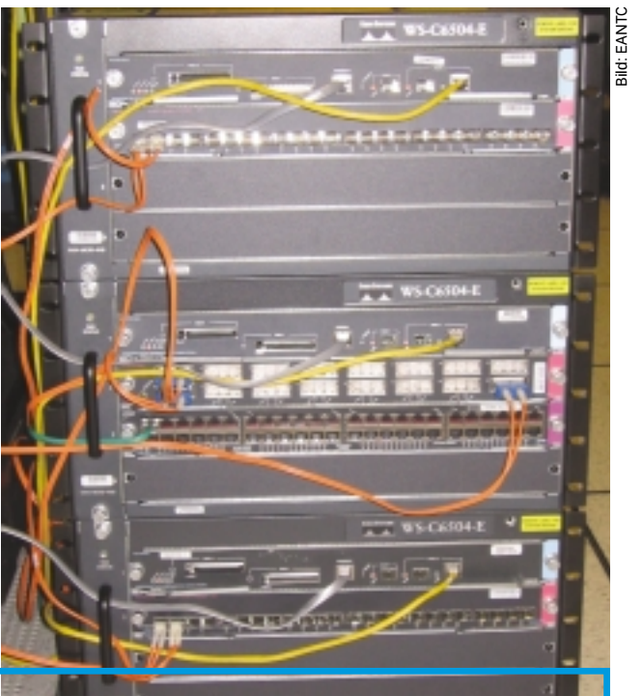

Bild: EANTC

Für Provider und Unternehmen wird es immer wichtiger, dass ihre Netze hoch verfügbar sind: Die Kunden fordern stete Erreichbarkeit von Internet- und anderen Datendiensten. Besonders Triple Play und VPNs sind Motor dieser Entwicklung, die auch erhöhte Anforderungen an die Software der Netzkomponenten bedingt.

Catalyst 6500 mit IOS Software Modularity im Test

Von Bernd Klusmann

Zusätzlich zu der hoch verfügbaren Auslegung der Netze, einschließlich redundant ausgelegter Hardware, wird deshalb von der Software der Netzkomponenten ebenfalls höchste Verfügbarkeit gefordert, wenn strikte Ende-zu-Ende-SLAs (Service Level Agreements) einzuhalten sind. Zwei redundante Prozessormodule nutzen nichts, wenn jedes Software-Upgrade einen mehrere Minuten dauernden Neustart (und damit Komplettausfall aus Kundensicht) erfordert.

EANTC testete die neueste, erstmals modulare Version des Cisco-Catalyst-Betriebssystems (IOS; Internet Operating System). Darin wird die Funktionalität modularer Software, die bisher ausschließlich auf Cisco Carrier-Router wie dem CRS-1 (siehe funkschau „40-GBit-Router im Test“, 1/2005, S. 38-39) verfügbar war, erstmals auch für Geräte angeboten, die in Unternehmensnetzen in Verteilerräumen, Rechenzentren oder im Anschlussbereich des WANs eingesetzt werden. Cisco Systems beauftragte das EANTC Ende August diesen Jahres, eine unabhängige Überprüfung des neuen IOS-Releases mit Software-Modularität durchzuführen.

Bernd Klusmann ist Projektmanager beim EANTC. Er leitet Tests bei Unternehmenskunden und Serviceprovidern.

Testkonfiguration und -methodik

Die Testkonfiguration bestand aus insgesamt drei Cisco Catalyst 6504-E (siehe Grafik „Logical Test Setup“). Das mittlere Gerät war das so genannte „DUT (Device Under Test)“, die anderen beiden stellen die NSF-Funktionalität (Non-Stop-Forwarding) bereit. Zu Beginn des Tests liefen alle drei Catalyst mit der generell verfügbaren IOS-Version 12.2.(18)SXE2. Während der Tests führten wir ein Software-Upgrade auf ein FCS (First Customer Shipment) Release 12.2 (18)SXF1 durch, dem ersten geplanten Release für die Catalyst-6500-Serie mit Cisco IOS-Software-Modularität.

