Cisco Discovery Service

Contents

Q. What is Cisco Discovery Service?

A. Cisco® Discovery Service is a set of advanced web services and tools to deliver detailed analysis and reporting on Cisco devices, including end-of-life milestones, security alerts, service coverage, IPv6 readiness, and other assessments. This information can be used to assess upgrade and service opportunities, and to identify hardware, software, and security vulnerabilities on existing equipment that could result in revenue opportunities from remediation. Cisco Discovery Service 2 expands the focus to address architecture-led selling. For more information, refer to the Cisco Discovery Service website.

Q. How do partners access Cisco Discovery Service?

A. Cisco Discovery Service is available through network assessment tools enabled for use with the service. Refer to the Cisco Discovery Service website for the current list of tools (or **desktop clients**). The CDS/360 web tools are accessible only to users who have completed an upload using one of the Cisco Discovery Service enabled clients.

Q. How do network assessment tools integrate with Cisco Discovery Service?

A. The user selects the option to submit the discovered data from his or her PC to Cisco Discovery Service through a secure Internet connection. Cisco Discovery Service acknowledges receipt of the network information and begins to process the data using Cisco Advanced Services inventory profiling services. No other action by the user is required. The user and his or her PC are free to move to another task.

Q. What does the partner need to make the connection to Cisco Discovery Service?

A. Partners are required to have a Cisco.com account with partner-level access credentials. In addition, certain data fields must be entered correctly for Cisco Discovery Service to function properly.

Q. Can you explain the Cisco.com partner-level access requirement in more detail?

A. The user must have a Cisco.com ID with access level 3, meaning that the ID has to be associated with the user's partner company. Users own their identity at Cisco; to protect their ID, this cannot be changed for them. Partners who do not have a Cisco.com ID can register for one. Following registration, users must associate their ID with their partner company, using the Partner Self Service tool. If a user cannot access Cisco Discovery Service, it may mean that he or she is not associated with the partner company and needs to use the Partner Self Service tool. For questions or assistance regarding your Cisco.com user profile or company profile, please contact Cisco's Partner Relationship Team.

Q. How do I access the Cisco Discovery Service CDS/360 web portal?

A. To access the CDS/360 web portal, you must complete a simple two-step registration process. The first step is to upload data to the Cisco Discovery Service back end for the first time, using your Cisco Discovery Service enabled desktop client. Once you have uploaded data, you are automatically registered to access the CDS/360 portal, which you can access via My Cisco Workspace. You first need to add the **Smart Services Connection** module to your workspace. CDS/360 will automatically be included as an available service within the Smart Services Connection module. See the CDS/360 User Guide for detailed instructions.

Q. Where can I see a demonstration and obtain training on the Cisco Discovery Service process?

A. Please refer to the Cisco Discovery Service website for the current list of Cisco Discovery Service enabled tools. Contact the appropriate vendor for training or demonstration assistance.

Q. How do I get support if I have problems using Cisco Discovery Service?

A. If you believe the problem may be related to the network assessment tool itself, contact the appropriate tool vendor for support. If you believe the problem is with Cisco Discovery Service, contact Partner Helpline.

Q. What devices will be discovered, and what results will I see from a Cisco Discovery Service enabled tool?

A. With Simple Network Management Protocol (SNMP) and Telnet enabled in the network, network assessment tools will return data related to each IP device discovered on the network. In the case of Cisco equipment, the resulting analysis is quite extensive. Cisco Discovery Service provides device inventory for core Cisco routing and switching devices and many advanced technology devices, as well as device end-of-life and end-of-sale milestones, Cisco Product Security Incident Response Team (PSIRT) alerts, service coverage (Know the Network, or KTN), product defect field notices, and validated serial number information. Most Cisco devices that support SNMP can be analyzed by Cisco Discovery Service, with the exception of some advanced technology devices (for example, wireless access points and IP phones), but these too are becoming supported through ongoing enhancements. By 2013, most Cisco advanced technology platforms should be supported.

