Best Practices for Inside Plant Administration and Oversight

January 2019

For additional information, please contact:

Planet Associates Inc.
24 Wampum Road
Park Ridge, New Jersey 07656
(201) 693-8700
www.planetassoc.com
info@planetassoc.com

Contents

Introduction

This document outlines a general approach to enable an organization to effectively document and manage its Inside Cable Plant (ISP) infrastructure. The approach assumes that a configuration management system (CMS) is in place to consolidate the necessary infrastructure data and facilitate the noted recommendations.

Scope

This document focuses on ISP infrastructure, and is limited to providing a general business approach to documenting and managing ISP. It also outlines many of the benefits that can be realized as a result of such an effort.

ISP Overview

ISP forms the physical foundation over which signals are transmitted throughout a building, and as such is a critical component of any organization's IT infrastructure. ISP is a very simplistic term. “Plant” refers to all layer 1 telecommunications infrastructure, to include cabling, pathways, and electronic equipment. For the purpose of this paper it is expanded to include local area network (LAN) circuits running over devices and cables as well. “Inside” limits the scope of the infrastructure to the insides of buildings. The term ISP can be contrasted with OSP, which refers to the infrastructure beginning at the building demarcation point (or demark) and travelling outside of the limits of the physical building.

The Entrance Facility (EF) is the first room within the ISP encountered by a signal entering a building. This room contains the demarc, a panel or set of panels that marks the transition between ISP and OSP. In large buildings, the next major sub-component of ISP is the main distribution facility (MDF), which may or may not be coincident with the EF. This room controls the distribution of backbone cables to the building's different floors or to different areas within a very large floor. These backbone cables may run to intermediate distribution facilities (IDF), which act as midway consolidation points for sets of floors or sectors within a very large floor. Backbone cabling will then run from the MDF/IDF to telecommunications rooms (TR[i]). A TR controls the distribution of cabling to individual user stations in a building. The cabling that runs from a TR to an office or workstation is called horizontal cabling, since these cables typically run horizontally throughout a single floor area. This can be contrasted with the term risers or verticals, which are often used to refer to backbone cabling that travels between floors.

The scope of each of the terms above (EF, MDF, IDF, TR) vary depending upon their environment, so it is important to understand the role that each facility type plays in the site's distribution structure. For example, MDF traditionally refers to the central consolidation point for a building, but in campuses with multiple buildings it is not uncommon to see individual building consolidation points referred to as IDFs, because of their “intermediate” distribution role in the overall plant topology. In addition, it is not uncommon for a single room to serve multiple purposes. An IDF may distribute backbone cabling between

[i] TR is synonymous with telecommunications closet (TC).

multiple TRs, but it may also contain a TR that distributes horizontals to offices and work stations in close proximity.

Within each of the facilities described above, there is a voluminous variety of electronic equipment and intra-room cabling. The equipment can generally be categorized as either active or passive. Active equipment has a heartbeat on the network and generally performs intelligent functions, such as storing data, routing signals, or monitoring the environment. Passive equipment, such as a patch panel or splice case, does not perform intelligent functions, requires no external power, and does not have an identity on the network. All of these devices are connected to each other through backbone cabling (which connects devices to equipment in other rooms or workstations), structured intra-room cabling, or patch cabling. Structured intra-room cabling is permanent cabling used to link racks together within a room. Patch cabling (which includes cross-connects) is used for administration and usually connects devices in the same rack or adjacent racks.

Pathways are used to house cabling traveling from one location to another, and are an important part of the ISP. Pathways come in many different forms, from open cable tray to enclosed conduit, and a lot of planning is required to ensure that cabling gets from place to place without having their signals degraded and still allowing room for growth.

LAN circuits are another important part of the ISP. They are used to associate specific signal paths with external or internal service providers. Before computer networks existed these circuits were used to associate telephone numbers with the static signal paths running from faceplates back to private branch exchanges (PBX). While this infrastructure is still used in some organizations, many have switched to IP-based telephony, where a phone number is no longer tied to a specific signal path but rather is dynamically routed according to the IP-enabled phone plugging into the network. Still, LAN circuits can be important to track inside a building. Instead of documenting data circuits all the way to user faceplates, however, they are typically now only documented from the EF to a switch.

Pre-Implementation Steps/Considerations

ISP and its components can be represented in a variety of ways. In general, there is a trade-off between the level of detail maintained in the CMS and the system's ease of maintenance. This is a very important consideration as too little detail or too much maintenance effort can place the continued usage of the CMS at risk.

