Cisco 4000 Series Integrated Services Routers: Architecture for Branch-Office Agility

The Cisco® 4000 Series Integrated Services Routers (ISRs) are designed for distributed organizations with multiple branch offices and remote sites. Today's branch offices offer full services through cloud, mobile, and multimedia applications, and require increased direct communication with both private data centers and public clouds across VPNs and the Internet. They also need a low total cost of ownership (TCO) for their networking hardware.

The Cisco 4000 Series ISRs extend the capabilities of previous-generation Cisco branch-office routers by offering increased bandwidth with fewer and physically smaller boxes, WAN traffic management to deal with new applications and use patterns, performance-on-demand capability, and consolidation of servers.

Challenges of the Branch Office

In the past, branch offices and remote sites provided static connectivity to local or data center–hosted applications. Because branch offices today serve up to 80 percent of employees, organizations are now facing the task of providing full-service branch offices with dynamic connectivity in order to accommodate a mobile workforce as well as the increased use of cloud-based applications. Businesses today are innovating with a new class of immersive applications, introducing high-definition (HD) video, location services, and other rich media services to promote employee productivity and customer loyalty.

However, network operating resources have not increased in proportion to actual requirements, resulting in branch-heavy businesses finding themselves having to handle an increasingly complex network with a relatively small number of IT staff. Add to that limited rack space for additional, required appliances plus limited budgets for hardware, energy usage, and cooling. These limitations make it difficult to operate a branch network consisting of an ever-increasing plethora of services, plus a growing number of required network service appliances.

Mobile users, cloud services, and multimedia applications have increased the demands on networks, with both higher network loads and new traffic patterns. WAN optimization, deep packet inspection, and advanced traffic-management techniques are more or less required today to support the new traffic patterns and application-based network policies that come from the use of cloud-based services. In addition, for services such as public cloud-based applications and guest networks, branch offices are realizing significant cost savings by using local Internet breakouts rather than hair pinning traffic through the data center. As effective as this practice may be, it adds a whole new dimension to a business's security policy, since every branch will be exposed to the Internet. With that

Branch-Office Challenges

Offering full services:
- HD video
- Location services
- Cloud-based services
- Mobile users

Overcoming limiting factors:
- Rack space
- Budget
- IT staff

Supporting increasing network demand and new traffic patterns:
- WAN optimization and intelligent caching
- Deep packet inspection
- Traffic management
- Hosting virtual servers

many points to protect, the security posture must be of the intelligent self-learning type to protect against day-zero attacks without manual intervention by network operators. Given the nature of today's threats, the security policy must furthermore protect the business against threats from inside, in addition to the traditional attacks from outside that we're used to protecting against.

Introducing the New Integrated Services Router Architecture from Cisco

The Cisco 4000 Series ISRs build on 20 years of branch-office routers, adding services and throughput for the needs of modern branch offices and allowing businesses to:

- Quickly open new remote offices or easily add services
- Operate an entire branch office with a single platform
- Give IT departments more time for innovation by automating repetitive tasks and orchestrating security and application services
- Provide solid, automated, intelligent security against today's cyber threats at all points in the network

The new architecture addresses the problems that modern branch offices face without giving up any of the existing services of previous-generation Cisco branch-office routers. It also brings virtualization to networking so that IT can adopt services faster and repurpose resources as needs change. Virtualization furthermore delivers additional computing power for local application survivability, data backup, and local analytics processing.

The new architecture of the Cisco 4000 Series ISRs delivers up to 2 Gbps in a converged platform, making it 4 to 10 times faster, on average, than the previous-generation ISRs with typical branch services enabled. The WAN and application optimization services of the 4000 Series ISRs include Cisco Application Visibility and Control (AVC), allowing IT to assess capacity planning; and Cisco Performance Routing Version 3 (PfR v3), which automatically sends traffic across the best connection for current network conditions. Not only does this architecture allow a branch office to run the network with a single platform, it also allows the use of converged network, computing, and storage resources in the same platform. The virtualization technology available within the Cisco 4000 Series and through additional data center–class server modules offers new levels of converged capability.