Q. Where can I see the results of the Cisco Discovery Service processing?

A. The information processed by Cisco Discovery Service is returned to the user's computer and is available for reporting from within the network assessment tool application or from the CDS/360 portal. Report formats include Microsoft Word and Microsoft Excel within the desktop client tools, as well as Excel or PDF from the CDS/360 web portal. Both feature full color and graphics that are easily customized by the user. Visit the Cisco Discovery Service website to see sample reports.

Q. What happens to the customer data after Cisco Discovery Service returns the results?

A. The data is retained by Cisco in a secure database. The network assessment desktop client provides an option to purge the data after the transaction is completed. Assessment data can also be purged from the CDS/360 portal from the transaction screen General tab (Figure 1). Click a transaction in the summary screen to reach this tab.

Figure 1. Purging Customer Data

KTN Inventory Spec

Command	Mandatory	Notes
show version	Yes	Always gather
show inventory	Yes	All that is required is supported by device
show diag	Yes	Always gather for IOS devices
show hardware	Yes	Always gather for IOS devices
show c7200	Cisco7200 only	Required Only If You Have Cisco7200 Product *Family Routers*
show gsr chassis-info	GSR only	Required only for 1200 series routers
show chassis eeprom	10K only	Required only for 10000 series routers
[ADMIN mode] show inventory all or [ADMIN mode] show diag chassis	CRS-1 only	Always required if you have CRS-1 to gain chassis serial number. This is an Admin command.
show rsp chassis-info	7500 only	Required only for 7500 series routers
show module	Catalyst only	Required only if you have Catalyst Switches
show IDPROM all	Catalyst	Required only if you have Catalyst Switches

Q. Can network discovery be done remotely?

A. It is possible to perform a network discovery remotely using VPN, but it is not recommended. The service is best performed by the partner on site with the customer.

Q. What is the maximum number of devices that can be discovered and analyzed?

A. The maximum number of devices supported per transaction is 5000. However, for performance and transaction management reasons, it is recommended that you break large networks into logical segments no larger than 2000 devices each, such as physical locations and subnets. Larger device counts increase upload and download time, as well as processing time.

Q. How long does it take to process a transaction?

A. Processing time is affected by several factors, including the number of devices in a transaction, the number of user transactions queued, the types of analysis requested, and overall system performance. During peak usage times, transactions may take longer to process. On average, we have seen a processing time of approximately nine seconds per device. Also, uploading and downloading of data can add to the overall time. These processes are usually very fast for a small network, but can take longer for larger networks, depending on the factors listed above.

Q. What is the enhanced PSIRT feature? Why does it require device configuration data?

A. Enhanced PSIRT alerts (feature-based PSIRT alerts) are based on the running configuration. Telnet enable passwords are required in the network assessment tool.

- Basic PSIRT analysis returns only Potentially Vulnerable alerts, which can require a lot of unnecessary engineering time to review and remediate. Though this information can be useful to you and your customer to get a snapshot of the security posture, it is not very useful for fixing issues, because the sheer number of PSIRT advisories can be unmanageable, especially for large networks. Therefore, Cisco recommends enhanced PSIRT analysis for remediation of security issues and customer satisfaction.
- Enhanced PSIRT analysis uses the running configuration data to match PSIRT alerts based on the software features installed on the device. This extra validation means that there are more actionable (or Vulnerable) PSIRT alerts and fewer Potentially Vulnerable ones. This can be a huge time-saver for professional services partners, since it reports only PSIRTs that require action.

Q. What are field notices?

A. A field notice is an important advisory about a Cisco hardware or software defect that needs to be replaced or fixed. Usually this requires replacement hardware or modules, but it can sometimes include fixes occurring through a software upgrade.

Q. Can Cisco Discovery Service enabled tools discover wireless access points and IP phones?

A. Wireless access points, as slaves to a controller, and IP phones are not accessible by SNMP and have to be inventoried using different means. Although they may be discovered, they are not supported in the Cisco Discovery Service analysis at this time (nor were they supported in the legacy Cisco Discovery tool for the same reason). Access points and IP phones will be supported in an upcoming Cisco Discovery Service release, probably by early 2013.

Q. What can I do if a customer does not allow me to connect a non-company PC to their network for security reasons?

A. Please contact the Cisco Discovery Service tool vendor and ask if they will supply a software based tool that you can provide to your customer to facilitate their discovery. The will not have access to Cisco Discovery Service and must transfer the data to you, the Cisco partner, for analysis.

