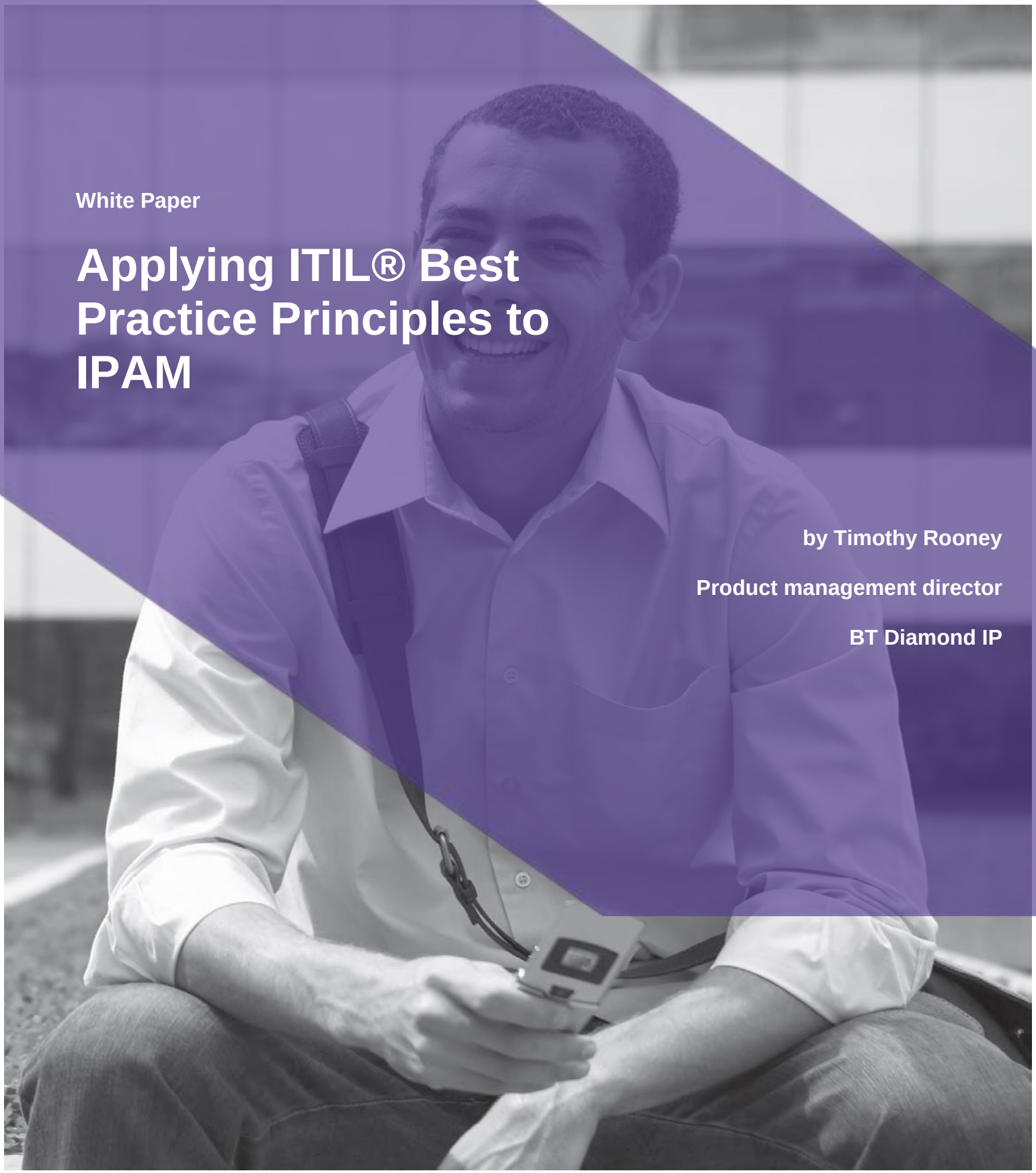
White Paper

Applying ITIL® Best Practice Principles to IPAM



by Timothy Rooney

Product management director

BT Diamond IP

BT Diamond IP

Applying ITIL® Best Practice Principles to IPAM

By Tim Rooney, Director, Product Management

Introduction

Many organizations have deployed network management systems and processes to provide structure and discipline to network configuration, changes and monitoring functions. Such discipline helps organizations reduce miscommunications and configuration errors, as well as continually improve processes and workflows. FCAPS has long been a standard framework for network management. Now the IT Infrastructure Library (ITIL) has come to the fore. Effective application of ITIL, either in concert with FCAPS or alone, can bring this important and potent discipline to the management of IP addresses.

