



Networking Overview

Borderless Networks Leveraging State-Of-The-Art Routing and Switching Technologies

OVERVIEW

KeyInfo's team of knowledgeable, experienced engineers and architects focuses on borderless networks leveraging state-of-the-art routing and switching technologies. These technologies include: converged infrastructures, high availability, resilience, flexibility, mobility, cyber security, wireless solutions and more. KeyInfo™ networking solutions include a strong investment in Cisco Application Centric Infrastructure (ACI) powered by an integrated architecture that uses a common policy-based operating model across ACI-ready network and security elements.

ABOUT KEYINFO



Key Information Systems, Inc. is a leading regional systems integrator with world-class compute, storage and networking solutions, and professional services for advanced software-defined data centers.

ENTERPRISE SOLUTIONS

CONVERGED NETWORKING

Converging network components reduces cabling complexity and along with components of software-defined networking mitigates potential errors due to cable mismanagement or physical media failures. In addition, capital expenditures are reduced by eliminating the need for multiple/different types of adapters. Reduced operational expenses are achievable, as fewer physical adapters contribute to lower overall power consumption.

SERVICE PROVIDER NETWORKING

DATA CENTER SWITCHING

Network architectures are undergoing a significant evolution. The traditional data center "Core-Distribution-Access" layers are flattening into more robust and fault-tolerant Spine and Leaf architectures. KeyInfo has a long and successful record of providing highly-resilient and adaptable Service Provider Networking. Our latest upgrade to the Cisco Nexus 9000-Series Application-Centric Infrastructure and Spine and Leaf architecture connected via high-bandwidth 40Gb links ensures that the superlative levels of service enjoyed by our customers will not only sustain but improve. KeyInfo's network engineering staff can provide networking solutions to your organization as a service, or can implement them for your organization in either an on-premises or hybrid model via our experienced Professional Services Group.

ADVANCED CARRIER ROUTING

As Virtualization moves more significantly into the network the associated technologies must keep pace. The Aggregation Service Routing (ASR) platform implements state-of-the-art route processors with integrated software-enabled services. This combination increases both hardware density and service agility resulting in lower overall space/power/cooling costs and reduced provisioning times. Aggregation Services Routers are capable of performing BGP, MPLS, VPN, OTV, IPS, and a number of other functions on the same hardware platform, leaving behind the legacy 1:1 service-to-hardware ratio.

BGP/FCP

Traditional BGP routing, while still the standard for Service Provider /Internet routing does not take into account the validity of the routing information received from upstream routers. To address this issue and ensure our client's traffic is following the most efficient and expeditious path to realize the highest performance,

[BGP/FCP CONTINUED >](#)

BGP/FCP (CONT...)

KeyInfo implements the InterNap Flow Control Platform (FCP). FCP consumes data from a SPAN port and performs network-level analysis across multiple hosts throughout the world via our providers. Based on the analysis of the results FCP will tune routes or create more specific routing entries to ensure customer traffic is always traversing the most reliable, highest-speed links.

SOFTWARE DEFINED NETWORKING (SDN)

ENHANCED AGILITY

Software-Defined Networking (SDN) enables rapid application deployment with specific network requirements and easily duplicates those settings to spin up network contexts for new applications.

REDUCED COSTS

SDN helps your enterprise make better use of equipment already on hand, providing a new software control layer on top of existing hardware. Your company becomes less dependent on one vendor's hardware, allowing optimization of commoditized hardware. Shifting the focus to software means improved network management efficiency. Together, these factors result in lower overall operating costs.

AUTOMATION AND CLOUD ENABLEMENT

Fluid automation of datacenter traffic flow throughout the network is a key advantage of Software-Defined Networks. An SDN solution enables you to help span your network within your current private cloud, and offers the option of expansion into one of many hybrid cloud offerings. Additionally, automation reduces the potential for costly outages due to human error.

NEXT GENERATION SECURITY

FIREWALL TECHNOLOGY

Network security must meet the demands of today's 24/7 mobile workforce. "Always on" requirements call for constant uptime and security. Contemporary firewalls can be hardware or software-based, extend protection from the corporate network down to end-users' devices, and are both flexible and granular. Rather than simply allowing or denying network access, new firewall technologies leverage the intelligence and capability to control access based on a specific application, operation requested, or originating location. The advanced firewall technologies KeyInfo implements protect assets anywhere (at the office, on the road), anytime, and on any platform (desktop, laptop, tablet, smartphone).

BRING YOUR OWN DEVICE (BYOD)

A well-implemented BYOD (laptops, tablets, smartphones) infrastructure can significantly reduce your business' capital expenditures. When combined with complementary technologies, you'll be able to extend the time between device replacement and upgrades. Challenges to acceptable use of personal devices and protecting your organization's intellectual property can be surmounted by instituting clearly defined and enforced acceptable-use policies. Available security technologies include mobile device management software, industry-standard X.509 digital certificates and on-demand virtual private networks.

DETECTION AND PREVENTION

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) protect your network by working in concert to quickly identify malicious activity within the computing environment and executing appropriate countermeasure action. Such efforts can be simple, such as disabling a rogue or troublesome network port. For more malicious attacks, IDS/IPS will isolate and log off offending network traffic to help identify and potentially apprehend/prosecute an attacker. A strategically placed and properly configured IDS/IPS system can save an organization substantial time and money associated with remediation efforts, including fines associated with violation of industry-standard regulations and protocols (e.g. HIPAA, SOX, SEC, PCI/DSS, GxP).