Next-Generation Network Operations
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What are we managing?</td>
<td>4</td>
</tr>
<tr>
<td>Lifecycle management</td>
<td>5</td>
</tr>
<tr>
<td>Release management</td>
<td>5</td>
</tr>
<tr>
<td>Provisioning</td>
<td>7</td>
</tr>
<tr>
<td>Network lifecycle management skills</td>
<td>8</td>
</tr>
<tr>
<td>Use case</td>
<td>8</td>
</tr>
<tr>
<td>Policy management</td>
<td>9</td>
</tr>
<tr>
<td>Policy change management</td>
<td>9</td>
</tr>
<tr>
<td>Policy compliance management</td>
<td>11</td>
</tr>
<tr>
<td>Policy management skills</td>
<td>12</td>
</tr>
<tr>
<td>Use case</td>
<td>12</td>
</tr>
<tr>
<td>Assurance management</td>
<td>13</td>
</tr>
<tr>
<td>Assurance management skills</td>
<td>15</td>
</tr>
<tr>
<td>Use case</td>
<td>16</td>
</tr>
<tr>
<td>Intent-based network operations roadmap</td>
<td>16</td>
</tr>
<tr>
<td>Next-generation operations maturity models</td>
<td>16</td>
</tr>
<tr>
<td>Example roadmap</td>
<td>17</td>
</tr>
<tr>
<td>Next steps</td>
<td>19</td>
</tr>
<tr>
<td>Appendix A: Acronym listing or full glossary</td>
<td>20</td>
</tr>
</tbody>
</table>
New Intent-Based Networking (IBN) capabilities promise to provide added security, service quality, and efficiency to infrastructure network services. Likewise, these capabilities will bring significant changes to how the infrastructure is operated and managed. Skills will change, processes must be updated, and new organizational structures may all be required. This paper first offers a new operational framework that better aligns with these new capabilities and then looks at potential requirements for next-generation network operations.

Intent-based networking is about simplifying provisioning, change, and fault resolution processes and verifying that the results match the original intent. This simplification requires the use of virtualization, domain fabrics, and network controllers that consistently manage scalability, prevent human error, and get the job done faster than with human intervention. New services can be set up, started, and stopped with a few key strokes while end-to-end policies will prioritize, re-reroute, and load share traffic based on business intent. We might think of this as the much-discussed “single pain of glass” concept where one interface can be used for automation, security, analytics, and assurance. The result is nothing less than a paradigm shift in the way we operate and manage our networks.

The ease with which we operate intent-based networks does require the deployment of more advanced, sophisticated technologies. Network domains may have their own overlay fabric to abstract technical details, while interdomain controllers and gateways provide translation for provisioning, policy, security, and assurance management. These new technical layers will then provide seamless end-to-end visibility and control. In addition, network functions that were previously embedded in network devices will be increasingly virtualized to allow for dynamic changes that can adjust network behavior in real-time based on the end-to-end policies or intended outcomes.

To prepare for this journey, Cisco recommends that organizations evaluate and adopt a few new processes key to intent-based networking. For now, we will call these processes lifecycle management, policy management, and assurance management. The framework below shows these three new process-focus areas in blue, and new or changing processes in green. Interactions with traditional IT Service Management (ITSM) process areas are also shown. The interactions with traditional ITSM processes and systems also may help identify potential integration capabilities with new intent-based networking controllers.

Figure 1. Next-generation operations framework
What are we managing?

The first goal of operations planning for intent-based networks is to start thinking about how the data center, WAN, cloud, campus, and wireless infrastructure will be managed and secured. Clearly, the industry is moving away from device management using CLI commands. Intent-based networking solutions replace conventional practices, using manual effort and element managers, with controller-led and policy-based abstractions that easily enable operators to express intent (desired outcome) and subsequently validate that the network is doing what they asked of it. As a result, network operators will not be managing individual boxes nearly as much as the controller and policy systems that drive business intent all the way from the user to the service. Network functions that were previously provided in network devices and appliances will also be virtualized themselves. The need for IT professionals will not diminish, but the transition period for skill development, process updates, and organization alignment will be a key for success.

The industry is in the early days of the intent-based networking journey. We currently need multiple systems for different environments and system capabilities. Many opportunities exist for orchestration and integration, and we have limited API capabilities in many cases. From past experience with technology shifts, we know that the change will be fast and early adopters will have a competitive edge. But organizations should also look at their tolerance for risk and available resources before deciding how aggressively they adopt next-generation capabilities.

