

Tellabs® ServiceAssured™ Upgrade for the Tellabs® 8800 Multiserver Router Series

Deliver Continuous System Availability

Tellabs® ServiceAssured™ Upgrade enables service providers to achieve the highest availability time in the industry. By upgrading the Tellabs® 8800 Multiservice Router (MSR) Series, service providers can assure that software-related maintenance upgrades do not adversely affect existing revenue streams. This paper provides a technical overview for performing a Tellabs ServiceAssured Upgrade and the steps necessary to complete the software upgrade process.

Requirements

Tellabs ServiceAssured Upgrade is available for Tellabs 8800 MSR series platforms with redundant designs including: Tellabs® 8860 Multiservice Router, Tellabs® 8840 Multiservice Router and the Tellabs® 8830 Multiservice Router. The minimum configuration requires two Switch Controller Cards (SCC). The target software release version is FP8.0.0.x and can be initiated from FP7.2.1.6 or later when upgrading to FP8.0.0.x. To ensure successful completion of the upgrade, the system must be functional and in a fully redundant state.

How it Works

A Tellabs ServiceAssured Upgrade is performed via a two-phased approach: 1) The preparation phase takes the node through a sequence of steps to ensure that it is fully functional and in service at the time of the Tellabs ServiceAssured Upgrade; and 2) The execution phase initiates the node upgrade process and performs a series of steps to complete the procedure. To ensure minimal user intervention, many of the critical steps in the execution phase are automated.

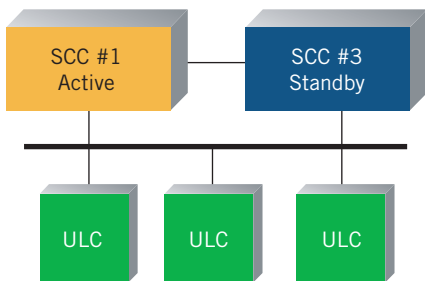


Figure 1. Tellabs 8800 MSR series with FP7.2.1.6 and FP8.0.0.x on all ULCs

In Figure 1, FP8.0.0.x is downloaded to SCC #1 and SCC #3 and all three Universal Line Cards (ULC). (Note: the Tellabs 8830 MSR uses only two SCCs, SCC #1 and SCC #2). Downloading the target software to the SCCs and the ULCs has no impact on the traffic flow. The SCCs and ULCs can store multiple versions of software.

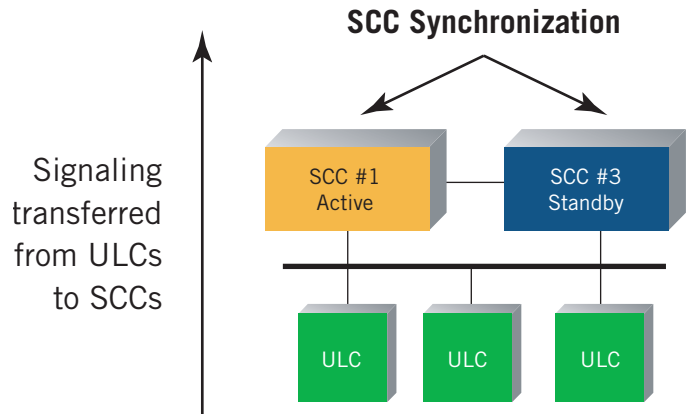


Figure 2. Upgrade SCC #3 and Synchronization

The target software and the currently running software are stored on the Random Access Memory (RAM) and the flash disk. This assures that the system can revert to the original code if any failure is encountered during the upgrade procedure. After the download, the system operates on FP7.2.1.6 software with FP8.0.0.x as the target software resident in memory.

The node is now ready to enter the preparation phase where a sequence of steps verifies node redundancy and full operational functionality. Once the preparation phase is completed, the node is ready for the execution phase.

In the execution phase, the first element upgraded is the standby SCC module. By resetting the SCC #3 card (SCC #2 on a Tellabs 8830 MSR) it becomes operational with FP8.0.0.1 software. SCC #3 then synchronizes with SCC #1 by receiving checkpoint data from SCC #1 as shown in Figure 2. During this step, data conversions are done and the configuration files are stored on SCC #3 with the new FP8.0.0.1 database format. This process saves a complete copy of the database in memory on both the active and standby SCC. This enables the operator to revert back to the original mode of operation if desired. The node is no longer fully redundant, and no configuration changes are allowed. Once the synchronization is completed, the configuration file and the database residing on both SCCs are identical.