Q. What information should customers provide for a successful discovery?

A. The following information is needed at a minimum for a successful discovery:

- IP ranges, subnets, and a seed router
- SNMP read-only community string, username, and password
- Telnet username and password (non-enable)

In addition, if you wish to retrieve Cisco configuration files, you will need one of the following:

- SNMP read-write community string
- Trivial File Transfer Protocol (TFTP) access, username, and password
- Telnet/SSH enable password (required to get the enhanced PSIRT report)

Q. Is there a test/lab transaction for training or testing purposes?

A. Yes. To identify a test/lab transaction (recommended for noncustomer engagements), choose Test/Lab in the pull-down menu on the Submit Network Assessment Request screen. Test transactions may be limited to a smaller device set, so they should be used only for training or lab purposes.

Q. What market segments can I select for Cisco Discovery Service analysis?

A. Market segments and industry market selections are mapped to most standard Cisco sales markets. Market segments include:

- Commercial
- Enterprise
- Managed services
- Public sector (for government)
- Service provider
- Small and medium-sized business
- Test/lab for training and lab transactions

Q. Will I be able to tell which Cisco SMARTnet® Service contracts have expired on my customer's devices?

A. You may need to do some work in advance to obtain complete service coverage data in your Cisco Discovery Service reports. Specifically, you must use the Cisco Service Contract Center tool to associate yourself with your customer contracts. Here are three important links that can help you through this process:

- **Registering Contracts in Cisco Service Contract Center Tip Sheet:** http://www.cisco.com/web/SCM/KTNx/html/Registering_Contracts_Tip_Sheet.pdf
- **Cisco Service Contract Center Contract Management Job Aid:** http://www.cisco.com/web/SCM/KTNx/html/CSCC_Contract_Management_Summary_Job_Aid.pdf
- **Cisco Service Contract Center for Partners:** http://www.cisco.com/web/partners/services/resources/cscc/index.html

Q. Why do I not see detailed service coverage (or PSIRT) reporting for all my discovered Cisco devices?

A. **Default operation:** To protect partner proprietary information, Cisco has implemented procedures to ensure that the information partners see in the Service Coverage Report pertains only to the contracts registered to their Cisco.com user ID. Service contract information is blocked and replaced with "Other" when a device is covered by a service contract not registered to the partner's Cisco.com user ID. However, in all cases partners will see the item's serial number, product ID, and item type. To maximize the service coverage data they see, partners should ensure that all their contracts are properly registered to the appropriate Cisco.com user IDs within the partner company. More information about how to register contracts can be found on the Cisco Service Contract Center training website.

Exception process for better service coverage reporting: There are some situations in which you may be entitled to additional contract information, with the customer's permission.

Troubleshooting error-derived empty Service Coverage Reports and Know the Network (KTN) Actionable Network Snapshot Report (ANSR) generation: There are a few known issues that can result in either empty service coverage details in the Network Assessment Report (NAR) or failure of the ANSR available from the KTN portal. The most common is an incorrect discovery configuration, in addition to other system issues.

Register with the KTN portal first: Before using the KTN portal, you must register. To get started, go to http://tools.cisco.com/ktn/.

1. **If KTN fails to return service coverage data to Cisco Discovery Service, check the KTN portal for the ANSR:** If Cisco Discovery Service processing is complete and returns a message such as CMPLKTNERR or PRTLKTNERR, it means that Cisco Discovery Service processing completed successfully and KTN service reporting failed **or** that KTN missed its transfer window to Cisco Discovery Service for inclusion in the NAR. The errors are fairly rare, so it more frequently means that KTN did not return service coverage data in its required time window to be included in the NAR. The first step in troubleshooting is to check the KTN portal to see if the ANSR has been generated (you need to be registered on the KTN portal; see above for the registration URL). If the ANSR has been generated, you can use that for contract reporting, or if you need the service coverage included in the NAR, the best recommendation at this time is to re-upload the engagement data to Cisco Discovery Service and see if the combined report is generated.

