Cisco ASR 9000 Series High Availability: Continuous Network Operations

The Challenge of Delivering Continuous Network Operations

End users require the network to be up at all times with little to no service disruption.

For service providers, offering continuous network operations is a basic requirement for all applications. Residential customers require access to data, voice, and video services at all times. Enterprise business customers depend on 24-hour network operations that require strong service-level agreements (SLAs) for mission-critical applications. Mobile phone subscribers expect to be able to make calls and access data services at all times. Best-effort service is no longer an option for most of today's applications. As service providers converge to a single, packet-based Carrier Ethernet network providing residential, business, and mobile services, network elements must be built for continuous system operations to meet these demands. In addition to node-level resiliency, service providers require network resiliency in order to provide service delivery even when network nodes or links fail.

Introduction

The Cisco® ASR 9000 Series deliver exceptional high availability into Carrier Ethernet transport networks for applications including residential broadband services, efficient IPTV and video distribution, voice over IP (VoIP), business VPN services, wholesale services, and mobile applications such as backhaul transport. To support these applications, the Cisco ASR 9000 Series is designed to work with many different types of access technologies, to reach consumer and business customers (for example, DSL, passive optical networks [PONs], Ethernet, cable, and mobile). The router is powered by Cisco IOS® XR Software—an innovative self-healing, distributed operating system designed for continuous system operations and supporting network resiliency to maximize overall network availability for these applications.

This paper focuses on the following continuous network-operations capabilities the Cisco ASR 9000 provides in order to maximize service availability:

- **Continuous system operations:** Redundant system design with intelligent software providing carrier-class service availability
- **Network resiliency:** Redundant network design with intelligent software to protect against unexpected network link and node failures

Continuous System Operations Overview

The primary design objective for a resilient, highly available Carrier Ethernet system is to gracefully handle both planned and unplanned downtime with minimum service disruption. Planned downtime typically consists of software and hardware maintenance tasks such as adding new features and services and performing configuration and policy changes, error corrections, and system upgrades. Unplanned downtime is generally the result of a software or hardware failure, configuration error, out-of-resource violation, security violation, or even natural disaster.

The critical design concept used in creating a high-availability infrastructure is to minimize and protect against single points of failure. The Cisco ASR 9000 Series achieves that goal in a scaled network environment through a combination of carrier-class hardware design and software resiliency through Cisco IOS XR Software.

Hardware Redundancy

The Cisco ASR 9000 provides a carrier-class solution to Carrier Ethernet service delivery by taking advantage of Cisco experience in core routing and extending that design to the network edge. Newer routing design should support distributed architectures with distributed asynchronous forwarding engines and distributed asynchronous route-processing capabilities to remove single points of failure. As a next-generation routing platform, the Cisco ASR 9000 offers several additional redundancy features, including route switch processor (RSP), switch fabric, power supply, fan tray, line card, and operating-system redundancy:

- **Route switch processors (RSPs):** RSPs are deployed in “active” or “standby” configurations. The Cisco ASR 9000 Route Switch Processor is designed with load-shared redundancy to support software upgrades and software patches.
- **Switch fabric:** Using an active/active configuration model allows for distribution of the traffic load across both switch fabrics, taking advantage of the processing capacity of both switch fabrics. If a failure occurs, the single active switch fabric continues to forward traffic in the system, with hardware support for zero packet loss on fabric online insertion and removal (OIR). Because both switch fabrics are active and forwarding traffic, they are both ready to assume the full traffic load.
- **Power supplies:** Redundant power supplies are deployed in load-balanced configurations to share the load across all power supplies. You can also configure the power supplies in 1:1 and 1:N modes to provide power-supply redundancy. An example of this configuration is 3:1 redundancy, where one redundant power supply is used to back up the other three power supplies.
- **Fan trays:** Redundancy is offered on a single fan tray (that is, through multiple fans) and between fan trays. If a fan tray fails, fan-tray redundancy allows for the protection of the fan tray, giving service providers an alarm and time window over which they can replace the failed fan tray.
- **Line cards:** The Cisco ASR 9000 Series can handle faults by bundling and protecting ports together on multiple line cards by supporting IEEE 802.3ad Link Aggregation. Cisco ASR 9000 linecard redundancy is supported through the bundling of up to eight interfaces across line cards into a single, logical Layer 2 or Layer 3 connection. Fast failover between ports within a bundle occurs if any port fails, providing more flexibility than simple linecard redundancy. This allows service providers to support stringent customer SLAs.
- **Operating system:** System infrastructure components are distributed to all cards in the system, and relevant data is replicated on different cards based on usage. This setup avoids single points of failure and allows distribution of applications based on resource availability.

