# Why Move to a Modern Network Operating System?

How operating system programmability, telemetry, and trust can help you meet new demands

## Modern networks need modern operating systems

Service providers have built their networks to serve the communication and connectivity demands of clients, but network innovation has been inhibited because of the operational complexities that result from multiple operating systems. Network infrastructure elements suffer from operating system bloat with unused features that consume vital memory resources and lack the ability to customize the operating system load. These limitations can lead to higher operating expenses for service providers as their network requirements expand. A modern operating system should integrate the different network infrastructure components to make management and operations easier.

© 2019 Cisco and/or its affiliates. All rights reserved.

## New demands require new software

Traditional network operating systems (NOSs) are designed to run in a native hardware environment. They have been designed so one-size-fits-all with a rigidity that complicates network device management and requires more time for updates and changes. At Cisco, we believe that modern NOS platforms need to be simple, powerful, and trustworthy. A modern OS should be able to support unique configurations, improve operational flexibility, and enhance security. Without a modern NOS, service provider engineers struggle to efficiently manage and operate a fast, reliable, and flexible network that can cope with unprecedented traffic growth and provide the services and performance that service provider customers demand.

As more devices are connected and more content is consumed, Internet traffic has seen a compounded annual growth rate of 30 percent over the last five years. It's anticipated that by 2022:

- IP traffic will increase to 396 exabytes per month.
- 1/3 of the Internet traffic will be in metropolitan service areas.
- More than 28 billion devices and connections will be online.
- Peak busy hour Internet traffic is growing faster than average Internet traffic because of increases in streaming video and online gaming.

In anticipation of this growth, Cisco designed the IOS XR7 (XR7) NOS to ease network operations. As a modern operating system, XR7 is designed to help engineers by:

- Providing a single, easy to maintain NOS paradigm across the network: edge, aggregation, and core
- Reducing operating expenses (OpEx) with simplified delivery and deployment of XR7 based on the features you need
- Using Linux-style workflows and support for standard Linux libraries to simplify provisioning and management of the device
- Improving operational efficiencies with management API integration to provide near real time, actionable telemetry data
- Allowing for automation to drive smoother implementations and remote configuration updates
- Validating trust within the network so service providers can work to operate a secure environment

## IOS XR 7 is built for simplicity

Service provider networks connect people and facilitate idea exchange and commerce. To keep up with the anticipated traffic growth, service providers have strained their budgets to increase capacity. In doing so, they have added increased operational complexity by adding more infrastructure components without rethinking their topology. More complex infrastructures and software increases OpEx because engineers require more time to sort out configurations, plan implementations, and work through software updates for the various NOS versions.

With IOS XR7, service providers can load and operate only the features needed for a specific use case, whether it involves access, edge, aggregation, or core. This software modularity allows engineers to better manage the costs and complexity of their network while benefiting from working within a single NOS environment. The NOS image can range from a full NOS version load on a multi-petabit core router to a scaled-back NOS version that runs on a multi-gigabit access router.

Loading configurations and software updates has also been simplified with XR7. Engineers can reduce complexity by building a Golden ISO image that includes the IOS XR7 Cisco router performance modules (RPMs), router configuration, third-party Linux applications, and secure zero-touch provisioning (ZTP) artifacts. By using a Golden ISO in combination with the RPM repositories,

© 2019 Cisco and/or its affiliates. All rights reserved.

engineers can build custom ISOs for specific applications and IOS XR files for a single deployment push. These custom Golden ISO packages are then stored so engineers can quickly reference them when they need to replicate the design for a new deployment.

Engineers can use the Golden ISO process to simplify programming design for their infrastructure. Then by using the ZTP supported by XR7, the team can reduce the costs related to sending technicians on site to complete installations. Once powered on and connected, the device uses dynamic host configuration protocol (DHCP) interactions to reach the bootstrap server and pull down its configuration through integrated APIs within IOS XR7. The iPXE feature supported in XR7 software allows an administrator to boot a device with TFTP, HTTP, or FTP from any location. These flexible access methods help improve the activation and update experience. Using the ZTP process, you can activate devices in minutes instead of hours, which returns time to the service technicians and engineering teams.

## Powerful telemetry and API integration

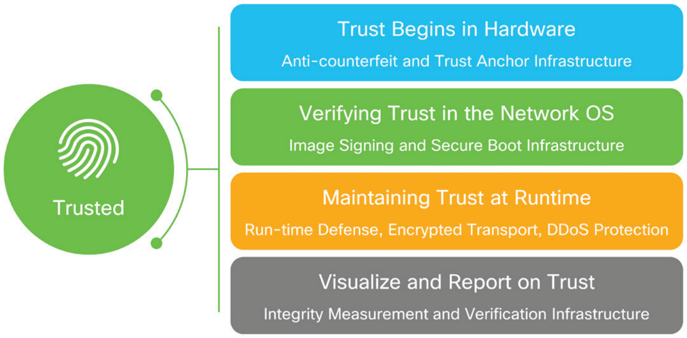
With the demands of a quickly digitizing world, service providers need complete visibility into their network. To support the scale and agility required of today's networks, visibility must be continual and automated. The IOS XR7 platform can help enhance network visibility by using telemetry data gathering and automated responses to network condition changes.