One of the three process areas that warrant attention is lifecycle management. The change to controller-led orchestration, automation, and assurance systems requires much stricter adherence to hardware, software, and security standards. A user making a CLI change may find that the controller will over-ride the command in future updates because they are not defined as a policy. Results could also differ for different versions of device software. The network devices, controllers, security systems, and other management systems will be much more closely integrated, which means that making a change to one could impact the desired outcomes of the whole. In many cases these systems are owned and managed by groups that don’t currently talk or work with each other. In next-generation network operations, the organization will need to have well-defined lifecycle management practices, including release management and change management, especially with automation that focuses on the network or service as a system.

Another key area will be policy management. This is a key area because network controllers will rely on strict network standards for hardware, software, configurations, security, and even integrations. Policies must first be defined and then updated. Policies must also be configured within network controllers to ensure that defined standards and policies are continually provisioned across the entire network. Finally, policies must be verified using compliance-verification methods. To perform this work, IT professionals will have to work across teams and with business contacts to define how the network should react under normal and abnormal conditions. Because policies are the key configuration of all controllers and in some case assurance systems, Cisco sees policy management as a key area as it defines how the network will be secured while providing the services required by the business.

Assurance management is also evolving by starting to utilize machine learning and analytics capabilities. In the industry’s current state, there is simply too much information to consistently analyze and draw solid conclusions. Many organizations are satisfied if they can manage alarms and notifications for an unreachable device. Repair always seems to mean a smart human logging into multiple devices to find and resolve the issue. New systems will make sense of this data and provide northbound alarms, notification, and self-repair. Self-healing networks with integrations to provide incident-and-change tracking will be a reality.
This will require a network organization to rethink the tools, systems, and integrations used to collect data and utilize knowledge effectively. A new operations development role will be required to provide the focus needed to achieve this paradigm shift.

In addition, the roles of network engineer may shift away from troubleshooting to lifecycle management of the systems and controllers used in assurance management.

Cisco sees these three process areas as the keys to success in managing intent-based networks and achieving the desired outcomes. Many organizations have these processes but will need to apply more resources and skills in the future. The next sections will focus on the processes, expertise required, and organizational structure that is recommended for mid-sized to large enterprise organizations.

**Lifecycle management**

The two key processes that make up next-generation lifecycle management are controller release management and provisioning. Controller release management focuses on the processes and activities needed to ensure successful controller releases, updates, and integrations. Provisioning focuses on the processes and activities needed for more automated device and service provisioning. Lifecycle management maps into the ITIL service transition area, which includes release management and change control.

**Release management**

Release management has previously been relatively simple, because many organizations simply install and forget network components until their end-of-life. However, with intent-based networking, the industry will see rapid feature release cycles that can impact many components of a network domain and potentially a network service. Organizations may need to adopt scheduled release cycles for features adoption and interrupt driven release cycles for controller patches and security fixes. Almost all new controller capabilities will have integration and operations implications. To facilitate these ongoing release issues, a strong linkage is needed between a release engineering function and the network operations function. Many organizations may choose to implement a DevOps approach for rapidly adopting new functionality and ongoing upgrades. Other organizations may choose to implement a release cycle approach where fewer releases are deployed to network operations each year. A governance function should help define the approach based on costs and business value.

*Figure 2. Intent-based networking release management interactions*
Each of these groups has specific roles and responsibilities. In larger organizations, these may be separate teams while in smaller organizations there can be combined roles or out-tasking involved to fill skill gaps.

**Service design**
- Ensures an overall architecture and design roadmap that encompasses network and operations technologies, people, process, and tools across the lifecycle
- Aligns with business in terms of budget, direction, and capabilities

**IBN vendor**
- Maintains release cycles for intent-based network vendor capabilities
- Releases new features, functionality, hardware, software, and patches to customers
- Provides training, support, and release documentation

**Release engineering**
- Works with governance and IBN vendors to define release cycles and feature deployment capabilities within their enterprise organization
- Performs release activities such as proof-of-concept, feature and integration testing, and feature pilots
- Works with network operations to provide a release package that includes change detail and an operations plan containing process changes, and training requirements
- Addresses security requirements to ensure that security policies have been updated or met
- Participates in pilot deployment and operations handover until deployment and operations teams accept the new IBN capability

**Deployment**
- Works with release management to determine release requirements
- Performs site planning and creates installation plan
- Identifies and assigns site-specific configuration detail
- Creates deployment and/or migration plans
- Works with change management to perform release deployment
- Tests and hands over to operation teams
- Provides feedback to release management with any release issues

**Network operations**
- Aligns with release engineering on new feature capabilities and changes to ensure operational readiness
- Performs change management to incorporate changes in production
- Changes the operational model or processes, based on release requirements or recommendations
- Collects and reports metrics on operation effectiveness and efficiency

**Note:** An easy way to capture progress and success with intent-based networking is to count the user logins to the desired set of infrastructure devices. With intent-based networking, eventually this can be driven down to zero!
Governance