Note: Cisco Discovery Service release 1.4 contained a new routine to help prevent the exclusion of KTN service coverage from NAR data. With this enhancement, service coverage data is added to the NAR data as soon as it is finished processing, without regard for the Cisco Discovery Service time window. In those cases, you will simply need to re-download the processed data and generate a new NAR, without a new transaction or a re-upload of data.

2. **IMPORTANT TIP: KTN service coverage and PSIRT data cannot be processed if the discovery configuration is incorrect (requires new collection):** One of the most common mistakes seen with users, which renders collected data mostly unusable and requires a new collection on the customer site, is a misconfiguration of the Telnet/SSH settings on the Discovery Configuration screen. Both KTN service coverage and accurate PSIRT mapping and reporting require specific command-line interface (CLI) commands to be issued, which requires that Telnet/SSH be enabled (in addition to checking the "Enable CDSs" checkbox). If this step is missed, KTN will not be able to validate serial numbers and the resulting contract mapping, and you will likely get an empty Service Coverage tab in the NAR and a mostly empty KTN ANSR, if the ANSR is generated at all. Or you may receive a KTN error on the Network Assessment Status screen. **To reiterate, if you do not enable Telnet/SSH on the Discovery Configuration screen, service coverage data will not be processed.** Additionally, CLI commands (show config and show running config) are required to collect the "features enabled" data, which is key to accurate PSIRT reporting. Without the CLI commands initiated, almost all PSIRT alerts will be tagged Potentially Vulnerable, and there will be a lot of them to sift through to determine real device vulnerabilities. So the Telnet/SSH enable setting in the discovery configuration should also be included for PSIRT reporting.
3. **IMPORTANT TIP: If contract data is missing, here's how to determine whether the discovery configuration was properly set up for Telnet/SSH collection.** The first thing users usually notice is empty service coverage details or, in the ANSR, that most or all devices are listed as unvalidated. But that in itself doesn't pinpoint the problem. To double-check this, you need to look at the PSIRT Details tab in the NAR (PSIRT reporting must have been enabled in the upload screen). Go to the NAR PSIRT Details Excel tab and scan through the Vulnerability column. If all, or nearly all, PSIRT alerts are listed as Potentially Vulnerable, and none or almost none are reported as Vulnerable (or if you have an inordinate number of PSIRT alerts), Telnet/SSH likely was not enabled and the collection must be rerun. **The combination of missing contract data and all PSIRTs listed as Potentially Vulnerable is a sure indicator that the CLI commands were not enabled.**

Q. How do I enable Telnet/SSH in the network assessment tool so that I receive complete raw data to process services coverage and PSIRT alerts?

A. Network assessment tool capabilities vary in this area. Check with the assessment tool vendor.

Q. I registered my missing service contracts in the Cisco Service Contract Center. Do I need to resubmit my discovery data to see the results?

A. If you previously submitted your discovery data (and all the device data was there), you can just click the existing Service Coverage Report link in the NAR to go to the KTN portal and retrieve the full ANSR, which will have been updated in real time. However, if you want to see the service coverage information updated in the NAR, you will need to resubmit.

Q. Is SSH is an option rather than Telnet?

A. Yes, you can use Telnet or SSH or both.

Q. Will network assessment tools discover Cisco Unified Communications Manager and other unified communications servers?

A. Network assessment tool capabilities vary in this area. Check with the assessment tool vendor.

Q. Is there any way to define multiple enable passwords?

A. Network assessment tool capabilities vary in this area. Check with the assessment tool vendor.

Q. Can I modify the collected IP addresses before uploading them to Cisco in order to hide details about the customer network?

A. There is no need to modify collected IP addresses, as they are automatically removed before they are submitted to Cisco for analysis. The assessment tool internally maps IP addresses to a locally generated device ID, which is sent to Cisco. After the analyzed data is returned to the tool, the device ID is mapped back to the appropriate IP address.

Q. Can I create discovery reports for third-party equipment?

A. Network assessment tool capabilities vary in this area. Check with the assessment tool vendor.

Q. Is there a charge from Cisco for uploading a file to Cisco Discovery Service?

A. No.

Q. How does a network assessment tool actually inventory devices?

A. Network assessment tools use the Telnet, SSH, and SNMP protocols to discover and interrogate network devices. Using public MIBs, such as System MIB and Entity MIB, they collect information on the devices. Neighboring devices are discovered using user inputs, routing tables, Address Resolution Protocol (ARP) cache tables, and Cisco Discovery Protocol tables.