The following tasks should be performed prior to the kickoff of an ISP documentation project:

- Establish the project team
    - Select the Project Manager.
    - Develop the team charter.
    - Select the team. Team should consist of subject matter experts (SME) from all key information technology (IT) infrastructure and/or facility management (FM) areas.
        - Recommended team members:

        - LAN operations
        - Applications
        - Network/Telecommunications
        - Facilities Management
        - Network Operations Center/Security Operations Center (NOC/SOC)
        - Acquisitions & Contracting
    - Develop the milestone plan with clearly delineated goals and trigger points.
    - Schedule regular In-Process reviews.
- Conduct project kickoff meeting including CMS representation to provide the team a technical overview and field product-specific question/concerns.

Preliminary Decisions

The first decision when establishing an ISP documentation project is whether the goal is to document only what exists or whether it will also be used as an opportunity to establish and enforce new standardization upon the infrastructure. The latter case does not apply to all scenarios. For example, if the existing infrastructure is well-organized and labeled according to a centralized set of standards, there may be no need to change what is already being done correctly. In addition, if the project is to design a new ISP installation in the CMS and use it to facilitate the build-out process, then this decision may be inapplicable. However, most organizations who seek out a CMS do so because their existing infrastructure is in some form of disarray.

It is important to realize that surveying the infrastructure, standardizing the infrastructure (common naming/labeling scheme, change management processes, etc.), and loading the infrastructure into the CMS are three separate and distinct projects. As such, they each need to be accorded time in the overall implementation schedule, and it may not make sense based on the circumstances to attempt all three projects simultaneously.

The second decision is a determination of the extent to which the ISP documentation may need to interface with other systems. These systems can include help desk applications, configuration management tools, property management databases, and many other components of a federated configuration management database (CMDB). It is also important to think ahead to whether the CMS may be used by the organization to document infrastructure other than ISP. For example, if the CMS is to be used to document OSP as well as ISP, then the ISP will need to be designed in such a way that signals can be traced through the demark. This typically means that the connections in the ISP must be managed at a media-level rather than a cable level.

It is important to consider the role that pathways will play up front. By spending the time in the initial phases of the implementation setting up all of the cable routes, it is possible to save time down the road when it comes to ensuring that imported cabling is following the correct physical path through site floor plans.

Note: the need for cables to follow their real-life routes and be assigned to pathways is not a requirement for every implementation. It adds a lot of work, and every customer may not see the benefits as outweighing the costs. But without having cables run through pathways, it is very difficult to diagnose the impact of a particular pathway being cut by wayward renovators, or to ensure that critical backbone cabling is traveling along diverse physical paths.

The choices from the options above may not be obvious, in which case it is necessary to weigh the costs and benefits of each option carefully. Oftentimes a readiness assessment is necessary to fully determine the consequences of these choices. A readiness assessment can determine the extent to which survey work needs to be done, the ease with which it will be possible to load existing documentation, and the quality and consistency of the current standards in practice throughout the ISP. It is also important to see the quality of data and level of detail maintained in the systems to be integrated, in order to determine an accurate estimate of the effort required to complete desired integrations.

Readiness Assessment

The ISP facilities manager and supporting staff, with the assistance of CMS personnel, should undertake a readiness assessment of the existing environment prior to implementation. This will involve input from every discipline in the management and configuration of the existing ISP operational environment. The purpose of this study is to identify the accuracy of existing documentation, information systems, standards, processes, and procedures. Below are the focus areas needed to provide documentation and control:

- Supporting infrastructure
- Service Level Agreements
- Asset Management
- Contract Management
- Financial Management
- Change Control
- Network Architecture
- Capacity Planning
- Stakeholder Management
- Resource Availability
- Logistical Planning
- Continuity of Operations / Disaster Recovery

The process of gathering and collecting this information may take months of audit, discovery, consolidation, correlation, and planning to complete. To effectively complete this phase, it is essential that a comprehensive set of data requirements for each input is clearly identified as these will drive the data collection process.

The organization does not benefit by taking a rushed or compressed approach to this assessment, as the information gathered during this process provides the strategic foundation for ensuring the successful documentation and maintenance of hardware, connectivity, and circuit data. It is for this reason that readiness assessments are typically performed after the project kickoff. While not ideal (as it means that the kickoff is run without the benefit of the knowledge that such an assessment provides), it is typical.