This white paper will explain how each of the main ITIL areas can be applied specifically to IP address management (IPAM), and the benefits that can be accrued from using this management framework.

The FCAPS Legacy

To fully understand and appreciate ITIL, let's start first with a quick review of the International Telecommunications Union (ITU) network management standard FCAPS, which is an acronym for the five major management functions: Fault, Configuration, Accounting, Performance and Security. These five functions should be considered when implementing a network management architecture, whether it's for a service provider or enterprise-type environment. FCAPS is specified in the ITU's M.3400-series, which deals with telecommunications network management.

- **Fault management** deals with alarming and detection of faults within the various elements of the network and the localization or identification of the root cause of those faults, as well as the correction, repair, testing and trouble-reporting of faults.
- **Configuration management** involves planning, installing and provisioning of a new network element, as well as adding in customer related data. Provisioning of a new customer, for example, on a telecommunications-type service would impact the configuration management function.
- **Accounting management** addresses the collection of information that can be used, perhaps by a billing system. As such, the accounting management function measures the use of the network and associated resource utilization, which can be used to generate goals further on in the process.
- **Performance management** encompasses the evaluation and reporting of the behavior and effectiveness of network equipment. This includes measurement of capacity and quality of

transmissions, usage of network elements and CPU utilization. In a nutshell, it helps make sure the network is running on all cylinders.

- **Security management** deals with the prevention, detection and containment of any security issues or concerns related to access controls. It also has an audit logging capability in order to troubleshoot or analyze any violations or to detect security violations.

Understanding ITIL

FCAPS was developed as a standard for management of telecommunications service providers' networks. The IT Infrastructure Library®, which was developed by the U.K. Office of Government and Commerce, provides a similar approach, but is geared to enterprise IT organizations with the aim of giving them a service-oriented approach, with IT acting as the service provider.

ITIL Version 3 is the most recent release. Compared to Version 2, the primary difference in Version 3 is the introduction of the service lifecycle structure. However, many of the main Version 2 processes are still valid. Some of these processes were split in Version 3; others were added. For example, incident management in Version 2 incorporates both the handling of service interruptions and service requests, whereas in Version 3, incident management covers only service interruptions while service requests, such as changing a password, are broken out into a request fulfillment process.

The ITIL Version 3 service lifecycle perspective incorporates five key phases, as shown in Figure 1. Starting from the left, Service Strategy entails the service and design, development and implementation of service management as an organizational capability and a strategic asset. That strategy, once developed, can feed into Service Design, which involves the design of new or improved IT services and services portfolios based on these strategic objectives.

Figure 1: ITIL Version 3 Service Lifecycle

The design itself can then move to the Service Transition phase, where new implementations (whether new infrastructure or new releases on the existing infrastructure) or the introduction of new services or new elements are transitioned into operation while minimizing the risk of disruptions or outages.

The Service Operation phase addresses day-to-day operations, that is, the daily delivery and support of these IT services. Finally, feedback from constituents feeds into the Continual Service Improvement process. This phase encompasses guidelines for improving services, by either

updating the strategy (perhaps some new technology has arrived that can provide better services) or any of the other phases in a continual feedback loop.

Note that another standard based on ITIL is gaining momentum: ISO/IEC 20000 Information Technology – Service Management. This powerful approach combines the guidance of ITIL best practices with a measurable and auditable set of specifications that can be independently verified. While ITIL provides guidance, ISO/IEC 20000 provides measurement.[1]

FCAPS vs. ITIL

A comparison between FCAPS and ITIL is shown in Table 1. FCAPS, as previously mentioned, is an ITU standard with a primary focus on telecommunications. ITIL, though not technically a standard, is focused on enterprises, though with a service-provider perspective.

Table 1: FCAPS/ITIL Comparison

	FCAPS	ITIL
Standard	ITU	None
Focus	Telecom	Enterprise
Coverage	Narrow – implementation	Broad – strategy, implementation, continual improvement
Orientation	Functional	Service
Advocates process	Yes	Yes
Proven, repeatable, disciplined	Yes	Yes
Best practices framework	Yes	Yes

FCAPS is narrow in scope with its focus on the nuts and bolts of implementation, e.g., what to do when you get an alarm. ITIL has a much broader scope, encompassing strategy and continual improvement along with implementation. ITIL looks at how IT can help the business—not only executing tasks from a brute-force methodology, but also folding IT into the overall strategy to provide the best service possible.