Q. Are Cisco IP phone serial numbers part of the information gathered for IP phones?

A. Network assessment tool capabilities vary in this area. For example, some use HTTP to discover information about Cisco IP phones, such as model number, MAC address, serial number, host name, sysDesc, and subnet mask. Check with the assessment tool vendor.

Q. Will assessment tools create a network map of the discovered devices?

A. Network assessment tool capabilities vary in this area. Check with the assessment tool vendor.

Q. Is the network assessment information transmission to Cisco encrypted?

A. Yes.

Q. Do network assessment tools work in a Multiprotocol Label Switching (MPLS) environment?

A. The basic requirement for discovery over MPLS is to have Telnet, ping, and SNMP access to the discovered equipment at all sites. Assuming that expansion from site to site is not possible, you will have to discover each site separately (using a seed router or address ranges). Network assessment tool capabilities vary in this area. Check with the assessment tool vendor.

Q. What is the difference between the service coverage reporting provided in the Network Assessment Report (NAR) and the full report that is available from the KTN portal by following the embedded link in the NAR?

A. **Register with the KTN portal first:** Before using the KTN portal, you must register. To get started, go to http://tools.cisco.com/ktn/.

The NAR provides a summary view of the full ANSR, restricted to the following fields:

- ANSR Cisco.com URL
- Validated serial number
- Contract number
- Ship date
- Service level

- Contract status (ACTIVE, OVERDUE, OTHER [owned by another entity or partner company, in which case contract number, service level, and coverage start and end date are not displayed], and BLANK [indicates no contract was found])
- Coverage start date
- Coverage end date

The following information is provided in ANSR and is also part of the NAR:

- Product ID
- Location
- Chassis (parent) and/or card (child)
- Last day of sale (LDoS): Cisco Discovery Service reports all lifecycle milestones, including:
  - URL for end-of-sale/end-of-life Cisco.com bulletin
  - LDoS announcement date
  - End of sale
  - End of engineering
  - End of contract renewal date
  - End of software maintenance
  - LDoS

The following information is provided in the ANSR but is not included in the NAR:

- Instance ID (specific to ANSR)
- Parent instance ID (specific to ANSR)
- Item type (covered in Cisco Discovery Service by chassis/card)
- Installed site ID (this could be added in the future, as we provide the data in the Cisco Discovery Service data stream)
- Installed-at customer
- Installed-at customer address
- Contract bill-to name
- Contract bill-to ID
- Part confidence

Q. What is the reason for offering the NAR and ANSR as separate reports?

A. There are a number of reasons, including:

- Many users will want just one report that includes data on inventory, end of sale/end of life, PSIRT alerts, field notices, validated serial numbers, and contracts, without the more detailed service coverage reporting provided by the ANSR.
- The KTN ANSR report is the “single source of truth” for Cisco Discovery Service contract reporting. Due to differences in data processing and serial number validation, the ANSR report may be more complete and reliable than the NAR or Cisco Discovery Service contract summary report. Therefore, we recommend either the KTN portal ANSR report screen or the downloadable ANSR report. The KTN ANSR report screen can be easily reached from the CDS/360 Reports tab, to the right of the Service Coverage Report link.

- Time: Cisco Discovery Service provides a 4-hour service-level agreement (SLA), compared to a longer SLA for the full ANSR. This means a user can get the combined NAR quickly (sometimes within minutes).
- The ANSR is generated for Cisco's Service Contract Management (SCM) team to track customer assets deployed in the field. The internal ANSR for Cisco users will provide **all** contract data, whereas a partner will receive only data for contracts they "own." In these cases, a partner may want to work with their Cisco channel systems engineer (SE) or account manager (PAM) to address the service coverage gaps where they do not have visibility.
- Some partner or customer users may be accustomed to the full ANSR and want that level of detail in service coverage reporting.
- The ANSR is constantly evolving. By including the ANSR option, we ensure that users will not lose access to new features.
- The ANSR/Online feature offers the ability to generate a quote for uncovered devices, if desired by the customer. This works well when the decision is made to use the ANSR results to generate new contracts based on this now-validated installed base data.
- Before using the KTN portal, users must register. To get started, go to http://tools.cisco.com/ktn/.