Readiness assessments are serious undertakings, and are projects all by themselves. If it is not undertaken as a separate pre-project, then it will be necessary to hold at least one follow-up kickoff meeting to discuss the assessment's findings and synchronize all stakeholders prior to ISP documentation and implementation.

Data Analysis

As part of the data collection process, it is essential to identify the customer's analytical requirements, expectations, and the minimum data requirements to assist in determining a transition plan. While it is possible to identify analytical requirements common to most ISP infrastructures, it is also essential to address any customer-specific requirements. The outcome of this analysis will drive the data collection requirements and detailed plans for the baseline data calls necessary to complete the data collection phase.

Analytical requirements should be collected by means of formal meetings and documentation so that a concise data collection plan can be formulated and agreed upon.

Infrastructure Documentation

The most important aspect of managing infrastructure is having up-to-date documentation detailing the current configuration. The administration team needs to understand the current configuration to foresee the impact of infrastructure outages or proposed configuration changes.

Data Collection Framework

Before being able to determine the best representation of the data from existing repositories, it is necessary to obtain a clear and concise picture of any existing infrastructure and its physical dependencies. This will require a thorough and coordinated data collection and audit plan to ensure that the relevant data is captured correctly.

For each ISP component, it is essential to:

1) Define the requirements for data collection and how different information sources will be correlated
2) Identify how the collected data will be presented and the analytical functions required
3) Define a mechanism for controlling and tracking the transition of each component's documentation from the legacy system

During each phase of this process, the information should be funneled into a single repository that becomes integral in procedures for updating data, retrieving data, and performing analytics.

A number of data collection initiatives are needed from varied disciplines to obtain and correlate the existing information into a format that can be loaded into the CMS. For each discipline, it is essential to classify and define the data collection requirements and expectations, and each must provide all information present in the minimum data collection requirements. By using this methodology, it is possible to define a clear, comprehensive data baseline.

If not previously completed in the Readiness Assessment, it is necessary for the manager of each discipline to provide access and information regarding all existing data repositories and information sources that are currently used to maintain and store their data. Once each repository is identified, then it will be analyzed by the implementation team leaders to identify any data which can be provided to the CMDB.

Floor Plans

The facilities department is generally responsible for obtaining and/or maintaining accurate floor plans for the building. These floor plans provide the underlying visual context for the ISP infrastructure, and as such are the foundation of the ISP documentation.

Pathways

Pathway routes are often embedded in floor plan drawings. It is rare that pathway details are found in spreadsheets, but it does happen. In many cases pathways are referenced in spreadsheets as being associated with specific cable paths. For these cases, it can be tedious to review all of the cable paths in order to consolidate a single list of pathways, and it may be less time-consuming to construct the pathways from floor plans or other means. However, the cable-pathway associations are important as they can be used to import cables and route them automatically.

Equipment Details

The Product Library stores templates for specific models of equipment. These templates (referred to as library objects or library definitions) consist of information that is common to every instance of that model that is entered into the CMS. This information includes dimensions, model number, port configurations, and many other details.

A library definition refers to a specific *model* of device, and a product instance refers to a specific device *unit* (with a unique serial number, etc.). This is important to know because once a library definition has been defined, it is no longer necessary to capture all of the details stored in that template. It is only necessary to relate the surveyed details for the instance (serial number, host name, asset number, etc.) to the correct library definition. Note that if, during survey, it is not possible to identify the specific model of the device being inventoried, then it is a good idea to note down the information that would otherwise be in a library definition. This information may then enable the correct mapping of instance to library or allow a new library definition to be created if necessary.

There are a number of properties that are important to collect when surveying ISP equipment infrastructure, including:

- Device Type, Make, and Model (used to match the device to a specific library definition)
- Device location (SDP, Room, Rack/Frame, Rack Unit)
- Device Serial Number, Asset Tag(s)
- Device owner / manager (if applicable)

The following details are also important to collect, though are generally only available for active devices, and so do not apply to patch panels, blocks, or any other passive infrastructure.

- Device MAC(s), Loopback IP
- Service Contract Details (CLIN, PO, Warranty)

Importance of Passive Infrastructure

The difference between active and passive equipment is outlined in the ISP Overview section. Active equipment, from a documentation standpoint, is much more likely to be currently tracked within an organization's property system. Active devices are typically much, much more expensive, and as such are afforded a spotlight in most IT Asset Management systems. For the purpose of ISP documentation, however, passive equipment is the true star.