From an orientation perspective, FCAPS is functional and task-oriented, whereas ITIL is service-oriented. Both FCAPS and ITIL advocate documented processes and proven and

[1] For more detailed information on ISO/IEC 20000, see BT white paper "Better Governance through ISO/IEC 20000."

repeatable disciplines that can be executed by anyone, with the expectation of achieving similar results each time. And both form the foundation of best practices frameworks for their respective focus areas.[2]

Understanding IPAM

Before we discuss how ITIL, as well as FCAPS, applies to IP address management, let's start with an overview of the key functions IP address management performs.

IPAM is comprised of three key functions:

- IP address inventory of address blocks, subnets and individual IP addresses
- Dynamic Host Configuration Protocol (DHCP) server management
- Domain Name Server (DNS) server management

IP address inventory entails rigorously tracking your IPv4 and IPv6 address space, allocation of address blocks and subnets and inventorying individual IP address assignments, whether they are static addresses for routers or servers, or those within an address pool. For address pools within subnets, the configuration of DHCP servers must be performed in accordance with the address plan such that end users accessing the network may automatically obtain IP addresses from the proper pools using the DHCP protocol.

Likewise, for static addresses in the address plan, you're going to have routers and servers and other devices that are statically configured, hence their denoting as static addresses. Once configured, you can reach these devices by the corresponding IP address. But you might want to reach them by name as opposed to remembering each device's IP address. Fortunately, DNS provides a way to map a device name to an IP address so I can type in my router's name, which my browser looks up in DNS, to find the corresponding IP address and connect to it. DNS provides that hostname to IP address mapping, and a lot more.

To summarize, the IP address plan component of IPAM minimizes the chance of errors in assigning the same address to one or more static addressed devices, let alone to portions of an address pool configured on a DHCP server. The use of DHCP itself automates address assignment; once configured in accordance with the address plan, a DHCP server dispenses addresses from its pools to laptops, printers and other devices as needed to access the IP network without manual intervention. Likewise, DNS works behind the scenes to resolve host names into IP addresses so computers can communicate and people can use them. IPAM helps IP network administrators cohesively manage these three core components—IP inventory, DHCP and DNS—to provide users easy access to and use of the IP network. Like other aspects of network management, IP address management should follow a rigorous and disciplined approach.

---

[2] For a more detailed discussion of ITIL, see BT white paper "The Hidden Value of ITIL – How it Facilitates Effective IT Governance."

Applying FCAPS to IPAM

FCAPS defines a disciplined network management-type approach for managing network elements. IP addressing, DHCP and DNS are critical network services, so application of a disciplined FCAPS framework is appropriate

- **Fault management** deals with the detection of DHCP and DNS server faults. This includes troubleshooting, isolating and resolving the faults through the monitoring and alerting process.
- **Configuration management** encompasses the accurate configuration of DHCP and DNS servers so that the DHCP address pools are consistent with the address plan and DNS-hostname-to-IP-address mappings are likewise consistent. Having a consistent and accurate address plan using a centralized inventory can help assure the accuracy and proper configuration of the DHCP and DNS services.
- **Accounting management** can be applied to IPAM with respect to tracking the usage of IP addresses. Being able to track what IP addresses an employee used over a specific time period is very helpful from an accounting management perspective.
- **Performance management** monitors resource utilization of the DNCP and DNS services and IP address space in general. It enables network administrators to know if they have enough addresses in their address pools and if the servers are running at full capacity from a processor and memory perspective.
- **Security management** supports network access controls. Its goal is to make sure not just anybody who connects to the network gets an address by providing some level of access control, as well as administrator access control. Audit logging for spot checking, troubleshooting and just for general auditing purposes also falls under security management.

Clearly, FCAPS principles can be applied to IPAM, and hopefully the IPAM solution you choose gives you the key functional areas needed from an FCAPS perspective without having to purchase additional tools

Applying ITIL to IPAM

There are a number of drivers that are spurring the use of ITIL best practice principles in IP address management activities. These drivers can be divided into two groups: business drivers and technical drivers.

