Saxon - Bug #4971

Deleting an entry from NamespaceMap can cause IndexOutOfBoundsException

2021-04-17 01:20 - Michael Kay

Status:	Resolved	**Start date:**	2021-04-17
Priority:	Normal	**Due date:**	
Assignee:	Michael Kay	**% Done:**	0%
Category:	Internals	**Estimated time:**	0:00 hour
Sprint/Milestone:		**Spent time:**	0:00 hour
Legacy ID:		**Fix Committed on Branch:**	10, trunk
Applies to branch:	10, trunk	**Fixed in Maintenance Release:**	

Description

The code at NamespaceMap.put() reads

```
                n2.prefixes = new String[prefixes.length - 1];
                System.arraycopy(prefixes, 0, n2.prefixes, 0,position);
                System.arraycopy(prefixes, position+1, n2.prefixes, position+1, prefixes.length - position);
```

The last line crashes because the destination array is too short. I think the 4th argument should be position rather than position+1.

It looks to me as if this path is untested. The failure arose in Saxon-CS development, where the maintenance of namespace maps is handled differently, because the input comes from a pull parser. But the failure certainly could occur in Saxon-10, especially but not exclusively when run with a pull parser.

History

#1 - 2021-04-17 01:25 - Michael Kay

The correct statement appears to be

```
System.arraycopy(prefixes, position+1, n2.prefixes, position, prefixes.length - position - 1);
```

and similarly, *mutatis mutandis*, for the uri array a couple of lines further on.

#2 - 2021-05-12 18:34 - Michael Kay

- Category set to Internals

- Status changed from New to Resolved

- Applies to branch 10, trunk added

- Fix Committed on Branch 10, trunk added

Added a JUnit test NamespaceMapTest.testIncrementalRemove() which demonstrates the bug and shows that the suggested fix works.