The Cisco 4000 Series includes several important features that make it a perfect choice for today's branch offices:

- **Price for performance:** The 4000 Series allows branch offices to handle increased bandwidth using a single box without the need for additional optimization appliances, and it can be managed by a small IT staff. The 4000 Series is built from the ground up to run complex service combinations in concurrent Intelligent WAN (IWAN) services, including security, application optimization, AVC, and PfRv3 for intelligent path selection.
- **Performance on demand (pay as you grow):** Branch offices can upgrade to a higher throughput without having to install a new platform. Each model in the 4000 Series offers additional performance over the base level that can be activated remotely when needed, simply by turning on a license. For example, a branch office might implement a Cisco 4351 ISR with a baseline performance of 200 Mbps. A couple of years later, when the use of new applications and traffic patterns mandates higher bandwidth, the network operator can log in and turn on the high-performance license, increasing the throughput to 400 Mbps. The entire operation is done in minutes and at a fraction of the cost of buying a new router.
- **Services on demand:** A built-in generic X86 architecture allows for KVM-based virtual machines to run within the 4000 Series. Essential branch-office services, which the branch office might already be running

on discrete servers, can thus instead run natively on the router, thereby consolidating branch servers and appliances and reducing the branch's hardware footprint and power usage.

- **Unprecedented built-in security**: In addition to traditional security features such as zone-based firewall and encryption, the 4000 Series introduces a whole new range of highly intelligent built-in security offerings, specifically tailored to today's cyber threats. Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. It is an agent built into Cisco IOS® Software that protects against malicious DNS traffic originating from inside the branch office. It keeps malware or already compromised hosts from reaching command and control servers and initializing or extracting data and using the branch as exit point. Cisco Stealthwatch® Learning Network (SLN), an app installed in a 4000 Series service container, provides artificial intelligence-like security with full day-zero protection, in that it learns the branch's normal traffic pattern and then looks for anomalies. A specific traffic pattern preceding an attack will thus not need to be known in order to be acted upon.

- **Market-leading cyber resiliency:** All 4000 Series ISRs ship with market-leading built-in cyber resiliency to help protect the router itself from being compromised. Enhanced Secure Boot and OS Validation protect against malicious software at startup time. Hardware mechanisms prevent attackers from modifying the system in order to change functionality. Encrypted storage of credentials protects against physical tampering with the intent of stealing secrets.

- **Scalable services:** The Cisco 4000 Series ISRs support Cisco Unified Computing System™ (Cisco UCS®) E-Series blade servers, which are comparable to a full-size server. The UCS-E-Series server blades run autonomously from the host router system, in that they use only the system's power and chassis. A reset of either the router or the E-Series server will hence not affect the other. The host router and the E-Series server can furthermore be managed completely separately from each other, allowing network operations to let a different department manage the E-Series server without having to provide any access to the host router. This setup gives an IT department all the benefits of a separate data center–class server without the need to maintain another physical appliance. In addition, a separate server virtual-machine license is not required, and troubleshooting involves only one point of contact instead of multiple vendors, resulting in better uptime and reliability. As an added bonus, hardware support costs through Cisco Smart Net Total Care™ Service are bundled into the router support cost. Any Cisco UCS E-Series Servers hosted in an ISR are covered at no additional fee. This is beneficial because support fees can add up when dealing with potential hard-drive failures in a server.

Cisco 4000 Series: Technical Highlights and Comparison

The Cisco 4000 Series uses Cisco IOS XE Software, the same Linux-based OS found on the bigger ASR 1000 Series platforms. Cisco IOS XE retains the design and user interface of the Cisco IOS OS used by previous-generation Cisco routers, yet allows the use of multicore CPUs. This setup facilitates separation of the data and control planes and uses dedicated CPUs for services.