Passive devices form the permanent structure upon which active devices may send signals and route network traffic. This category of devices includes faceplates, patch panels, fiber shelves, pull boxes, blocks, splitters, taps, and many other types of relatively inexpensive devices. Because these devices are generally treated as commodities, they are less likely to be labeled with asset tags or have visible serial numbers or even model numbers. This makes the documentation of passive infrastructure more of a challenge.

Subject matter expert support is generally required to document passive infrastructure successfully. IT facilities personnel or contractors doing the data collection will often survey a passive device and label it as a patch panel without describing how many ports and what types of ports are on it. And since there is no model number to cross-reference against specifications readily available on the Internet, this can cause problems if the specifications are inaccurate.

Horizontal and Backbone Cabling

Horizontal and backbone cabling are designed to be static fixtures in a building's ISP infrastructure. The cable types that are used in these runs are typically rigid and inflexible, and the connection types made on either end are generally permanent. Horizontal and backbone cables also rarely change pathway routes, which makes the maintenance of this information easy once it is loaded into the CMS.

In an ideal world, all horizontal and backbone cables in a building would be clearly labeled, with labels placed at the cable endpoints that indicated the near-and far-end connections as well as the cable's type, number of media, and unique identifier. This is not always the case, and surveying backbone cabling without the help of cable labels can be extremely labor-intensive and time-consuming. If labels do not exist on backbone or horizontal cables (or the devices to which they connect provided they indicate the far-end connection), then it is essential that someone who knows the infrastructure very well be made available to provide as much of that information as possible. If such a person is not available, then be sure to allow a lot more time in the survey schedule.

Within the CMS, horizontal and backbone cables are given unique identifiers that correspond directly with the endpoints of the cable. Because these cables do not change often, neither do these identifiers. This is contrasted with the identification and labeling for administration cables, which change often and are named in such a way as to avoid the hassle of changing labels and identifiers.

Patch Cabling and Cross-connects

Patch cables and cross-connect cables are intended for administration, and as such may be changed frequently. The cables themselves are flexible, and most of the cable ends have connectors on them that allow for easy disconnection and reconnection.

Because patch cables and cross-connects are typically very short, the pathway routes that they take from one device to another (either in the same rack or adjacent racks) do not need to be maintained.

Unlike horizontal or backbone cables, patch cables and cross-connects require frequent re-labeling if their labels include reference to both endpoints of each cable. There are a couple of approaches for dealing with this.

1) Label patch cables with a reference to only to one endpoint, and never administer on that end. So for example, if a patch cable was connected to a switch port on one end and a patch panel on the other, label both ends with the name of the switch and switch port. Just make sure never to change the connection on the switch side, or else both ends of the patch cable will be incorrect.
2) Label patch cables on both ends with an incremental identifier. So a patch cable might be labeled “C0023”, meaning “copper cable #23”. The endpoints that this identifier belongs to are then maintained in a separate location.

Both methods come with advantages and disadvantages. The first option runs less risk of having the patch cable label refer to incorrect endpoints, provided that one end is never changed. It is possible to purchase and install cable clamps that prevent individual cables from being manipulated on a single side, which would help enforce this rule. On the other hand, this option is less flexible and more difficult to maintain if there is additional work involved to change a connection on the unfixed end (such as pulling back a patch cable that runs to another rack and rerouting it to an adjacent rack on the other side).

The second option is more flexible, and may hasten the adoption of an external CMDB into the change management process if engineers are forced to use it to determine the endpoints of cables associated with a specific number. Unfortunately, changes that are not documented could lead to a situation in which the CMS is no longer trusted, which would likely hasten its demise.

With everything in consideration, the second option is generally recommended.

LAN Circuit Data Collection

LAN circuit data is generally maintained by the facilities engineers for the building. Network engineers may also be excellent sources of information for how circuit bandwidth is distributed throughout the network.

Network Diagrams

Network diagrams generally denote logical relationships between active network devices. As such, they do not usually include passive equipment or cabling details. It is very common for customers to provide logical diagrams to the documentation team and assume that everything needed to document the ISP infrastructure is included. This is rarely the case.

The proper documentation of ISP infrastructure will include, in addition to network diagrams:

- Rack elevations
- Patch cable and cross-connect cut-sheets
- Horizontal and backbone cut-sheets
- Cable types
- Details on device cards and modules
- Physical locations of infrastructure within a floor plan

Configuration Management

An effective Configuration Management (CM) plan provides the means to track and manage the topology, hardware, firmware, software, and code configurations in a diverse communications system.