- Ensures that release management function is working effectively and meeting security and business requirements
- Prioritizes and approves IBN releases based on business needs
- Manages metrics or cost models to determine the business value of new capabilities
- May implement continuous service improvement with metrics to drive business requirements

Provisioning

Provisioning focuses on the organizational responsibilities, processes, and software integrations required for more automated provisioning of service adds, changes, and deletions or the provisioning of controller-owned named features and network functions. This is separated from release management because these changes are tested and performed day-to-day. In many cases provisioning can be performed as a standard change without change management approval. Initially provisioning will be some combination of automation and administrator effort but over time provisioning will be integrated with end-to-end orchestration systems providing true one touch provisioning from service ordering to service delivery. A wide variety of operations systems may be integrated with orchestration that can include policy, assurance, and configuration allocation systems.

Figure 3. Intent-based networking provisioning processes

Policy administration

- Couples with policy management to define provisioning configuration and standards policies in the context of controller capabilities
- Ensures that those policies are reflected (and configured) in network controller systems. Policies may include software, patching levels, configurations for security, Quality of Service (QoS) configuration, and other configuration standards.
- Ensures that any manually provisioned policies are included in the provisioning process

Deployment

- Works with policy administration to ensure that provisioning standards are configured correctly
- Performs device provisioning, which includes manual and automated tasks
- Manages the entire provisioning process, including manual steps such as installation requirements and communications with network operations
- Communicates with network operations to meet change management and device turn-up requirements
Network operations

- Approves change management records for new provisioning
- Ensures changes are properly reflected in operational systems such as inventory, asset management systems, and configuration management systems
- Accepts new devices under appropriate operation-support levels

Network lifecycle management skills
New skills will be needed in next-generation network operations lifecycle management. Organizations may choose a combination of hiring, training, and/or out-tasking in the following skill areas:

Business skills - The ability to ascertain and translate business requirements into network infrastructure, software, and other technology requirements

Network strategy and architecture - The ability to build and plan network updates that will meet future business needs and justify the plan to management

Security - Defining security architectures and deploying security technologies

Automation skills – The ability to use advanced automation tools, scripts, and provisioning templates to provision and maintain an advanced network

IT process re-engineering and integration - Have a full understanding of IT processes and workflows with the ability to change and integrate network operations to improve efficiencies and streamline alignment to changing business needs

Technologies and operations - Command of technology architectures and protocols across domains, including data center, WAN, cloud, LAN, wireless, DMZ, etc.

Network DevOps and programming - The ability to bring development and operations together to enable new visual and natural-language tools that will focus increasingly on meeting network operation needs and streamlining IT processes. Agile methods may also be used to reiteratively and rapidly deploy smaller releases

Network provider management - Command of technical and business relationships associated with third parties such as network vendors, service providers, managed service providers, and cloud providers

Cloud networking expertise - Have a full understanding of private and multicloud technology as it relates to planning, orchestrating, and maintaining the multicloud network and collaborating with cloud architects

Use case
An organization will typically start with automated provisioning to decrease engineer time with installation and turn-up of new devices. Many organizations currently need an onsite expert to set up, configure, turn up, test, and turnover a single device. This may require more than a day if travel is needed. With automation, an out-tasked service or office worker could install the device and ensure that it is discovered by controller software for further provisioning.

An initial provisioning system could increase service delivery speed, improve service quality, and lower cost. Saved resources could be applied to help manage policies and compliance. The result can be improvements in service quality and further cost reduction. Additional cost could be realized with additional integrations to the service catalog, IP Address Management (IPAM) systems, inventory systems, change control, and others.
Once the organization has mastered device provisioning, they may then add orchestration capabilities to automate service delivery and management all the way from service catalog ordering to service assurance enablement.

The organization might start by applying the savings to a hardware refresh involving hundreds of devices. Multiplying the number of devices by the anticipated time saving could yield the resource hours needed for more advanced skill training and resource allocation for lifecycle and policy management. IT management should ensure that it is driving the business requirements with automation capabilities. Network teams should make sure they understand the tool and integration requirements and have their roles and responsibilities assigned.

A more advanced provision capability would be to allow controller-led secure provisioning of services to and from the enterprise edge or between a public and private cloud. With virtualization and interdomain secure controller capabilities, service set up, start, and tear-down can be much more dynamic where manual methods may have been all but impossible.

**Note:** A common challenge with automation is organizational change management. Ensure that a governance body is in place to drive the organizational and skill changes. Organizations might reward desired behavior or drive metrics that demonstrate the desired outcome.

**Policy management**

Perhaps the most significant change with intent-based networking involves managing policies. With a network controller, policies will need to be well-defined with centralized implementation, change, and compliance enforcement. Organizations with many administrators in different groups making changes to the network will have to change their approach to ensure that all change is first defined as a policy, then appropriately configured in the controller, and lastly deployed to the network.