Because the services plane is separate from the data and control planes, the router can handle more and heavier services on a single platform, allowing an office to consolidate devices. Solutions such as Cisco Unified Border Element (CUBE), Cisco Unified Survivable Remote Site Telephony (SRST), or various routing services can be deployed more easily and efficiently on a single ISR. In addition, for many of the services, such as CUBE, the scalability is significantly greater without added costs per port. Performance also remains solid across most typical branch-office deployments, providing application-specific integrated circuit (ASIC)-like performance in a highly reliable platform.

X86-based embedded service containers offer dedicated virtualized computing resources that include CPU, disk storage, and memory for each service. An industry-standard hypervisor presents the underlying infrastructure to the application or service. This design offers better scaling and flexibility than a tightly coupled service. Deployment with zero footprint, security through fault isolation, and the flexibility to upgrade network services independently of the router software are other benefits.
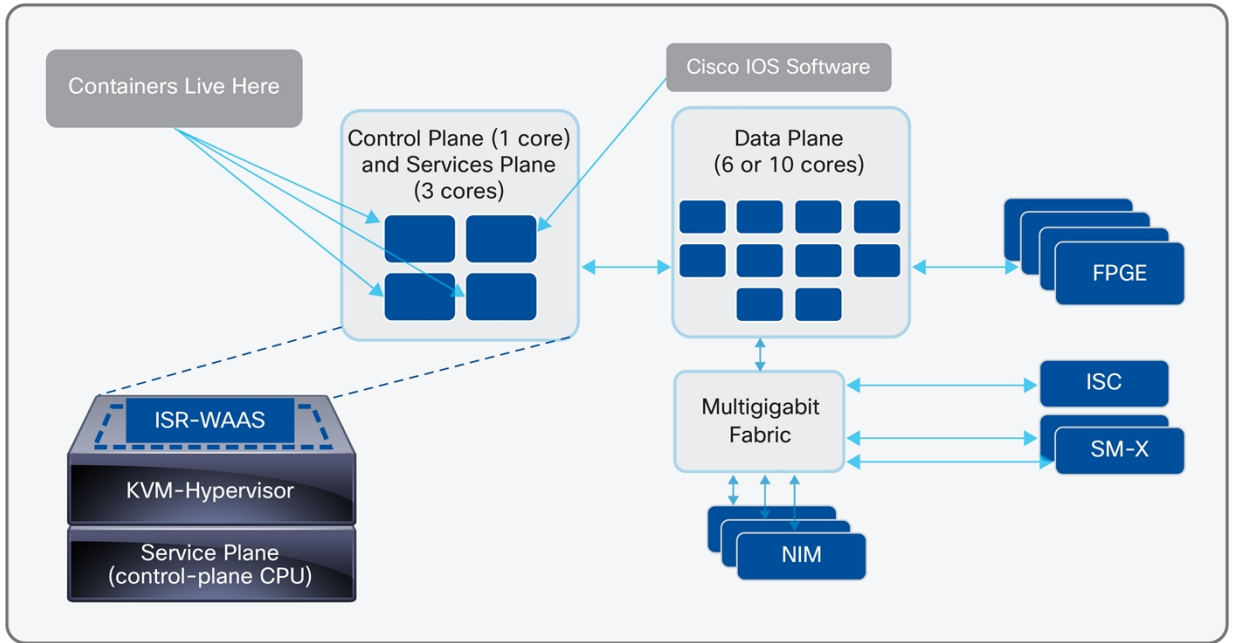
The Cisco 4400 and 4300 Series

The Cisco 4400 and 4300 Series ISRs have a very similar user interface design. The biggest difference to most users is that the 4400 Series supports dual power supplies, whereas the 4300 Series does not; this difference makes the Cisco 4451 and 4431 the preferred choices for organizations that cannot tolerate any downtime. The 4400 and 4300 Series are both designed with the same base architecture as their close relative, the ASR 1000 Series, using distributed control and data plane resources. The 4400 Series routers have a physical separation between control and data planes, using dedicated CPU sockets for each. The 4300 Series uses a single socket with multiple CPU cores, providing the distributed control plane, data plane, and service plane resources. This is, however, a difference most users will never be aware of.