These features are used to deliver hardware redundancy for the node. Now consider the software operating system running on the node.

Software Resiliency Through Cisco IOS XR Software

The Cisco ASR 9000 Series high-availability infrastructure is delivered through the distributed and modular design of the Cisco IOS XR Software Operating System. By using a preemptive microkernel in combination with a distributed hardware architecture, Cisco IOS XR Software offers highly available, flexible, and modular services with high performance.

The Cisco IOS XR Software microkernel architecture offers granular fault isolation, protection, and graceful recovery, keeping the mean time to repair (MTTR) low. System infrastructure process (for example, TCP/IP stack) failure is generally recoverable and does not cause failure of a RSP or line card -- or the entire system.

As a true distributed architecture, Cisco IOS XR Software runs an independent copy of the operating system on every Cisco ASR 9000 Series Line Card. As a result, a software fault on one line card does not affect others. Discrete software components (subsystems) are implemented as separate processes, each running in a protected address space so that faults or memory corruption in one subsystem cannot negatively affect another. You can restart device drivers and protocol stacks without bringing down a card or the system, and you can use the drivers and protocol stacks in conjunction with packet Nonstop Forwarding (NSF) and Nonstop Routing (NSR). Important aspects of the intelligent design of Cisco IOS XR Software include modularity, process restart, fault handling, continuous forwarding, and upgradability.

Modularity

Modularity is an important attribute when preparing for planned events and guarding against unplanned ones. To protect against unplanned downtime, most current-generation routers offer hardware redundancy, fault handling, and failover features. However, because they do not support continuous system operations during maintenance cycles, these routers can create service downtime and add to operational expenses through time-consuming tasks.

The Cisco ASR 9000 supports continuous system operation during planned and unplanned downtime through its modular hardware and Cisco IOS XR Software design with features such as:

- **Release modularity:** Cisco IOS XR Software is based on a development model in which features consist of components. These components are aggregated into installation packages and composites that can be independently upgraded, and are pretested and certified for use in service provider networks.
- **Run-time modularity:** Deployed features and components are broken down into processes, supporting fine granularity of fault isolation, restarts, and upgrade capability. Cisco IOS XR Software avoids a performance penalty by supporting multiple threads that perform tasks in parallel, taking full advantage of the Cisco ASR 9000 Series hardware architecture.
- **Physical distribution of components:** Software components are distributed and replicated across line cards and RSPs, creating fault isolation for resiliency.
- **Logical distribution of components:** Cisco IOS XR Software separates software into three distinct planes -- the control, management, and data planes. Planned or unplanned outages on any of the planes do not affect services on others.

Process Independence and Restart

Modern network operating systems require millions of lines of code to implement protocol stacks, management interfaces, control-plane features, file systems, device drivers, and other critical services and features. To minimize the effect that failure in any of these processes can have on other processes, each process must execute in its own protected memory space, and communications between processes must be accomplished through well-defined, secure, and version-controlled application programming interfaces (APIs).