After synchronization, the system is now ready to enter the isolation period. This ensures that data and configuration integrity is maintained during the execution of the upgrade procedure. During the isolation period, typically lasting 2 to 13 minutes

(depending on the database size), alarms, routing updates and configuration changes are ignored. The signaling (e.g., RSVP hellos) is transferred from the ULCs to the active SCC for each application. By transferring the signaling to the SCC, the ULC software is no longer in the critical path for maintaining and passing circuit data.

The ULCs are then upgraded to FP8.0.0.x through a soft reset as shown in Figure 3. By transferring the signaling function to the SCC, the Tellabs ServiceAssured Upgrade prevents a soft reset of the ULC due to signaling errors and an eventual link failure report by a remote node. Each ULC reloads the FP8.0.0.x software from RAM, which minimizes the startup time for the ULCs. ULCs do not write to hardware as traffic continues to be forwarded. All Layer 2 and Layer 3 sessions such as LSPs, OSPF, IS-IS are fully maintained by SCC #1 during the reload. The ULCs replay connection information from the active SCC and create a RAM image, but do not write to the hardware at this point.

After all of the ULCs completely reload, they rewrite all of the hardware (PP, PM, PS, CAM) at once to match the reloaded configuration. The signaling on the SCC is also suspended. The process is synchronized so that connections, microcode and CAM entries across all ULCs are from the same FP8.0.0.x version before activating the traffic flow again. During this rewrite step, there is a short period (<2.5 seconds) where traffic forwarding halts while the hardware reinitializes.

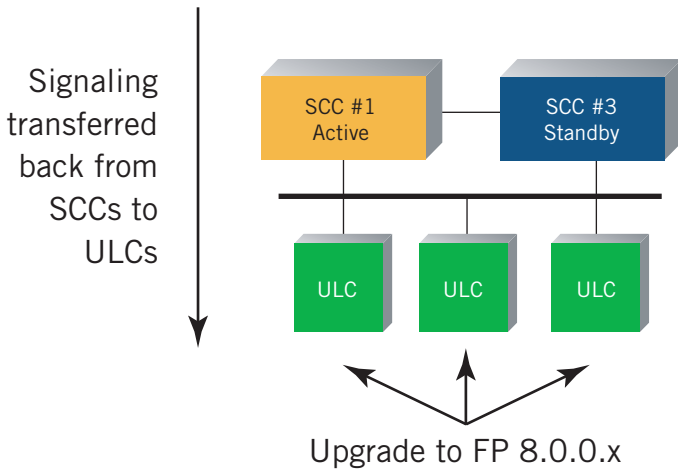


Figure 3. Upgrade all ULCs to FP8.0.0.x

Once all the connections, microcode and CAM entries are synchronized across all the ULCs, signaling functionality is returned to the ULCs.

The node now performs an SCC switchover as shown in Figure 4, where SCC #3 running the target software becomes active and node isolation ends. SCC #1 is reset and reloaded with the target software and becomes the new standby after synchronizing with the active SCC. The node is now fully redundant and operational with the target software version.

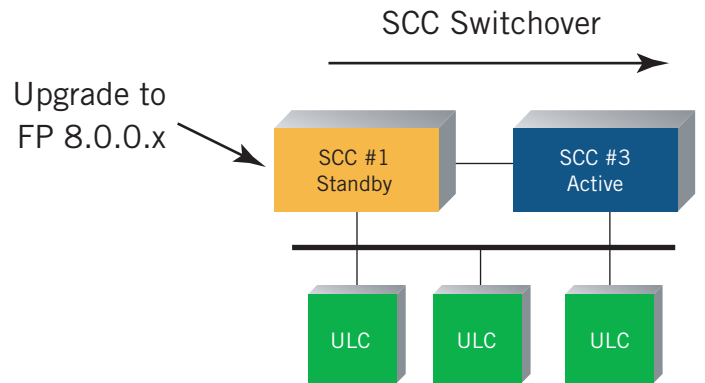


Figure 4. Fully redundant with FP8.0.0.x

Summary of ServiceAssured Upgrade Steps

The entire Tellabs ServiceAssured Upgrade process is shown with the timing diagram in Figure 5. Prior to the preparation phase, the SCCs and ULCs are loaded with the target FP8.0.0.x software. During the preparation phase, the system undertakes internal checks and verifications to assure that the software upgrade is successful. The node is checked to make sure that it is fully functional and completely redundant. The operator then issues an “enable config node upgrade” command to initiate the SCC reset.