Q. Is there a list of third-party vendors and devices that network assessment tools can report on?

A. Network assessment tool capabilities vary in this area. Most network assessment tools will discover devices from all vendors as long as they support SNMP. Check with the assessment tool vendor.

Q. When network assessment tools discover third-party equipment, what information is reported?

A. For third-party devices, there is no Cisco Discovery Service analysis or reporting on service coverage, PSIRT alerts, or field notices. Most network assessment tools will discover information based on generic MIBs, such as IP and MAC addresses, and system description. With Entity MIB supported equipment they will discover cards, ports, and similar entities.

Q. If a customer does not allow their data to be uploaded through Cisco Discovery Service to Cisco for analysis, what information will be omitted from reports?

A. If you do not submit discovery data to Cisco for analysis, you will not get PSIRT alerts, field notices, Cisco validated serial numbers, and service coverage (KTN) reports.

Q. Are Telnet/SSH credentials required for Cisco Discovery Service analysis?

A. Telnet enable passwords, for access to configurations, are highly recommended for accurate PSIRT and service coverage reporting. Without the CLI commands, this resulting data is far less accurate. For example, not all Possibly Vulnerable PSIRT alerts are reported, and service coverage is best effort only. End-of-life/end-of-sale data is also far more reliable with Telnet. You will get far better reporting with CLI data.

Q. Are Cisco configuration files stored in the discovery PC in clear text or encrypted files?

A. Network assessment tool capabilities vary in this area. Check with the assessment tool vendor.

Q. Why do we need Telnet/SSH? Why isn't SNMP enough?

A. The CLI data collected with Telnet/SSH is used in cases when SNMP alone does not provide sufficient data:

- CLI data improves product ID validation, which can improve end-of-sale/end-of-life data.
- Accurate PSIRT reporting requires CLI commands that return configuration information for the purpose of identifying the features enabled on each device. This results in fewer ambiguous Potentially Vulnerable PSIRT warnings and more Vulnerable warnings.

- KTN service coverage reporting requires specific CLI commands to validate the serial numbers that enable matching of the contracts. Without Telnet/SSH enabled, KTN fails to perform this processing.

Q. What are the specific CLI commands used, and what is their purpose?

A. The **show running-config** and **show config** commands are used primarily to enhance the PSIRT matching. If turned off in the Submit Network Assessment window, that data will not be sent to Cisco.

The following are the specific **show** commands currently used with Cisco Discovery Service and KTN:

Basic Cisco Discovery Service inventory:

- show version
- show diag

Enhanced PSIRT profiling:

- show config
- show running-config

KTN service contract validation:

- show hardware
- show inventory
- show c7200
- show gsr chassis-info
- show chassis eprom
- show inventory all
- show diag chassis
- show rsp chassis-info
- show module
- show IDPROM all

Q. What is the meaning of the Network Assessment Transaction status messages?

A. The following is a list of the transaction status messages and their meanings:

Cisco Discovery Service "Complete" Messages:

- COMPLETE: 100% of devices profiled, including KTN if selected, processed, and returned
- PARTIAL: Complete and ready to download, but with fewer than 100% of devices profiled, processed, and returned to Cisco Discovery Service
- CMPLKTNPND: Complete and ready to download, with 100% of devices profiled, but with KTN pending
- PRTLKTNPND: Complete and ready to download, but with fewer than 100% of devices profiled, and with KTN pending
- CMPLKTNERR: Complete and ready to download, with 100% of devices profiled, but with a KTN error, meaning KTN either had an error during processing or missed the window for inclusion in the Cisco Discovery Service report data
- PRTLKTNERR: Complete and ready to download, but with fewer than 100% of devices profiled, and KTN error (see above)

Other Messages:

- INCOMPLETE: Processing did not complete. This may be caused by a DesignXpert installation problem
- ERROR: Usually caused by a Cisco Discovery Service error. The XML file needs to be analyzed or data re-uploaded
- PROCESS: Transaction is still processing. Either it has not had enough time to process or there is a backlog

Q. Can Cisco Discovery Service profile all discovered devices?

A. No, however Cisco Discovery Service is continually being updated to add new discovery and profiling methods for unsupported device architectures and product lines. For example, Cisco Discovery Service 2.0 added support for Catalyst 3750 stacks, however profiling for Catalyst 6500 Virtual Switching System (VSS) is not yet supported. It is important to keep in mind that Cisco Discovery Service is a free service, and while we endeavor to continually make it better, there will always be limitations. In some cases, you may be better served by engaging with Cisco Advanced Services for more comprehensive assessment services and support.