Figure 1 shows the Cisco 4400 Series architecture. The abbreviations in the figure are as follows:

- **FPGE:** Front-panel Gigabit Ethernet. The Ethernet interfaces on the front panel.
- **ISC:** Internal services card. An internal module used for expanding the capabilities of the system. Commonly used for digital signal processor (DSP) modules.
- **SM-X:** Enhanced service module. A larger module type used mainly for Cisco UCS E-Series Server blades and high-density Ethernet switch modules. Some of the SM-X modules are compatible with the ISR G2 product line.
- **NIM:** Network interface module. Half the size of an SM-X, and generally used for WAN, voice, and low-density Ethernet interfaces. NIMs are not compatible with previous-generation ISRs.

Figure 1.   Cisco 4400 Series Architecture

Containers Live Here

Cisco IOS Software

Control Plane (1 core)
and Services Plane
(3 cores)

Data Plane
(6 or 10 cores)

FPGE

ISR-WAAS

KVM-Hypervisor

Service Plane
(control-plane CPU)

Multigigabit
Fabric

ISC

SM-X

NIM

The Cisco 4400 Series uses two multicore CPU complexes for the data plane (packet processing) and control and services planes. In Cisco IOS XE Software, classic Cisco IOS Software runs as a single daemon within a Linux OS, helping ensure control-plane protocol compatibility with all other Cisco routers. This setup is indicated as "Cisco IOS Software" in the figure. Additional system functions now run as additional, separate processes in the host OS environment. "ISR-WAAS" in the figure is an example of a typical virtualized service in a Cisco IOS XE Software service container. As with the previous ISR G2 routers, a multigigabit fabric supports direct intercommunication on Layer 2 between the Internal Services Card (ISC), Cisco SM-X EtherSwitch® modules, and network interface modules (NIMs) without having to be routed through the host router data plane.

Figure 2 shows the Cisco 4300 Series architecture, which is similar to the 4400 Series but does not include physical separation of the control and data planes. All functions are, however, exactly the same, with identical end-user experiences and feature support.

Figure 2.   Cisco 4300 Series Architecture
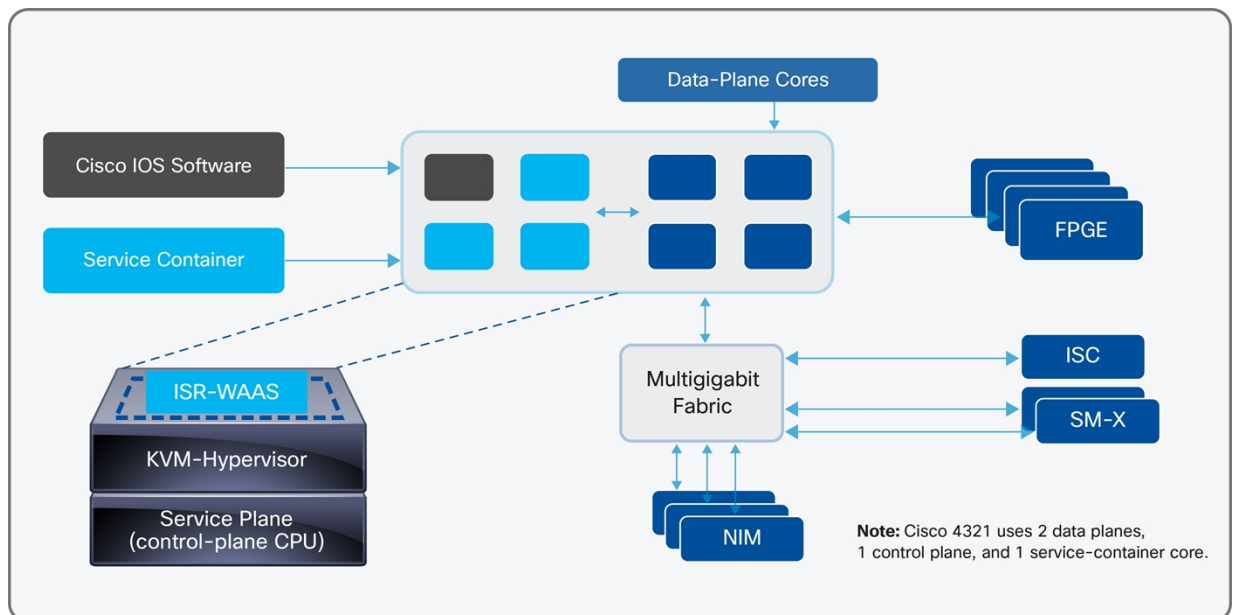
Individual Models in the Cisco 4000 Series