Organizations anticipate challenges, because this can be a culture and process change. Some organizations have well-defined policies but still struggle to maintain them due to many hands making changes. Others lack oversight from the business or governance team on policies resulting in little or no formalized governance or compliance. Other organizations have little or no policies resulting in significant solution deviations. Two significant processes, policy change management and compliance management, are needed in policy management to address these challenges. These processes map into the ITIL Service Configuration Management and Information Security Management practices of ITILv4 but are not explicitly defined.

**Policy change management**

The policy change management process is important because it helps maintain infrastructure consistency while ensuring that the policy changes go through an approval process with consideration from multiple groups. In the past, infrastructure consistency was more problematic due to noncentralized control and multiple groups changing the environment. But controllers have to rely on consistent hardware, software, and configuration standards to be effective. Just think of applying a policy to 100 different devices with different software versions and configurations. Would you be comfortable hitting the go button for a policy update and achieving success? What about 1000 devices? A significant value of intent-based networking provides the ability to push policies with an “easy” button, but it requires an effort to centralize control and maintain a consistent environment via a policy management capability.
An intent-based networking policy may be applied to a number of different areas and can include specific configurations, hardware, and software. Policies may also be under the authority of different groups. For instance, security policies may be owned and managed by an InfoSec team while device hardware and software will most likely be owned by the network infrastructure team. Different organizations will set policies based on size, organization structure, and policy area. This could be a centralized, federated or distributed approach. The key is to understand all the policies that need standardization and governance and then ensure policy management is in place with a rigorous policy change management approval process. The policy change management process may also consider checks and balances in provisioning to ensure that policies are deployed correctly. Here are a few examples of policies needed for intent-based networking:

- Device access policy management
- User access policy management
- Macro-segmentation and micro-segmentation policy management
- Device hardware and software standards and lifecycle policy management
- Quality of Service (QoS) policy management
- Network protocol and configuration policy management

The best model for policy administration involves separation of duties between policy definition, change management, and infrastructure operations so there is a clear path of accountability and verification for configured policies. A governance model would also be needed to ensure that the checks and balances are in place, and that the policy management functions are improving over time.

Figure 4. Intent-based networking policy change management

Governance

- Links to the business to define business requirements and priorities
- Ensure infrastructure policy is meeting service objectives
- Ensure separation of duties in policy management to ensure quality

Policy definition

- Roles and responsibilities for policy definition across infrastructure
- Defines detailed policies for areas that include hardware, software, protocol configuration, Quality of Service configuration, IP address management, and other areas

Policy administration

- Applies policies defined by policy definition group to the enterprise controller systems for provisioning and change policies
- Documents manual policies as needed
- Helps to ensure that policies are applied appropriately and ready for operational staff to efficiently utilize and/or deploy
Network operations

- Perform policy push based on change management requests from policy change management
- Report exceptions to policy administration

Policy compliance management

Policy compliance management brings in an additional function, which works to ensure that policies are being provisioned consistently and correctly. This function may be critical for automation and also to meet regulatory requirements, such as PCI or HIPPA, for example.

Figure 5. Intent-based networking policy compliance management

Governance

- Links to the business to define compliance and industry requirements
- Helps define compliance processes
- Defines policies for compliance audits

Policy definition

- Defines, manages, and changes infrastructure policies
- Translates InfoSec policies into configurable policies for infrastructure security
- Works with business and governance to define QoS policies for infrastructure
- Defines, manages, and changes current hardware, software, and configuration standards for infrastructure devices

Policy administration

- Defines policies that require compliance verification
- Defines methodology for compliance verifications

Compliance operations

- Performs independent compliance verification audits based on policy administration definitions
- Works with policy administration on discrepancies and issues to help prevent further deviations
- Identifies compliance deviations and reports them to network operations for remediation
Network operations

- Work with compliance operations to remediate any policy or compliance deviations
- Work with compliance operations to help automate remediation processing
- Assist with potential integrations with incident and change management

Policy management skills

New skills will be needed in next-generation network operations policy management. Organizations may choose a combination of hiring, training, and/or out-tasking in the following skill areas:

Business skills - The ability to ascertain and translate business requirements into network policy requirements.

Security - Understanding of security architecture and security measures including firewall rules, authentication/authorization methods, segmentation capabilities, threat models, monitoring systems, IoT concepts, etc.

Automation skills - Ability to use advanced automation tools, scripts, and provisioning templates to provision and verify policies throughout the network.