The CM plan is built upon several components:

- Processes and procedures define the roles and responsibilities of the CM staff and define the mechanisms for tracking asset, circuit, or configuration changes. This includes changes from growth, design, or failures.
- A data management tool to store, maintain, backup and track system assets and circuits through their lifecycle.
- An inventory of manageable assets and circuits for all system components that reflect the hardware and software configuration of the fielded infrastructure. Configuration items are mapped to the infrastructure nodes in which they are installed.
- Infrastructure drawings maintained to illustrate the current system design.

Operations and Maintenance (O&M)

A typical O&M plan consists of a variety of workflows in which procedures are laid out and responsibilities are assigned for ongoing tasks such as repairs, upgrades, infrastructure maintenance, and MACs (moves, adds, changes). A chain of command is established to approve and document all changes in order to ensure current records, justify the need for changes, and limit unauthorized activities.

In a given organization, there are a number of tools used to facilitate these actions. Examples include a help desk system, a service provisioning system, and a CMS. These tools exist to make operations and maintenance easier by automating workflows, generating work orders, maintaining audit records, providing data, analyzing impacts, and reducing human error.

A well-organized change and configuration management system makes use of technology to perform these functions, but no single software product can do everything. In order to ensure streamlined processes, the various tools in use need to have a way to pass information back and forth. For this reason, application programming interfaces (API) are essential, and can be used to link multiple systems together in a way that preserves workflow and maintains consistency.

For example, a help desk ticket can result in a request for connectivity to a certain office. This request is sent to the CMS, which could be used by an engineer to analyze the current infrastructure in order to determine what ports are available and what ISP cabling may already exist to that room. The engineer initiates a MAC transaction, reserving ports on a switch and a patch panel within the CMS for this purpose. The CMS then generates and issues a work order and communicates the status of the MAC back to the help desk system, in case the user needs to be updated on the progress of the ticket. Once the physical change is complete, the engineer can finalize the MAC in the CMS, which communicates with the help desk system and provides an updated status along with a list of all the steps performed in the MAC, which is filed in the help desk system's records.

This is a simplified example of how connectivity might be provisioned. Depending on the organization, certain systems may not exist or may interact in different manners; but the example does serve to highlight the role that interfaces between software tools can play in streamlining activities. Without automated communication between systems, the odds of process delays or failure grow considerably.

Conclusion

This document is for general use, and as such does not take into account the subtle details that determine the most effective strategy for ISP implementation in a specific enterprise. It does provide a number of discussion points, however. All of the elements mentioned in this document should be examined for relevance, as it is *always* easier to adjust an implementation strategy prior to execution.

Should you require assistance, Planet Associates Inc. provides consulting services in addition to software tools. Their staff possess years of experience in designing specialized ISP documentation population and maintenance strategies. Planet personnel are also experienced in overcoming the inevitable difficulties that arise during any CMDB implementation.

Guide to Abbreviations

API	Application Programming Interface	LAN	Local Area Network
CM	Configuration Management	MAC	Move, Add, Change Transaction
CMDB	Configuration Management Database	MDF	Main Distribution Facility
CMS	Configuration Management System	NOC	Network Operations Center
EF	Entrance Facility	PBX	Private Branch Exchange
FM	Facility Management	SME	Subject Matter Expert
IDF	Intermediate Distribution Facility	SOC	Security Operations Center
ISP	Inside Cable Plant	TR	Telecommunications Room
IT	Information Technology		

Planet IRM

Planet IRM acts as a visual front-end to a comprehensive CMDB. This database stores ISP infrastructure information with an emphasis on the physical layer.

In addition to ISP, Planet IRM is able to document LAN, data centers, outside plant, wide area networks, and many other types of IT infrastructure. Combining all of these data points into a single CMDB can provide significant benefits over stovepipe systems in ease of maintenance, accuracy, and analytics.

The Planet IRM software is distinct from many CMS tools in that it does not actively monitor a customer's network, but rather focuses on the physical locations of network components and their relationships. In general, these physical data cannot be discovered, captured or managed adequately by Layer2+ discovery tools, and yet they are essential components for providing overall inventory and configuration management of each configuration item - be it a hardware element, location, or circuit connected to the IT infrastructure.

Planet IRM also acts as an aggregator of information. It can import and correlate logical relationships and discoverable data into the CMS, providing a comprehensive view of the infrastructure. This greatly assists in resolving conflicts between trusted data sources, such as:

- help desk systems
- billing databases
- network discovery tools
- patch management tools
- cut sheets
- logical diagrams
- ... and many others.