At this stage, the system is no longer fully redundant. Once the standby SCC recovers and is operational with FP8.0.0.x, the user is prompted before entering the isolation phase. Prior to entering the isolation phase, any abort or failure reverts the node to the old software (FP7.2.1.6) with no effect on network traffic.

If the user decides to proceed with the upgrade, the node enters the isolation mode. During the isolation phase, signaling is first transferred from the ULCs to the active SCC. The ULCs then reload and the SCC performs a final switchover. The hardware on the ULCs is reprogrammed during this period.

It is important to note that upon initiating a standby SCC reset before the time the node exits the isolation period, no configuration changes or routing updates are accepted. During the isolation phase, an abort or failure reverts to old software only through a node reset. The purpose of having the isolation mode is to assure that the upgrade sequence proceeds successfully without any external interruptions (i.e. configuration changes).

Once the system leaves the isolation phase, the upgrade is complete and the standby elements are reloaded and synchronized with the active elements. The node at the completion of this stage is fully redundant and operational.

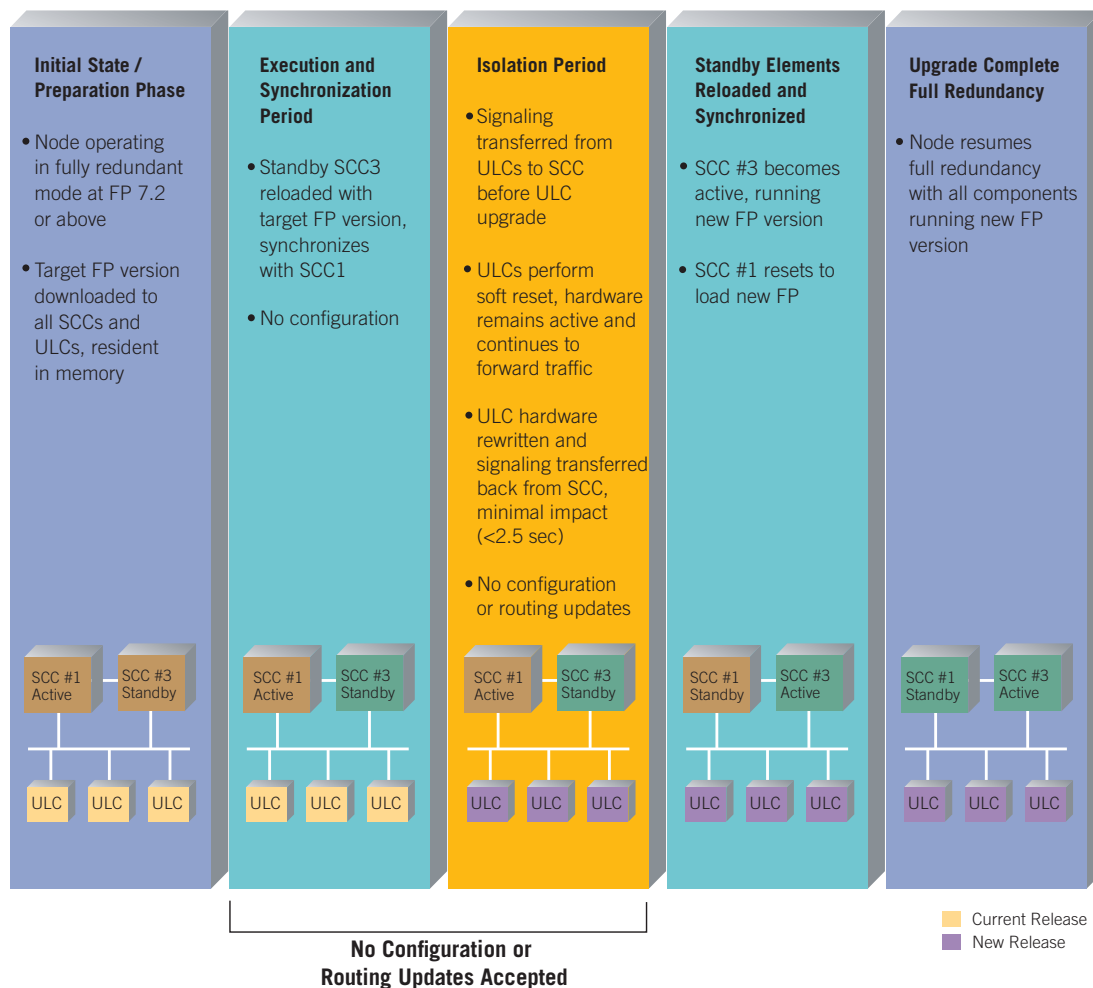


Figure 5. Tellabs ServiceAssured Upgrade Summary

Graceful Restart

The Tellabs 8800 MSR series supports the following standards-based graceful restart and nonstop routing mechanisms to ensure the control connections remain active during the Tellabs ServiceAssured Upgrade process:

- IS-IS graceful restart
- BGP graceful restart
- LDP fault tolerance
- RSVP stateful redundancy (non-stop routing)
- OSPF stateful redundancy (non-stop routing)
- Non-stop Bidirectional Forward Detection (BFD) sessions with auto-adjustments of BFD timers

The Tellabs 8800 MSR series achieves high availability in IS-IS with the graceful restart mechanism as defined in RFC 3847. When control traffic switches over from the active SCC to the standby SCC, the graceful restart mechanisms are deployed to reacquire the adjacencies and the link state database without any adjacency flaps on the neighboring routers. During the SCC switchover, IS-IS hello Protocol Data Units (PDU) are continuously sent from the ULCs so that the adjacencies are maintained with neighboring routers. IS-IS routes are maintained in the forwarding tables throughout the SCC switchover operation.



For Border Gateway Protocol (BGP), graceful restart is an important feature. This protocol carries a large number of routes relative to other protocols and, consequently, the network may take longer to reach equilibrium after a BGP failure. BGP usually runs at the network edge, affecting the critical link between businesses and the service provider network. Therefore, a failed BGP process can potentially affect multiple networks.