Business drivers

Since ITIL is focused on the big picture—the business, the strategy and so forth—business drivers are the primary push for applying ITIL to IPAM. The most important business drivers are:

- Reducing the cost of delivery of IT services.

- Improving IT service levels and consistency—for instance, consistently allocating a new address for a user within two hours.
- Managing risk bybeing able to identify risks up front and developing backup plans.
- Maximizing efficiency by documenting processes, executing them the same way every time and by honing them over time through the continuous feedback cycle.
- Meeting regulatory and compliance requirements (may be industry specific).

Technical drivers

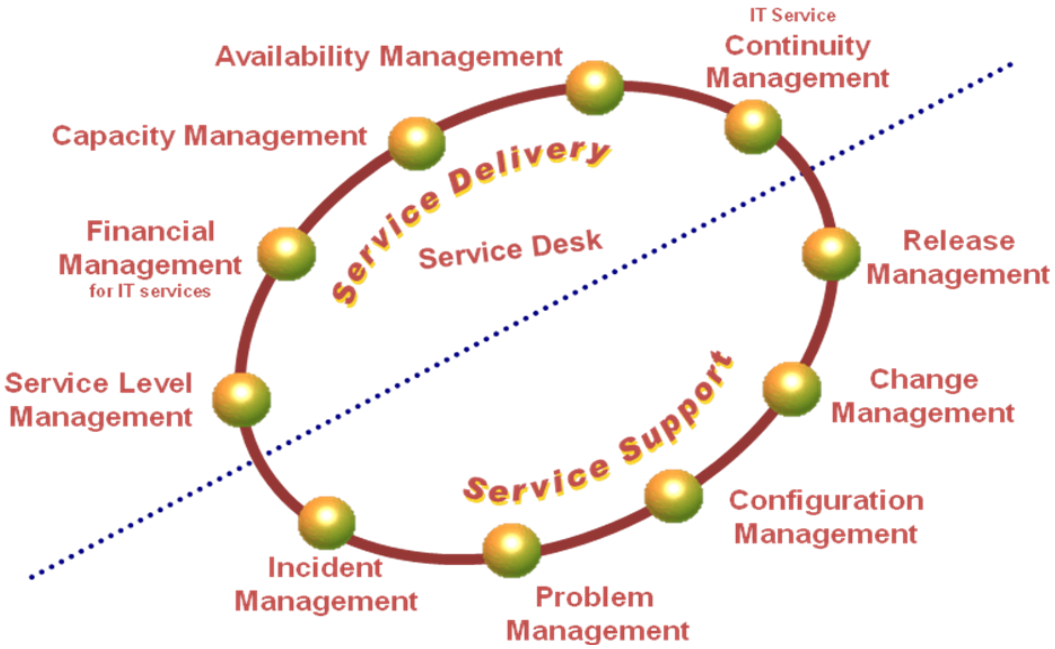
As previously stated, IP inventory, DHCP and DNS form the glue layer between applications and the network. When users connect to the network, they must get an IP address. They don't want to have to think about it; it should just happen. Likewise, when users type a website address, the network should just take them there without them having to think about the IP address assigned to that website.

DHCP and DNS are critical network services, and configuring these services needs to stem from a centralized IP addressing plan. Maintaining a plan and updated documentation is a key ingredient in implementing a disciplined process like ITIL.

ITIL process areas

ITIL Version 2 processes are split into two areas: service delivery and service support, as shown in Figure 2. ITIL Version 3 has some splits in additional services, but for simplification, I'll focus on V2, as these still apply in a V3 world with only minor modifications.

Figure 2: ITIL Version 2 Process Areas



Service delivery

- **Service level management** entails specifying and measuring the level of service that IT provides, for instance, provisioning an IP address for a new server within an hour.

  IPAM impact: This process seeks to define and measure the level of service provided to those requesting IPAM related services, whether it be end users requesting an IP address or the business needing to open a new retail office. Treating the end user or the business in these cases as customers, this process seeks to gauge whether service delivery is meeting defined service levels, such as timeliness of completion of these requests. Automating IPAM related service delivery, whether solely IPAM-impacting such as these examples, or involving IPAM as part of a larger IT service such as VoIP deployment, facilitates timely and accurate services delivery.