IT process re-engineering and integration - Have a full understanding of IT policy management processes and workflows with ability to change and integrate network operations to improve efficiencies and streamline alignment to changing business needs

Network DevOps and programming - The ability to bring development and operations together to enable new visual and natural-language tools that will focus increasingly on meeting network operations needs and streamlining IT processes. Agile methods may also be used to reiteratively and rapidly deploy smaller releases.

Multidomain integration - Ability to understand and implement network policy requirements aligned across multiple domains (including access, WAN, data center, cloud, and IoT)

Network provider management - Command of technical and business relationships associated with third parties, such as network vendors, service providers, managed service providers, and cloud providers

Use case

Many organizations have somewhat informal policies that are managed by different groups, including security groups, firewall groups, network operations, and others. In many cases, these rules are cut- and pasted from individual user files or some system of authority. Errors occur when the overall system initially works but some event changes the anticipated behavior or security of the network. In many cases, software versioning, patching, and ongoing configuration is done on a best-effort basis only. Organizations may have regular audits performed, but errors are frequently found.

As a controller is added to the network, it becomes more critical to have well-defined policies for configuration, software, and security that follow the intent of the business. A group that focuses on business and security alignment to define the policies helps because it can focus on the business intent and not technical day-to-day operations. Accountability is also then created between policy definition and policy administration, which configures the software and controller systems. Further accountability is added when a third group is responsible for pushing policies out to the network.
The added accountability and careful process helps to make sure that the network behavior is always following business intent. Driving the policy and standards also helps to ensure that the network is predictable and resilient, resulting in improved agility, less service impact, and improved user or business satisfaction.

**Note:** A common challenge with policy management is the initial standardization of the network before policy systems are put in place. If policy management controllers are put in place prior to complete standardization, then errors or failure can more easily occur. Organizations should start policy management in greenfield areas, new installations, or after a rigorous standardization effort is performed.

**Assurance management**

Assurance management is about maintaining network health through rapid fault identification, prevention, and resolution through six basic process areas. The requirements in each area can vary significantly from organization to organization but tend to be directly proportional to the size and complexity of a network. In other words, small networks tend to be easily managed with human hands and brains, but larger networks become nearly impossible to manage without tools, network data, and significant processes.

Intent-based networking assurance management improves and integrates these processes with analytics, API integrations, machine learning, correlation capabilities, advanced reporting, and enrichment. Analytics and/or enrichment is the ability to provide additional details and insights about a network fault that will facilitate rapid resolution or improved health. For larger networks the result will be improved service quality, rapid issue resolution, and operational efficiency.

The key to effectiveness may always be in the ability to integrate automation or assurance capabilities into several different assurance processes. The key is to first capture key knowledge about the network through existing assurance processes, new AI tools, or machine learning. As new information is captured, it can be flagged and cataloged for DevOps analysis to determine how the knowledge is consumed. This could mean forwarding the information to a security event and incident management system, to an incident, problem, or change management system, or to a knowledge base to support troubleshooting, or it could mean simply logging the information for root-cause analysis. The DevOps team can then code any necessary integration and potentially also “enrich” that information to make it easier for internal processes to use effectively. The following assurance process areas are potential consumers of assurance knowledge:

**Event detection and correlation** - The ability to identify and forward service-affecting events via notifications, alarms, and integrations. Intent-based networking promises intelligent detection and correlation of issues and can also enrich alarms with key troubleshooting steps. Networks have thousands of events recorded per day, so some correlation and/or filtering is needed to identify health issues. Event detection and correlation steps may be invoked when service impact has been identified by users rather than intelligent tools.

**Incident recording and workflow** - The ability to document, archive, and report network issues and faults in order to rapidly resolve network fault issues and report success metrics. Incident recording systems can be viewed as a workflow tool that assists operations in driving a network fault from detection to resolution. In many cases, the documented information is also helpful for chronic issue identification and root-cause reporting to the business.

**Troubleshooting** - The ability to identify the cause and resolution of a network fault. Troubleshooting starts after an issue has been detected and reported and relies on tools or network data to help identify the source of the problem in order to formulate a resolution. Actual resolutions are a portion of the incident management process, but troubleshooting may rely on various tools and automations to capture root-causes and offer potential fixes.
Root-cause analysis - The ability to identify and record why a problem occurred. Typically, this requires a controller playback function and/or the collection and archival of log, event, and incident information. Any system that collects data from the network, including the devices themselves, may be valuable for root-cause analysis. Tool integration can be set up to automatically collect and distill this information.

Network health - The ability to understand the health of a network through reporting of performance indicators relevant to the environment. When detection of health symptoms arises (for example, through measurement threshold breaches), those issues can then be resolved. Potential network health issues are recorded and managed through a problem management system (also called a known-error database) that also records and documents root-cause analyses, and chronic health issues identified in the Incident recording system.