To support continuous system operations, allow for In Service Software Upgrades (ISSUs), and ensure quick recovery from process or protocol failures with minimum disruption to customers or traffic, every process in the system must be capable of restarting while minimizing effect on services. Granularity of process restart during software upgrades allows system operators to restart perhaps a few thousand lines of code instead of the millions that might comprise the entire operating system. The Cisco IOS XR Software distributed and modular microkernel operating system enables process independence, restartability, and maintenance of memory and operational states. By providing protected memory space for system processes such as the TCP/IP stack, file system, device drivers, and routing protocols, Cisco IOS XR Software offers granular support of fault handling and upgradability.

Fault Handling

Although the quantity of faults can be reduced through quality design, the nature of unplanned events makes fault handling a reality of network operations. To prepare for these conditions and maintain low MTTR, a high-availability infrastructure must provide rapid and efficient response to single or multiple system component or network failures to minimize service outage. When local fault handling cannot recover from critical faults, the system should offer robust fault detection, correction, failover, and event management capabilities.

- **Fault detection and correction:** Both Cisco ASR 9000 Series hardware and software support fault detection and correction. In hardware, the router offers error correcting code (ECC)-protected memory. If a memory corruption occurs, the system automatically restarts the affected processes to fix the problem with minimum effect. If the problem is persistent, the Cisco ASR 9000 supports switchover and OIR capabilities to allow replacement of defective hardware without affecting services on other hardware components in the system.
- **Resource management:** As part of its fault-handling capabilities, the Cisco ASR 9000 Series supports resource threshold monitoring for CPU and memory usage to improve out-of-resource (OOR) management. When threshold conditions are met or exceeded, the system generates an OOR alarm to notify operators of OOR conditions. The system then automatically attempts recovery, and allows the operator to configure flexible policies using the Cisco IOS Software Embedded Event Manager (EEM). The system also reserves some system memory to allow the operator to log in and clean the system during worst-case OOR conditions. This setup provides a proactive—rather than a reactive—solution, avoiding router reset and network reconvergence.
- **Switchover design:** Cisco IOS XR Software allows system processes such as the TCP/IP stack, device drivers, routing protocols, and signaling stacks to be restarted on individual RSPs or line cards without causing service outage. In circumstances where process dependencies are distributed across separate, failed hardware or software components, recovery can require a large amount of time. To support continuous system operations, the

Cisco ASR 9000 supports a fast switchover of traffic when linecard protection mechanisms are enabled. It also uses redundant RSPs in a rapid and flexible RSP switchover configuration while maintaining NSF and NSR, allowing services to be designed to the most appropriate active or standby mode based on their scale, performance, and availability requirements.

- **Event management:** Cisco ASR 9000 embedded manageability offers mechanisms such as fault-injection testing to detect hardware faults during lab testing, a system watchdog mechanism to recover failed processes, and tools such as the Route Consistency Checker to diagnose inconsistencies between the routing and forwarding tables.

Upgradability

Because downtime must be avoided and minimized, next-generation routers must be designed with mechanisms to support planned maintenance tasks such as adding and replacing hardware, installing new features or services, and applying patches or upgrades to software, without affecting the routing system, customers, peers, or traffic.

The Cisco ASR 9000 Series offers exceptional upgradability for rapid response to faults or new service demands, extending platform availability and longevity. As with process independence and restart, Cisco ASR 9000 upgradability is enabled by its distributed and modular architecture, and the following features:

- **OIR:** In addition to supporting fault handling, when hardware needs to be upgraded to add scale, features, or performance, the Cisco ASR 9000 supports OIR for system components such as RSPs and line cards, while the system is in service and performing at full capacity.
- **Programmable network processor:** To support high service velocity, system longevity for capital investments, lower operational costs, and the lowest possible MTTR, Cisco ASR 9000 Linecards support software feature upgrades through the programmable network processor.
- **Simplified software upgrades:** Cisco IOS XR Software release modularity makes it easy to perform the installation of a software upgrade. Most Cisco IOS XR Software fixes are non-service affecting, allowing customers to update a specific process or group of processes without affecting service. Operators may target particular system components for upgrades based on software packages or composites that group selected features. Cisco preconfigures and tests these packages and composites to help ensure system compatibility.
- **Software maintenance upgrades:** To simplify point fixes at component-level granularity, Cisco IOS XR Software uses software maintenance upgrades (SMUs) that can cross package boundaries, depending on what needs to be updated. Because SMUs are typically a short-term fix, permanent fixes roll into maintenance releases.
- **Security and integrity:** To support system security and integrity, Cisco IOS XR Software authenticates packages being installed and verifies version compatibility between the new packages and those in operation. If these two checks pass, the software restarts only those processes that a package advertises as changed, hence decreasing MTTR and improving system availability.