Figure 3 shows the Cisco 4451-X ISR.

Figure 3.   Cisco 4451-X ISR

The Cisco 4451-X is suggested for migration from the existing Cisco 3925E and 3945E routers. It offers 1-Gbps performance, upgradable to 2 Gbps, in a 2-rack-unit (2RU) form factor with three NIM slots and two enhanced service module (SM-X) slots. The 4451-X includes an option for built-in redundant power.

- 4-core processor (one control and three services processors)
- 10-core data plane
- Single or double-wide Cisco UCS E-Series support
- Up to 16-GB control and services memory

Figure 4 shows the Cisco 4431 ISR.

Figure 4.   Cisco 4431 ISR

The Cisco 4431 is suggested for migration from the existing Cisco 3925 and 3945 routers. It offers 500-Mbps performance, upgradable to 1 Gbps, in a 1RU form factor with three NIM slots. Like the 4451, the 4431 includes an option for built-in redundant power.

- 4-core processor (one control and three services processors)
- 6-core data plane
- Up to 16-GB control and services memory

Figure 5 shows the Cisco 4351 ISR.

Figure 5.   Cisco 4351 ISR

The Cisco 4351 is suggested for migration from existing Cisco 2951 routers. It offers 200-Mbps performance, upgradable to 400 Mbps, in a 2RU form factor with three NIM slots and two SM slots.

- 8-core CPU with four data-plane cores and four cores for control-plane and containerized services
- Single or double-wide Cisco UCS E-Series support, and up to 16-GB control and services memory

Figure 6 shows the Cisco 4331 ISR.

Figure 6.   Cisco 4331 ISR

The Cisco 4331 is suggested for migration from the existing Cisco 2911 and 2921 routers. It offers 100-Mbps performance, upgradable to 300 Mbps, in a 1RU form factor with two NIM slots and one SM slot.

- 8-core CPU with four data-plane cores and four cores for control-plane and containerized services
- Single-wide Cisco UCS E-Series support, and up to 16-GB control and services memory

Figure 7 shows the Cisco 4321 Integrated Services Router.

Figure 7.   Cisco 4321

The Cisco 4321 is suggested for migration from the existing Cisco 2901 and 1941 routers. It offers 50-Mbps performance, upgradable to 100 Mbps, in a 1RU desktop form factor with two NIM slots and no SM slots.

- 4-core CPU with two data-plane cores, one control-plane core, and one core dedicated for services
- Up to 8-GB control and services memory

Conclusion

The Cisco 4000 Series is designed to help branch and remote offices do more with less. These routers provide higher bandwidth for heavy service combinations and greatly enhanced WAN management. They also introduce embedded X86-based virtual machines together with options for data center–class servers, and an unprecedented flexibility in upgrading. All in all, the 4000 Series provides the branch office with less need for rack space; lower cost for maintenance, power, and cooling; faster rollout of new services; and less time spent by IT staff managing routers.

For more information, contact your local Cisco sales representative, or visit cisco.com/go/isr4000.