fornire servizi di Firewall traversal (mediante la realizzazione di una VPN leggera dedicata solamente alle comunicazioni in videoconferenza) ed alle cifratura dei dati (per una maggiore protezione delle comunicazioni).

Nella tabella della pagina seguente vengono indicati i protocolli, le porte statiche e le porte dinamiche richiesti dallo standard di videocomunicazione H.323.

**Attenzione: nel caso in cui il protocollo H.323 debba essere fatto passare attraverso un firewall, tutte le porte statiche e la gamma delle porte dinamiche devono essere aperte sia al traffico TCP che al traffico UDP.**

Porte IP e Protocolli utilizzati dai sistemi H.323						
Porta/e	Tipo	Descrizione	H.323 Client	Microsoft ILS	H.323 MCU	H.323 Gatekeeper
80	Static TCP	HTTP Interface (optional)			x	
389	Static TCP	ILS v2.0 Registration (LDAP)	x	x		
1002	Static TCP	Win 2000 ILS Registration	x	x		
1503	Static TCP	T.120	Non supportato	x		
1718	Static TCP/UDP	Gatekeeper Discovery	x		x	x
1719	Static TCP/UDP	Gatekeeper RAS	x		x	x
1720	Static TCP/UDP	H.323 Call Setup	x		x	
1731	Static TCP/UDP	Audio Call Control	x		x	
8080	Static TCP	HTTP Server Push (optional)			x	
22136	Static TCP	MXM endpoint administration	x			x (MXM)
26505	Static TCP	MXM remote admin login	x			x (MXM)
5004 - 6004	Dynamic TCP	H.245 (Call Parameters)	x		x	
5004 - 6004	Dynamic UDP	RTP (Video Stream Data)	x		x	
5004 - 6004	Dynamic UDP	RTP (Audio Stream Data)	x		x	
5004 - 6004	Dynamic UDP	RTCP (Control Information)	x		x	

Nota: l'utilità di upgrade di Emblaze-VCON utilizza le seguenti porte: 21 (FTP); 32000 (UDP); 60001 (HD).