Continuous Forwarding

An important aspect of high availability is maintenance of traffic forwarding, even in the case of control-plane switchovers. Cisco IOS XR Software has several built-in features that can provide continuous forwarding, including RSP stateful switchover (SSO), Nonstop Forwarding (NSF), Graceful Restart, and NSR.

- **RSP SSO:** The Cisco ASR 9000 Series maintains state information on a per-protocol basis to support stateful switchovers between the RSP modules. Critical protocols protected in this way include Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), Border Gateway Protocol (BGP), and Label Distribution Protocol (LDP).
- **NSF:** Cisco IOS XR Software supports forwarding without traffic loss during a brief outage of the control plane through signaling and routing protocol implementations for Graceful Restart extensions as standardized by the IETF. In addition to standards compliance, this implementation has been compatibility tested with Cisco IOS Software and third-party operating systems.
- **Graceful Restart:** This control-plane mechanism ensures high availability by allowing detection and recovery from failure conditions while preserving NSF services. Graceful Restart is a way to recover from signaling and control-plane failures without affecting the forwarding plane. Cisco IOS XR Software uses this feature and a combination of check pointing, mirroring, RSP redundancy, and other system resiliency features to recover prior to timeout and avoid service downtime as a result of network reconvergence.
- **NSR:** This feature allows for the forwarding of data packets to continue along known routes while the routing protocol information is being refreshed following a processor switchover. NSR maintains protocol sessions and state information across SSO functions for services such as Multiprotocol Label Switching (MPLS) VPN. TCP connections and the routing protocol sessions are migrated from the active RSP to the standby RSP after the RSP failover without letting the peers know about the failover. The sessions terminate locally on the failed RSP, and the protocols running on the standby RSP reestablish the sessions after the standby RSP goes active, without the peer detecting the change. You can also use NSR with Graceful Restart to protect the routing control plane during switchovers.

The Cisco IOS XR Operating System provides system resiliency through a comprehensive set of high-availability features including modularity, process restart, fault handling, continuous forwarding, and upgradability. These intelligent software features, combined with hardware redundancy, enable the Cisco ASR 9000 to deliver continuous systems operations in the Carrier Ethernet transport network. Building on top of continuous system operations, the next section covers the aspects of network resiliency that help to integrate multiple nodes into one high-availability network.

Carrier Ethernet Network Resiliency Overview

Having covered the importance of continuous system operation for an individual node, now we consider the network-resiliency aspects that are supported between nodes in the network. Network resiliency includes recovery from transient control-plane outages in the network, rapid recovery from catastrophic failures, and ways to prioritize protection and recovery for the most important network traffic.

The Cisco ASR 9000 is positioned within the IP NGN Carrier Ethernet design to provide both aggregation and distribution provider-edge router capabilities. The IP NGN Carrier Ethernet design provides converged transport for residential, consumer, business, wholesale, and mobile services. A critical element of this design extends the end-to-end network to include many different types of access network technologies such as DSL access concentrator (DSLAM), Ethernet, cable, PONs, and mobile transport.

The Cisco ASR 9000 Series supports the industry-leading Cisco IOS XR Software, which offers many network resiliency features for:

- IP routing
- MPLS Traffic Engineering-Fast Reroute (MPLS TE-FRR)
- Multicast fast convergence
- Layer 2 VPNs

These resiliency features are discussed in the following sections.