Der Switch 1 repräsentiert die Grenze eines Serviceproviders, der 180.000 E-BGP-Routen (Border Gateway Protocol) vom Smartbits-Lastgenerator empfängt. Der Switch 3 repräsentiert einen Catalyst in einem Unternehmensnetz, der vom Smartbits-Lastgenerator 10.000 OSPF-Routen (Open Shortest Path First) bekommt. Das DUT, der Switch 2, wurde in die Verbindung dieser beiden Switches mittels BGP und OSPF konfiguriert, womit der Switch in Summe 190.000 Routen halten musste. Mit voll vermaschtem Verkehr haben wir insgesamt 3,6 Millionen unterschiedliche Verkehrsströme generiert. Für die Tests nutzten wir zwei GbE-Ports, die wir mit bidirektionalen Testdatenströmen zu je 95 Prozent der Link-Bandbreite auslasteten, um noch den Austausch von Steuerungsdaten, etwa für die Routing-Protokolle BGP und OSPF zu erlauben. In dieser Konfiguration leitete der Catalyst insgesamt 2,828 Millionen 64-Byte-Pakete pro Sekunde je Übertragungsrichtung ohne Paketverlust weiter; wir ermittelten eine mittlere Paketlaufzeit von 21,2 Mikrosekunden.

1. Migration auf IOS mit Software-Modularität

Dieser Test hatte das Ziel, die Migration von einem Release ohne auf ein Release mit SW-Modularität zu evaluieren. Nachdem wir die neue Software über FTP auf die Supervisor Engine des Catalyst geladen und den Bootstring auf das neue Image konfiguriert hatten, führten wir ein Reboot

des Switches durch, um das modulare IOS im so genannten „Binary Mode“ zu laden. In diesem Modus besteht das IOS noch aus einem einzelnen Image, während der „Installed Mode“ auf ein Filesystem aufbaut („bootdisk:“ oder „disk0/1:“), in welchem dann auch Patches auf einzelne Module der Software ausgeführt werden können. In dem „Binary Mode“ prüften wir die Konsistenz der Konfiguration und das CLI. Nachdem wir in den „Installed Mode“ gewechselt hatten, prüften wir über verschiedene „show-“Befehle („show install running“ oder „show install disk0:/sys“) die neue Installationsumgebung. Zur weiteren Überprüfung der Prozessarchitektur nutzten wir erweiterte Befehle, „show process“ und „show process cpu“, womit wir mehr als 20 modulare Prozesse beobachteten.

Für die Migration auf das neue 12.2SX-Release mit Software-Modularität waren nur wenige einfache Schritte nötig. Die neue IOS-Version veränderte in keiner Weise die Konfiguration des Gerätes (mit Ausnahme des Bootstrings), das „Look & Feel“ sowie das CLI änderten sich ebenfalls nicht. Mit Ausnahme des Systemstarts zur Aktivierung der neuen Software konnten wir zu keiner Zeit Paketverluste oder eine erhöhte Paketlaufzeit feststellen.