Model-driven telemetry improves network monitoring because data is streamed and captured continuously from devices with efficient, incremental updates. Within XR7, model-driven telemetry is fully configurable using YANG data models, so you can program the data to stream to a given location using specific encoding and transport protocols. The entire operational space is opened up for fine-grained control at scale. The increased visibility helps engineers focus on the most critical elements of the network so they can properly affect the client experience.

With XR7, you can build automation into your network that takes advantage of the reporting tools and structures that are already in place. By integrating open APIs that can access the software stack at all levels, XR7 provides the custom access you need to efficiently build and operate a network. For example, with the service layer APIs integrated into XR7, service providers can use their existing controller agent and telemetry data collection tools. This integration gives the operations team access to familiar tools and takes advantage of the licenses that you have already purchased for those tools, which can save both time and money. It also gives teams fine-grained control over the network with API access to the control plane. By combining these service layer APIs with the Open Forwarding Abstraction (OFA) API, engineers can build routing controls for specific applications based on critical service-level agreements and provide quick responses to changing network conditions.

## Trustworthy for your critical infrastructure

Attacks on the underlying hardware or firmware of a system are commonly used to establish persistence in compromised systems after a breach. Often, they're designed to continue to operate even after an operating system has been reinstalled. Two examples of these types of attacks are "Blue Pill" and "ThunderStrike," both of which compromised the running NOS kernel and infiltrated the firmware for ongoing compromise. Attackers use this persistence to gain control of the network and affect traffic flows, create mirrors, or otherwise compromise the validity of the network and data transmissions.


Trusted
Trust Begins in Hardware
Anti-counterfeit and Trust Anchor Infrastructure
Verifying Trust in the Network OS
Image Signing and Secure Boot Infrastructure
Maintaining Trust at Runtime
Run-time Defense, Encrypted Transport, DDoS Protection
Visualize and Report on Trust
Integrity Measurement and Verification Infrastructure

© 2019 Cisco and/or its affiliates. All rights reserved.

## The need for modern network operating systems

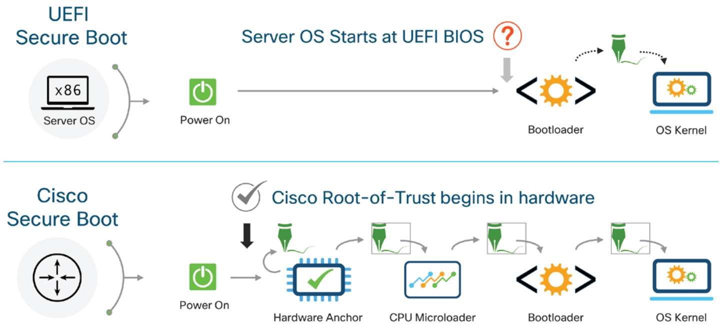
To adapt to shifting market demands, service providers are working to build networks that are flexible and dynamic. A modern network can't be built on an operating system that isn't flexible or one that forces restrictions on the operation of the network. A NOS for these dynamic networks should be simple to manage with powerful reporting. It should integrate data modeling and include robust security features. The Cisco IOS XR7 release is the newest version of one of the most widely deployed operating systems in the world. XR7 offers flexible deployments of feature sets with API integration to improve management access for changes to the device. XR7 also can help validate trust in the network infrastructure. With IOS XR7, service providers now have the tools they need so they can focus on developing new services knowing that their network has the flexibility to support the demands of their clients.

## Learn more

To learn more about Cisco IOS XR7, please visit the IOS XR page or the technical discussion page for IOS XR7. To learn more about Cisco Trust factors for more secure networks, visit the Built-in Trust page.

Any modern NOS needs to take service provider network security into account. As network elements are moved closer to users, engineers need to be able to validate that those infrastructure elements are authentic and uncompromised. Cisco builds in the capabilities to establish, verify, and measure trustworthiness in our products and in the critical network infrastructures we support. Our hardware and software have embedded security features and a secure device identity that builds trust across a network infrastructure. Building trustworthiness begins in the Cisco supply chain and continues to a secure boot process that readily validates the firmware and components when a unit is powered on.

Many Cisco service provider routers use signed images and a hardware-anchored secure boot process to prevent inauthentic or compromised code from booting. Secure boot is already a familiar term in the world of x86 servers. It's used to cryptographically verify the authenticity of the OS bootloader and the OS kernel as part of the boot process. Secure boot is commonly used to protect against boot-kit attacks in server OS like Linux or Microsoft Windows Server. In traditional x86 server systems, this secure boot process begins in UEFI BIOS and doesn't have a hardware root of trust or trust anchor.



Within IOS XR7, an extensive boot process is designed around a hardware trust anchor. This process begins before the CPU is allowed to boot and offers significant protections against compromises to the hardware or firmware. Anchoring the first code in the boot sequence in hardware establishes a chain of trust that begins when the hardware anchor implements self-measurement, followed by measurement and signature verification of the CPU microloader. It then verifies the signature of the bootloader and the NOS kernel. By adding a trust anchor to the secure boot process, users can then verify the reported values of the infrastructure pieces against the known good values from manufacturing to validate the device firmware as authentic.

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)