Note: We recommend that you use other methods to restrict and block calls and do not rely solely on Cisco Unified MeetingPlace for restricting and blocking calls.

All outdial requests are independent of each other, except for the delay between outdials. They all go through the translation table in exactly the same way, looking for matches from the first entry to the last. Once the system selects a port group, the ports in the group will be always be selected starting from the lowest numbered one, for all outdial requests.

The following sections provide information about how hackers might try to circumvent the translation tables to allow calls that should be blocked and what you can do to avoid it:

- Smart Dialing
- Long Distance Access Numbers
- No Translation Characters

Smart Dialing

Problem: Hackers can circumvent translation tables by smart dialing, which means dialing in a certain way to bypass the translation table. For example, say a translation table for a Cisco Unified MeetingPlace system connected to the PSTN has the following entries:

From	To	PortGroup	DestType	Comment
976....	0	BLOCK	GENERIC	Block 976 calls own area code only.
...976....	0	BLOCK	GENERIC	Block 976 calls on all area codes.
.*	0	\0	GENERIC	No translation

The above entries may give the impression that all 976 calls in the local area code and all other area codes are blocked, and that all other calls can go through.

A hacker could circumvent this in more than one way, for example by dialing 976 1 2. This number, when checked against the translation table, does not match the first or second entries because the number of digits is different, but does match the third entry. Once the first five numbers are dialed and a voice path is created between the caller and the PSTN, a hacker can dial the rest of the digits and a call that should have been blocked will go through.

Another way to break the block of 976 calls with the above translation table is to dial more digits than the

ones specified: dialing "976 1234 5" or dialing "408 976 1234 5" would not be blocked.

Solution: This problem can be avoided by not including ".*" in the translation table. It can also be avoided by making more broad the detection of a 976 office code. For example:

From	To	PortGroup	DestType	Comment
976.*	0	BLOCK	GENERIC	Block all calls starting with 976

will block all calls that start with 976, no matter how many digits are dialed after 976. Also "...976....+" and "...976.+" will block the cases when more than four digits are dialed after the office code 976.

Long Distance Access Numbers

Problem: Access numbers for long distance carriers create opportunities to circumvent blocked calls. In the above example, if a hacker dials 10288 976 1234 or 10288 408 976 1234, plus any long distance carrier access number and then the 976 number, the system does not block the call.

Solution: This problem can be avoided by not including ".*" in the translation table. Also, the following entry will block all calls that use a long distance carrier access number:

From	To	PortGroup	DestType	Comment
10.*	0	BLOCK		

No Translation Characters

Problem: Having an entry such as ".*" at the end of a translation table, which means no translation and may allow calls that should be blocked.

Solution: To block calls, use the ".*" construct, but for calls that you want to allow, be as explicit as possible. You may initially block more calls than necessary, but you can adjust your translation table entries later.