IP Routing

Cisco IOS XR Software provides carrier-class routing capabilities that can now be extended to the Carrier Ethernet transport network. A full suite of routing protocols is supported, including OSPF, IS-IS, BGP, Routing Information Protocol Version 2 (RIPv2), and static routing. In order to maximize network uptime, numerous mechanisms on the Cisco ASR 9000 Series are used to quickly detect a failure and reconverge network traffic around failures.

- **Fast link-failure detection:** Cisco ASR 9000 Linecards support interrupt-based loss-of-signal detection, which can detect link- and port-level hardware failure in a few milliseconds. Such failures are signaled to the RSP, which can then trigger Interior Gateway Protocol (IGP) and MPLS reconvergence.
- **Distributed Bidirectional Forwarding Detection (BFD):** BFD can be used to quickly detect forwarding-path failures and trigger the routing protocol to provide fast convergence. It can be used with IS-IS, OSPF, MPLS TE-FRR, and Protocol Independent Multicast (PIM). The Cisco ASR 9000 Series implements BFD in a distributed fashion, where the line cards are equipped with a powerful local CPU and intelligent Cisco IOS XR Software system, enabling the support of thousands of BFD sessions per line card with a configurable hello timer as low as 15 msec.

The Cisco ASR 9000 Series inherently supports many advanced IGP routing fast-convergence features in Cisco IOS XR Software, including shortest-path-tree (SPT) optimizations to ensure packets are taking the most direct path though the network. Listed below are a few examples of Cisco IOS XR innovations in the area of fast convergence.

- **Prefix prioritization:** This feature provides a way to prioritize which prefixes converge first, based on the network administrator's guidelines. A good example would be giving a high priority to the IPTV source prefix of a video server application. Then during a change in the routing topology (for example, due to a link failure), the IPTV source prefix, which has a high priority, will be reconverged first to reduce down time for video services.
- **IP FRR:** This Cisco IOS XR Software innovation provides subsecond IP fast convergence for both IS-IS and OSPF routing protocols in a properly designed network topology. By taking advantage of these protocols, the Cisco ASR 9000 can extend superior routing

performance and fast convergence into Carrier Ethernet transport networks to increase network resiliency.

- **BGP fast convergence:** The Cisco ASR 9000 supports many advanced BGP fast-convergence features in Cisco IOS XR Software, including BGP next-hop tracking, BGP local convergence upon provider edge-customer edge link failure, and BGP prefix-independent convergence (PIC) for the core and edge. For example, the BGP PIC feature provides fast convergence in a scalable way. The Internet BGP routing table has hundreds of thousands of routes, and many BGP routes share the same provider-edge next hop. The Cisco ASR 9000 Series implements the forwarding table hierarchically so that during network reconvergence it does not need to update the entire BGP prefix in the forwarding table. Only the forwarding entry for the common BGP next hop is updated, resulting in a faster convergence time that is independent of the number of BGP prefixes. This feature is just one of the many Cisco IOS XR Software routing features that can help to maximize network availability.

MPLS TE-FRR

The Cisco ASR 9000 Series supports MPLS FRR options using MPLS Traffic Engineering (TE) backup tunnels to quickly reroute traffic around failures. MPLS TE-FRR addresses MPLS local link, path, and node failure protection by prebuilding a backup traffic-engineering tunnel that can be used in the case of a failure. When a primary traffic-engineering tunnel failure is detected, it can switch over to the backup traffic-engineering tunnel instantly. With the help of hardware-based loss-of-signaling detection and a preprogramming backup forwarding table, the Cisco ASR 9000 can switch over to the backup traffic-engineering tunnel in less than 50 msec. The Cisco ASR 9000 implements TE-FRR in such way that the convergence time is independent of the number of prefixes and the number of traffic-engineering tunnels. The MPLS TE-FRR features allow the Cisco ASR 9000 to provide Layer 3 MPLS network fast convergence in a simple and scalable way.