- **Financial management** deals with accounting, similar to accounting management in the FCAPS model except it addresses actual dollars and cents as well. It also addresses chargebacks or allocations for certain departments, for example, under an IT funding allocation model. Depending on your business model, the financial management area may have a large or small focus.

  IPAM impact: If you are accounting for IP addresses in use by user or department, you will need to archive historical data in order to track usage over time and apply it to the billing cycle. Audits and history data in your IPAM system can be a big help with allocation or conducting a business case analysis.

- **Capacity management** involves making sure resources are available for a business to conduct its work.

  IPAM impact: As related to IPAM, capacity management means making sure there are sufficient addresses in the address pools for employees to get an address and access the network. It also means tracking utilization, i.e., how the subnet is doing with respect to address assignment to ensure there are enough addresses even when there is a spike in usage. Being able to track and then look at address utilization trends helps to plan for adding or shifting capacity when increased usage is expected.

- **Availability management** involves assuring that IT services are available to end users, so that once they get on the network, they can access applications (and DNS servers to resolve hostnames).

  IPAM impact: Availability management applied to IPAM requires deploying DHCP and DNS servers in redundant configurations, and also assuring availability of the IP inventory and configuration functions. Redundant configurations include deployment of appliance clusters, multiple authoritative DNS servers for a given zone, one or more DHCP failover servers and a backup IPAM database. Monitoring of availability enables proactive detection of outages to facilitate rapid outage resolution (mean time to repair) while redundant components shoulder the load.

- **Continuity management** entails the provision of continuous services. For example, in the event of a disaster, this would ensure a disaster recovery plan is in place.

  IPAM impact: Continuity management deals not so much with the short-term perturbations with respect to availability management (although it is related) but rather with the bigger picture in terms of planning for redundancy. Namely, the IPAM system within a network operations center will likely require redundancy planning and implementation. A backup IP address management database stored at an alternative site can be accessed should the primary site suffer a severe outage.

Service desk

In the center of the circle is the service desk, which is the interface to the user community. It serves to funnel user requests or problems to any one of the other ITIL areas around it, providing end users with a helpdesk-type function.

IPAM impact: Providing service-desk personnel access to IP inventory information is critical to providing good service. For instance, if a person located in the New York office is not able to get an IP address, the service desk needs to know the address plan for New York in order to focus the problem and trouble resolution process on that particular subnet, associated routers or DHCP/DNS servers. Possessing IP inventory information is also necessary to construct a planned-versus-actual view of that inventory. An inventory on a spreadsheet is great, but requires constant updating. So having the ability to collect information from the network and then compare it with the plan is key. Audits go hand in hand with inventory information collection. Arming the service desk with this information can provide a solid first line for addressing calls immediately, or to at least moving them through the process more quickly.

Service support

- **Incident management** involves tracking and resolving incidents. In ITIL V2, it also deals with change requests, whereas in Version 3, these are split into separate process areas.

  IPAM impact: Access to IP inventory data is indispensible to troubleshooting and incident resolution. In addition, proactive monitoring with thresholds, alerts, logging information and audits can provide a head start to incident detection and management.

- **Problem management** calls for tracking a database of known problems and resolutions. For example, if someone calls into the service desk with an issue it gets bumped over to problem management, which can quickly determine if this is a known issue and if a resolution exists.

  IPAM impact: Collecting a database of problem information can be accomplished through logging, inventory and audits, as well as network management and system integration. IPAM is a key part of the overall network or IT service management approach, but it's not comprehensive. Having that integration is a key to having a holistic view of the problem management scope.

- **Configuration management** in ITIL is similar to the FCAPS configuration management functionality in terms of identifying, recording and controlling configuration items affecting IT services.

  IPAM impact: Configuring new address pools from a DHCP perspective, zones and resource records in DNS, subnets on routers, etc. all fall into the realm of configuration management. Administrator controls are necessary to ensure that changes to DHCP and DNS configurations are done with the appropriate permissions. For instance, you may want administrators to be able to make changes, but not actually deploy them on the DHCP and DNS servers, restricting that function to a higher level of administrator.

- **Change management** provides controls on the implementation of changes in the IT infrastructure. This involves assuring that all affected parties are in agreement with respect to the scope and implementation timing of the proposed change.

  IPAM impact: The scope of change management commonly affects IPAM components, such as the addition of an address pool, deployment of a new DHCP/DNS server in the network or upgrading a server to a new software version. Basically, anything affecting any part of the infrastructure, whether it's physical or software or even underlying appliance operating system, falls under the change management process, which makes sure all appropriate approvals are in place and corresponding back-out plans are available.