Automated resolution - The new and growing capability of assurance controllers is the ability to identify a service impact and automatically resolve or work around the issue via assurance automation capabilities. In most cases, this will need to be tightly integrated with both incident management and change management tracking systems and processes. Any automated change should also go through an agreed upon change-approval process to prevent further service impact.

Depending on business requirements or complexity of the environment, the organization should consider a new working group that we are calling “operations development.” This group focuses on the development and integration of assurance capabilities and works with the network operations team to update processes and move new capabilities to production. The group would have a roadmap of integrations, tools, analytics, and other new capabilities based on metrics or perceived business value. This group would also be important to drive tool integrations in multi-vendor environments where a commercial off-the-shelf solution is not available.

Figure 6. Intent-based networking assurance management

Controller and tool vendors
- Maintains and publishes release cycles for vendor capabilities
- Releases new features, functionalities, hardware, software, and patches to customers
- Provides training, mentoring, and release content and knowledge as needed

Operations development
- Defines the operations tool, automation, and integration architecture and roadmap
- Works with controller and tool vendors to define feature deployment and integration capabilities within their enterprise organization
- Develops operational solutions using integration; the knowledge base; analytics tools; data capture, collection, and archiving; reporting; alarming; and scripting
- Performs release functions such as proof-of-concept, feature testing, and feature pilots
- Works with network operations to provide release package and operations plan
- Participates in pilot and operations handover until operations accept the new IBN capability
- Provides operation solution support to the network operations team
Network operations

- Aligns with operations development on new feature capabilities and changes to ensure operations readiness
- Performs change management function to incorporate operations process and tool changes into production
- Changes the operational model based on release requirements
- Collects and reports metrics on operations effectiveness and efficiency

Assurance management skills

New skills will be needed in next-generation assurance management. Organizations may choose a combination of hiring, training, and/or out-tasking of the following skill areas:

**Business skills** - The ability to ascertain and translate business requirements into network assurance requirements

**Automation skills** - The ability to use advanced automation tools, scripts, and provisioning templates to provision and verify policies throughout the network

**Network management architecture** - The overall architecture of network management can be quite complex with collectors, upstream and downstream integrations, correlation engines, notification systems, ITSM integrations, analytics engines, reporting tools, and others. Focus on the overall architecture is needed in order to best drive business intent and desired results

**Technologies and operations** - Command of technology architectures and protocols across domains including data center, WAN, cloud, LAN, wireless, DMZ, etc.

**IT process re-engineering and integration** - Have a full understanding of IT policy management processes and workflows with ability to change and integrate network operations to improve efficiencies and streamline alignment to changing business needs

**ITSM service operations** - A full understanding of ITIL processes, including service transition and service operations in order to effectively link assurance systems to ITSM capabilities

**Network DevOps and programming** - The ability to bring development and operations together to enable new visual and natural-language tools that will focus increasingly on meeting network operations needs and streamlining IT processes. Agile methods may also be used to reiteratively and rapidly deploy smaller releases

**Multidomain integration** - Ability to understand and implement network policy requirements aligned across multiple domains (access, WAN, data center, cloud, and IoT)

**Cloud networking expertise** - Have a full understanding of private and multicloud technology as it relates to planning, orchestrating, and maintaining the multicloud network and collaborating with cloud architects

**Network provider management** - Command of technical and business relationships associated with third parties, such as network vendors, service providers, managed service providers, and cloud providers
Use case

Many organizations lack operations development capabilities, and tools can often be an after-thought without well-defined roles and responsibilities for tool requirements. This is often due to a lack of available resources and/or time to focus on the tools. As a result, most organizations will not have the budget to rearchitect assurance platforms.

A good place to start is with network analytics and health tools that focus on reducing the troubleshooting effort or that prevent service impact by identifying potential issues. Organizations can implement these tools at limited expense and then utilize internal training and notification methods to act on information in a timely manner. The expectation is that incident numbers and resolution time are reduced. Driving metrics such as incident reduction, incident resolution time, and impacted user minutes with governance and business representatives can help demonstrate business impact and show where service quality, security, and costs can be reduced with further assurance development, integrations, and tools capabilities.

Note: A common challenge with assurance management is alignment with business requirements. Many organizations have very loose service-level definitions or requirements, which typically means that the business expects 100% availability at low cost. Measuring current service-level quality utilizing a service level manager can help show the business the service levels they are currently getting, and align what they are willing to spend with further improvements.

Intent-based network operations roadmap

An operations roadmap demonstrates how an organization may need to fully realize the benefits of intent-based networking. Most customers will have unique business requirements and/or operation environments that will necessitate a customized roadmap. A place to start is the evaluation of requirements and current-state operational capabilities to determine operational priorities, immediate, and potential dependencies.