Multicast Fast Convergence

The Cisco ASR 9000 Series is optimized to provide subsecond multicast video delivery using PIM integration with routing-protocol convergence and prioritized multicast source prefix during the IGP convergence. In addition, the Cisco ASR 9000 supports new Cisco IOS XR Software innovations such as Multicast-only FRR (MoFRR) to improve multicast network convergence times even more.

The basic idea of MoFRR is to send a secondary join to a different upstream interface. The network then receives two copies of the multicast video stream over two separate and redundant paths through the network. When a primary path fails, it can switch over to the backup path instantly without issuing a new PIM join. This Cisco IOS XR Software solution is an extremely simple way for the Cisco ASR 9000 to take advantage of the native IP network in order to improve network convergence for multicast traffic.

Layer 2 VPN

As a Carrier Ethernet router, the Cisco ASR 9000 provides a comprehensive set of Layer 2 VPN (L2VPN) services. With the industry-leading IP routing and MPLS fast convergence features mentioned previously, the L2VPN pseudowires can be built on top of the resilient MPLS TE-FRR foundation in order to offer less than 50-msec convergence for the L2VPN data-path traffic. Redundancy mechanisms for both L2VPN pseudowire technologies and native bridging are

supported. Following is a summary of the specific redundancy protocols that are designed to protect pseudowires at Layer 2:

- **Pseudowire redundancy:** Pseudowire redundancy creates both primary and backup pseudowires that are connected to different remote nodes in the network. When the primary pseudowire goes down, it can quickly switch over to the backup pseudowire, ensuring access to the network.
- **Hierarchical Virtual Private LAN Service (H-VPLS) pseudowire redundancy with VPLS MAC withdrawal:** When an access pseudowire is used to connect into the VPLS network -- a technology known as Hierarchical VPLS (H-VPLS) -- pseudowire redundancy can be extended to protect the access pseudowire. Combined with VPLS MAC withdrawal technology, pseudowire redundancy in the H-VPLS scenario can be used to avoid a possible packet-oriented black hole.
- **Multisegment pseudowire redundancy:** When a L2VPN pseudowire crosses different administrative domains, a multisegment pseudowire is typically used to stitch multiple segments of pseudowires. Pseudowire redundancy technology can be applied to multisegment pseudowire scenarios as well.

To support the protection of native bridging interfaces, the Cisco ASR 9000 Series supports the following protocols:

- **IEEE Multiple Spanning Tree (MST) protocol:** To support native IEEE Layer 2 bridging environments, the Cisco ASR 9000 supports the standard IEEE 802.1s MST protocol to protect native bridging traffic.
- **MST Access Gateway:** In many scenarios where native Layer 2 access and Layer 2 VPN technologies are combined to provide Layer 2 service for the end user, traditional Layer 2-based redundancy protocols such as MST do not provide sufficient protection to avoid Layer 2 forwarding loops. In these cases, a mechanism is required to connect Layer 3 MPLS and Layer 2 access for both the control and data planes. To solve this problem, the Cisco ASR 9000 MST access gateway solution was developed to provide a unique solution for aggregating Layer 2 access networks regardless of the access network topology and protocols used.

By taking advantage of the industry-leading IP routing, MPLS TE-FRR, multicast, and L2VPN fast-convergence capabilities of Cisco IOS XR Software, the Cisco ASR 9000 provides many forms of network resiliency that you can use to maximize overall network and service availability.

Summary

As a market leader in networking solutions, Cisco takes advantage of years of experience in developing network high-availability solutions. At the system level, the Cisco ASR 9000 provides a distributed hardware architecture with redundant RSPs, switch fabric, line cards, power supplies, and fan trays. Adding Cisco IOS XR Software support for both continuous system availability and enhanced network resiliency enables the Cisco ASR 9000 Series to offer a resilient, high-availability solution for Carrier Ethernet transport networks. With this solution service providers can achieve continuous network operations for consumer high-speed access and IPTV, business VPN and wholesale services, as well as mobile backhaul transport services.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-501797-00 10/08