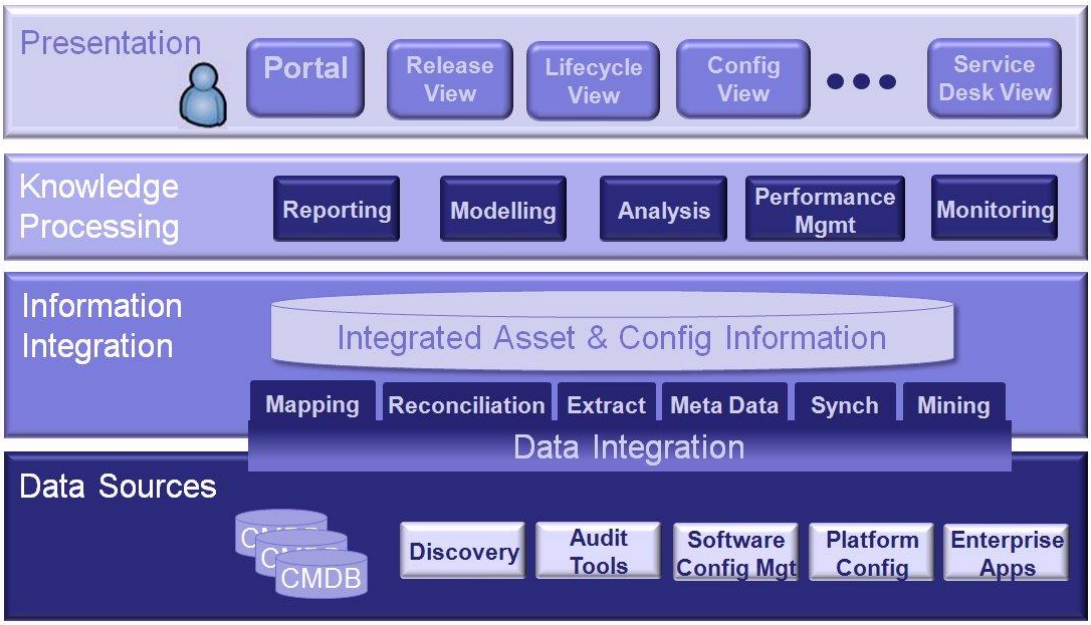
- **Release management** deals with software versions, not only for operating systems, but also for applications.This process area is responsible for making those versions available and making sure there's an authorized set of releases and versions available that can be deployed appropriately.

  IPAM impact: Release planning, release management and dealing with upgrades and patch management for DHCP and DNS servers from a central location can be a big timesaver. The alternative, requiring on-site upgrades of operating systems, patches and application software is costly and time-consuming. Release management of the IPAM system also falls within this category.

Configuration management example

Now that we've summarized the major ITIL process areas and how they apply to IPAM, let's take a closer look at configuration management, which is shown as a layered approach in Figure 3.

Figure 3: Configuration Management Layered Approach



At the bottom of the figure are the data sources, basically what is on the network. The configuration management database (CMDB), which is depicted as a collection of databases, tracks network configuration information, including IPAM information.

Data sources can be accessed or supplemented through various techniques such as discovery, audit tools for tracking, configuration management software, platform configurations and other enterprise applications. The information integration layer seeks to blend these disparate data sources into a holistic repository of integrated asset and inventory information using a variety of techniques such as mapping, reconciliation, meta data, et al.

Moving up the graphic, knowledge processing takes that integrated information to process it based on varying perspectives, for instance, modeling the addition of a new network element in order to understand how it will impact capacity and performance. Knowledge processing then feeds this data up to the presentation layer, which is where end users access that information, typically in the varying views of the multiple users of the information, such as those involved in release planning, configuration management, service desk, etc.