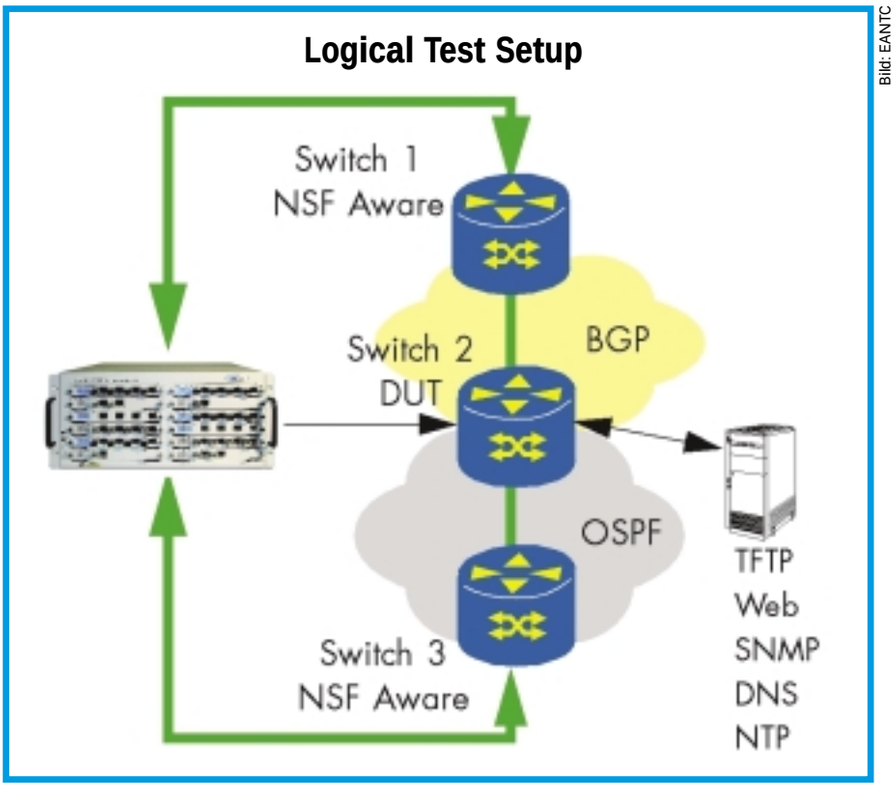

Bild: EANTC

Die Testkonfiguration bestand aus insgesamt drei Catalyst 6504-E-Geräten

2. Prozess-Restart und NSF-Funktionalität

Mit diesem Test sollte gezeigt werden, dass modulare Prozesse, wie der Routing-Prozess, der für BGP und IGPs verantwortlich ist, neu gestartet werden können, ohne ein einzelnes Paket der Testdatenströme zu verlieren. Vorbedingung für diese Tests war die Interoperabilität der BGP- und OSPF-Nachbarn zum NSF-Protokoll um Route-Flaps und dadurch bedingte Paketverluste aufgrund kurzzeitig fehlender Nachbarschaftszuständen zu vermeiden.

Vor und nach dem manuellen Neustart des Routing-Prozesses „iprouting.iosproc“ beobachteten wir den detaillierten Prozessstatus mit „show process detail iprouting.iosproc“. Parallel zum Prozess-Neustart sendeten wir unseren Referenzteststrom, um die NSF-Funktionalität zu beobachten, das heißt zu prüfen, dass keine Pakete verloren gingen. Wie erwartet konnten wir keinen Paketverlust und nur einen sehr kurzen, minimalen Anstieg der Paketlaufzeit (Aktualisierung der HW-Tabellen mit den neu kalkulierten Routen) während des Prozessneustarts beobachten.

3. Patch Management (ISSU, Rollback und Repackaging)

Mit diesem Test sollte gezeigt werden, dass Angriffe auf zwei bekannte und für diesen Test erneut in das IOS-Image eingefügte Schwachstellen, die zu einem Neustart eines Prozesses führen, keinen Paketverlust beziehungsweise keine Dienstunterbrechung zeigen. Ebenso wenig sollte ein Prozessneustart aufgrund eines daraufhin eingefügten Patches zu Paketverlust oder erhöhter Paketlaufzeit führen. Weiterhin sollten mit diesem Test noch folgende Punkte gezeigt werden:

- Prozessstatusinformationen prüfen,
- Installation und Aktivierung eines Patches,
- Zurückspringen zu definierten Patch-Zuständen über so genannte „Tags“ und über die „Rollback“-Funktion und
- Abbilden eines bestimmten Patch-Status in einem neuen Image über die „Repackaging“-Funktion und Neuinstallation dieses Images.

Insgesamt nutzten wir für diesen Test drei unterschiedliche Patches, zwei bezogen sich auf zuvor von Cisco korrigierte Fehler (siehe www.cisco.com/go/psirt), die speziell für diesen Test wieder in das IOS-Release eingefügt wurden, und ein Patch veränderte die Ausgabe des Befehls „show cdp neighbor“.

Bei dem ersten Fehler (PSIRT Dokument-ID 61365) konnte der Switch über ein auf bestimmte Weise nachgebildetes OSPF-Paket zum Reload gebracht werden. Der zweite Fehler (PSIRT Dokument-ID 50960) bezog sich auf ein spezielles TCP-Reset-Paket, mit welchem TCP-Verbindungen abgebrochen werden konnten. In einem Referenztest überprüften wir die jeweils eingebauten Fehler auf das erwartete Fehlverhalten, nach der Installation der Patches machten wir einen Gegentest.

Nach dem Ende der Tests nutzten wir das „Rollback”-Feature und die Informationen aus zuvor konfigurierten „Patchtags“ um in der Patch-Historie einen Schritt zurückzugehen. In diesem Status erstellten wir mittels der „Repackage-“Funktion aus dem Basisimage und den aktiven Patches ein neues binäres Image. Dieses neue Image installierten wir anschließend und aktivierten auf das neue Filesystem den CDP-Patch. Nach einem Reboot prüften wir die Konsistenz des installierten Images sowie den Patch, den wir auf das noch nicht aktive System angewendet hatten. Während sämtlicher beschriebener Tests prüften wir, dass unsere Referenztestströme keinen Paketverlust zeigten und dass die Paketlaufzeit nicht anstieg.

Der Cisco Catalyst 6500 mit IOS-Software-Modularity erfüllte in allen Testbereichen die Cisco-Spezifikationen im Hinblick auf Funktionalität und Hochverfügbarkeit. Durch den Einsatz von „stateful process restarts“ und „ISSUs“ wird die Verfügbarkeit der Systeme deutlich erhöht, und damit die Risikoabschätzung SLA-relevanter Dienste für Serviceprovider ein Stück kalkulierbarer. *(AW)*

Der vollständige Testbericht kann von der EANTC-Homepage unter **www.eantc.de/test_reports** heruntergeladen werden.