Next-generation operations maturity models

Many organizations will be in the “responsive” category in the following areas. Intent-based networking requires the evolution of operational maturity in these three process areas. Organizations can evaluate maturity and business goals to determine priorities and evolution of their next-generation operations environment.

Table 1. Next-generation operations lifecycle management maturity

<table>
<thead>
<tr>
<th>Reactive</th>
<th>Responsive</th>
<th>Proactive</th>
<th>Predictive</th>
<th>Business-optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changes in network infrastructure are done manually based on reactions to business needs and conditions.</td>
<td>Respond to infrastructure lifecycle markers and security alerts. Has release and change processes to maintain initial level of standards and compliance across the infrastructure.</td>
<td>Proactively manage hardware, software, and configuration standards with well-defined tools, and release or change processes to maintain a consistent infrastructure environment.</td>
<td>Compliant infrastructure environment consistently provisioned with automation tools. Well-defined lifecycle change triggers and processes.</td>
<td>Orchestration and automation capabilities to make real-time lifecycle and infrastructure changes based on business intent.</td>
</tr>
</tbody>
</table>
### Table 2. Next-generation networking policy management maturity

<table>
<thead>
<tr>
<th></th>
<th>Reactive</th>
<th>Responsive</th>
<th>Proactive</th>
<th>Predictive</th>
<th>Business-optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reactive</strong></td>
<td>No formalized security, service, or application policies for infrastructure network. Existing policies implemented on best-effort basis or in response to events or issues.</td>
<td>Standard security policies in place and utilized across infrastructure. Limited Quality of Service policies for key business traffic or non-business uses.</td>
<td>Infrastructure teams proactive in understanding quality of service requirements for business services. Service profiling, policy definition, and policy administration consistent across infrastructure.</td>
<td>Organizations are in tune with changing business conditions using service monitoring tools or changing business requirement and can initiate policy changes using automation and provisioning toolsets in near real-time.</td>
<td>Intent-based systems or controllers responsive to changing business condition able to make policy changes based on time of day, key events, or other business circumstances.</td>
</tr>
</tbody>
</table>

### Table 3. Next-generation operations assurance maturity

<table>
<thead>
<tr>
<th></th>
<th>Reactive</th>
<th>Responsive</th>
<th>Proactive</th>
<th>Predictive</th>
<th>Business-optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reactive</strong></td>
<td>React to user-initiated notifications of service disruptions.</td>
<td>Respond to network alerts to identify and resolve a majority of service-impacting issues.</td>
<td>Almost all service impact is identified and resolved via alarms. Organization also monitors health, performance, and capacity and consistently lowers impact over time.</td>
<td>Remediate health and service-impacting issues before they happen with the user of analytics and automation technologies.</td>
<td>Health and performance are dynamically managed using business-intent systems, analytics, and automation capabilities. Service impact significantly reduced or eliminated.</td>
</tr>
</tbody>
</table>

### Example roadmap

An example roadmap starts with focus on release management and policy management to ensure that IBN capabilities are deployed with consideration for operations, security, and lifecycle impacts. Developing these processes helps to ensure a tighter coupling with deployment, security, and operations teams and provides additional consideration for tool, controller, and infrastructure integration.

**Figure 7.** An IBN operations roadmap example
Many organizations have a release management process that focuses on initial deployment success. With IBN release management the infrastructure teams need to be more focused on continuous releases, operational readiness, and integration. The following checklist might be used for release management to understand potential process changes needed for IBN networking:

- Roles and responsibilities for solution design, including High-Level Design (HLD) and Low-Level Design (LLD)
- Roles and responsibilities defined for ongoing feature development, verification, and deployment covering both security and network functionality
- Roles and responsibilities identified for operations integrations, turnover, operations process changes, and training
- Roles and responsibilities for controller lifecycle management including software upgrades, patches, and controller configuration changes
- Solution verification environment for testing, training, and operations turnover
- Release cycles defined for feature or solution upgrades

Policy management is the next phase of the roadmap where the organization defines roles and responsibilities for defining, implementing, and verifying several classes of policy that may be managed from the IBN controller. The following checklist might be used for policy management to understand potential process changes needed for IBN networking:

- Roles and responsibilities for security policy definition, implementation, and compliance (organizations often prefer to use a separation-of-duties method to help ensure that the configured policy is accurate and effective)
- Roles and responsibilities for Quality of Service policy definition, implementation, and verification
- Roles and responsibilities for configuration template management
- Roles and responsibilities for device hardware and software standards and compliance
- Roles and responsibilities for policy management processes
- Skills development for policy management focus areas
- Policy management process ownership and sponsorship with security and business leads

When an organization has taken time to make release and policy management changes for intent-based networking, the initial deployments will have more long-term success. However, a few additional steps that help ensure deployments will be a success are given below:

- Roles and responsibilities for developing and documenting deployment and/or migration steps
- Roles and responsibilities for verifying quality deployment or migration methods
- Roles and responsibilities for installation, configuration, and deployment
- Roles and responsibilities for creating any required “as-built” documentation
- Roles and responsibilities for infrastructure change management
- Roles and responsibilities for turnover to operations
- Roles and responsibilities for project management in phased deployments or migrations
- Training and expertise requirements for engineers and installers
Organizations should always work to fully utilize controller assurance and integration capabilities to maximize service quality and staff efficiency. The following steps can help to ensure that assurance capabilities are fully integrated into network operations:

- Roles and responsibilities for defining challenges and opportunities in current operations
- Designation of an operations development team or DevOps to focus on assurance-tool and automation capabilities that improve service quality and staff efficiency
- Roles and responsibilities to identify vendor assurance capabilities and identify how they integrate into key operations processes
- Roles and responsibilities for process engineering and staff training to effectively implement process and tool changes
- Development of an assurance roadmap for tool, integration, and process changes
- Roles and responsibilities for success metrics for assurance management

These roadmap areas help to ensure both initial and long-term success with first-generation IBN networking capabilities. When these are operating successfully, the organization can turn to new features for integration and assurance that provide additional service quality and operations efficiency. For now, organizations should look for integration and assurance opportunities and work to incorporate those into existing process areas with available resources.

Next steps

Intent-based networking poses new challenges for infrastructure teams who typically need to develop new processes, skills, and responsibilities for ongoing success. The three process areas that warrant initial investigation in relation to next-generation network operations are lifecycle management, policy management, and assurance management. There are, of course, many other service management areas that are defined in the ITIL v4 service model that can also be considered for process changes.

This paper introduces process areas unique to next-generation network operations and includes guidelines for developing a new operational model. Organizations investigating the operation of IBN solutions should consider the following stepped approach for success:

- Review current state
  - Business requirements
  - IT challenges
  - Technical challenges
  - Current inflight projects
- Develop an operations transformation strategy
  - Next-generation use cases and impacts on operations
  - Identify transformation value via ROI, risk, or comparison models
  - Identify immediate opportunities
  - Create initiatives and assign roles
  - Time and budget resources
  - Risk and mitigation strategy
• Identify transformation requirements
  ◦ Organizational structure
  ◦ Process (lifecycle management, policy management, assurance management)
  ◦ Skills, roles/responsibilities, training, hiring, out-tasking
  ◦ Technology
  ◦ Governance and success metrics

• Change management
  ◦ Design approval
  ◦ Pilots
  ◦ Migration methods
  ◦ Communications
  ◦ Transformation steps
  ◦ Governance and success metrics
  ◦ Continuous improvement

Further assistance is always available by contacting your Cisco Services consultant. Additional operations white papers can also be found at: https://www.cisco.com/c/en/us/tech/availability/high-availability/tech-white-papers-list.html.

Appendix A: Acronym listing or full glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agile</td>
<td>A development methodology that utilizes an iterative approach that focuses on collaboration, customer feedback, and small, rapid releases.</td>
</tr>
<tr>
<td>DevOps</td>
<td>A development or release methodology that brings development and operations teams together. The smaller the team (with the fewest people possible in it), the faster the team can move.</td>
</tr>
<tr>
<td>IBN</td>
<td>Intent-based networking</td>
</tr>
<tr>
<td>SDN</td>
<td>Software Defined Networks</td>
</tr>
<tr>
<td>CI/CD</td>
<td>Continuous Integration/Continuous Deployment</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnect refers to the layers necessary for application connectivity and includes physical, link, network, transport, session, presentation, and application.</td>
</tr>
<tr>
<td>ITIL</td>
<td>Formerly an acronym for Information Technology Infrastructure Library, ITIL is a set of detailed practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. Generally replaced with the term ITSM.</td>
</tr>
<tr>
<td>IPAM</td>
<td>IP Address Management is a tool that manages and allocates blocks or individual IP addresses for the network</td>
</tr>
<tr>
<td>ITSM</td>
<td>IT service management. This is a general term describing a strategic approach to design, deliver, manage, and improve the way businesses use Information Technology (IT). An IT service enables access to information and processes to accomplish important business goals or otherwise provide value.</td>
</tr>
<tr>
<td>RACI</td>
<td>Method to define roles and responsibilities including those responsible, accountable, consulted, and informed.</td>
</tr>
<tr>
<td>RBAC</td>
<td>Rules-based access control</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>RBML</td>
<td>Rules Based Markup Language</td>
</tr>
<tr>
<td>CLI</td>
<td>Command Level Interpreter. The need to utilize CLIs in devices will diminish over time.</td>
</tr>
</tbody>
</table>