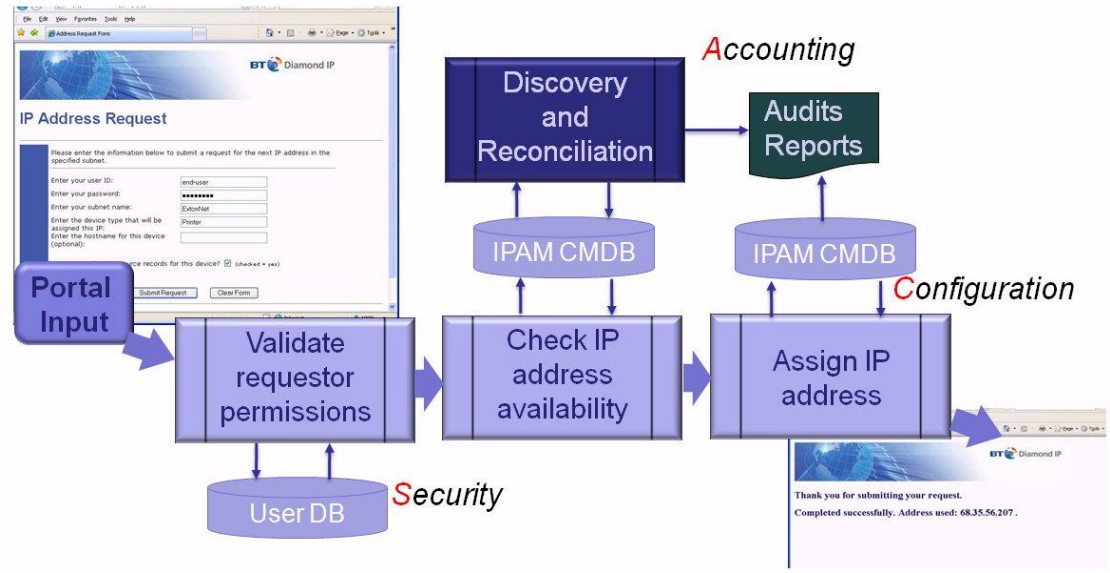
The idea behind this layering approach is to be able to blend all data sources together to provide a holistic view from the perspective of a particular end user. Let's say you wanted to see the lifecycle view of a given network element. Being able to filter through the reporting and the associated integrated asset and configuration information affords a lifecycle view of the utilization of a given address pool, for example.

The portal view

Now let's take a quick look at an example portal view as depicted in the presentation layer of Figure 3. A portal provides a convenient and simple means to illustrate this process through the

stack. Figure 4 shows a Web-based IT services portal that allows end users to make simple requests, such as requesting an IP address.

Figure 4: Requesting an IP Address



Let's say a user wants to add a new server to the network in the Philadelphia office. To do so, she would log into the portal. Once authenticated, she can check address availability by looking at the IPAM configuration management database, which enables her to determine which subnet in a given location has an IP address available for the server. In the background, the discovery and reconciliation process assures that addresses in the database match what's actually being used in the IP network. Finally, the user assigns the IP address, which of course needs to also be reflected in the configuration management database. All of this can then be audited at a later time for accountability tracking or troubleshooting.

This portal concept avails the end user instant gratification by providing an address when they need it without undue delay. It also helps to offload work from the IT organization by automating this service request function. It also improves service delivery.

Conclusion

Whether you're comfortable with the tried and true FCAPS model or the evolving ITIL service management approach, the institution of a disciplined and documented approach to performing IT functions can help save time and money. Performing service delivery functions in a consistent, repeatable manner yields predictable and measureable service levels. These service levels can then provide a measure of IT service expectations for the end user community and enable IT to meet or exceed such expectations regularly, maximizing efficiency and productivity.

As IT services increasingly require IP-based applications and services, the reliance on an effectively managed IP network grows. It follows that IP address management functions should be on the forefront when implementing a disciplined IT management scheme. The IPControl™ Sapphire product line from BT Diamond IP addresses many of the IPAM impacts discussed in this white paper and can provide a key ingredient in implementing FCAPS and/or ITIL.

About BT Diamond IP

BT Diamond IP is a leading provider of software and appliance products and services that help customers effectively manage complex IP networks. Our next-generation IP management solutions help businesses more efficiently manage IP address space across mid-to-very large sized enterprise and service provider networks. These products include IPControl™ for comprehensive IP address management and Sapphire Appliances for DNS/DHCP services deployment. Our cable firmware management product, ImageControl™, helps broadband cable operators automate and simplify the process of upgrading and maintaining firmware on DOCSIS devices in the field. Our customers include regional, national and global service providers and enterprises in all major industries.

For more information, please contact us directly at +1-610-321-9000 worldwide, email to btdiamondip-sales@bt.com or consult www.diamondipam.com.