In BGP graceful restart, the multiservice router may lose its TCP connection to the peer router. Instead of clearing all routes associated with the failed router, the peer router simply marks all routes as stale. It continues to use the routers to forward packets while waiting for the failed router to re-establish the BGP session. All configuration and various states are actively saved on the standby SCC of the multiservice router.

Throughout the failover process, the IP forwarding table is maintained in the ULC hardware, ensuring that all packet forwarding is unaffected and BGP peers maintain routes learned from the Tellabs 8800 MSR platform. When the switchover is complete and the new BGP session begins, it will again send BGP capability to its peers. Appropriate flags are set in the graceful restart capabilities exchange to inform the peer router that the BGP process has restarted.

To assure non-stop BFD sessions during the Tellabs ServiceAssured Upgrade, larger values of BFD timers are automatically negotiated with all BFD neighbors (without operator intervention). This requires that BFD packet drops during the ASIC re-write period are within the adjusted BFD timer and BFD sessions remain up during the upgrade. The original BFD timer values are restored after the upgrade is completed.

Other mechanisms employed by the multiservice router include LDP fault tolerance as defined by RFC 3479, RSVP and OSPF stateful redundancy. These work with the redundant components in the Tellabs 8800 MSR series to offer the highest availability possible to the end-customers.

Summary

The Tellabs ServiceAssured Upgrade process provides increased network service availability and protection against planned downtime by offering a true in-service software upgrade procedure to service providers. Deploying Tellabs 8800 MSR series with Tellabs ServiceAssured Upgrade capabilities at critical network locations improves system and service availability and helps service providers meet availability conditions set through Service Level Agreements (SLA). With a Tellabs ServiceAssured Upgrade, service providers can offer continuous network service and connectivity.

North America

Tellabs
One Tellabs Center
1415 West Diehl Road
Naperville, IL 60563
U.S.A.
+1 630 798 8800
Fax: +1 630 798 2000

Asia Pacific

Tellabs
3 Anson Road
#14-01 Springleaf Tower
Singapore 079909
Republic of Singapore
+65 6215 6411
Fax: +65 6215 6422

Europe, Middle East & Africa

Tellabs
Abbey Place
24-28 Easton Street
High Wycombe, Bucks
HP11 1NT
United Kingdom
+44 871 574 7000
Fax: +44 871 574 7151

Latin America & Caribbean

Tellabs
1401 N.W. 136th Avenue
Suite 202
Sunrise, FL 33323
U.S.A.
+1 954 839 2800
Fax: +1 954 839 2828