Q. I can get end-of-life/end-of-sale, PSIRT and service coverage data directly from Cisco.com. Why should I use a Cisco Discovery Service enabled tool?

A. Cisco Discovery Service adds powerful capabilities to assessment tools, including superior analysis and guidance that will improve customer satisfaction and increase partner profitability. In addition, it provides automated, up-to-date, Cisco validated analytics based on the single source of truth (Cisco intellectual capital). Among the key deliverables:

- Product lifecycle milestones: Easily and accurately identify network devices that are nearing end of life or end of support. It is important to note that this does not merely refer to accurate end-of-life/end-of-support reporting that can be done manually using bulletins from Cisco.com. It also involves accurate product matching using a library of thousands of product rules. For example, you may have a device that was purchased as product ID 1234-01-A, but because components or features were modified, it is now actually product ID 1234-03-B, and the corresponding end-of-life/end-of-sale data is significantly different.
- PSIRT alerts: This is a significant differentiator, highly valued by customers and usually accessible only through fee-based services. Cisco has a large infrastructure in place to monitor and address security threats; PSIRTs can be extremely difficult to analyze for true vulnerability without the Cisco Discovery Service enhanced PSIRT capability (requires CLI collection).
- Cisco field notices: These have a value similar to PSIRT alerts.
- Service coverage: Quickly identify devices that are not covered by a service contract.
- Seamless integration with best-in-class third-party tools that bring additional value to partners and customers.
- Cisco recommended migration and replacement products for obsolete devices.
- Powerful and customizable reporting capabilities through Cisco Discovery Service enabled vendor tools.

These features offer tremendous value to customers, and are available at no additional charge to partners or Cisco Discovery Service tool vendors. Furthermore, there is a rich product roadmap for future enhancements that will be added to Cisco Discovery Service over time.

Q. Why do I sometimes see different serial numbers returned for the same device?

A. It is not uncommon to see variations in results when multiple processing methods are utilized. Serial number validation is particularly challenging because one device may have two or more serial numbers stored in different locations in the software and firmware. Cisco Discovery Service enabled network assessment tools obtain and validate serial numbers in a number of ways, including:

- The tool itself may provide a serial number mapping algorithm, irrespective of Cisco Discovery Service or KTN. It is possible to derive different serial numbers based on different SNMP MIBs being used.
- Cisco Discovery Service chooses the "best" serial number based on its product validation engine, rules, and a check against the Cisco manufacturing database.
- KTN serial number validation is based on a complex check against the manufacturing and contract databases, in which all serial numbers are compared and the "most likely" result is chosen.
- Cisco Discovery Service uses KTN serial number validation, if available, and replaces its validated serial numbers with KTN validated serial numbers. Note, however, that KTN is not always available.

The bottom line is that results may vary depending upon the tool or process used. In general, KTN validation is the most accurate, followed by Cisco Discovery Service and then the vendor tool.

Q. What network data do the different Cisco Discovery Service reports require?

A. Advanced reports (beyond basic inventory and end of sale/end of life) may require additional data beyond the SNMP. For example, even accurate product ID validation may require additional Telnet/CLI commands. PSIRT, medianet, IPv6, Cisco EnergyWise™, and Service Coverage reports all require more CLI data for processing. Table 1 lists the requirements for different reports.

Table 1. Commands Required for Cisco Discovery Service Reports

	SNMP	Share Device IP	Show Diag/Show Version	KTN Inventory Spec	Show Config/ Running Config
Raw Data Shared & with Cisco & Profiled >>	Common SNMP commands pull MIB, for basic PID validation	Upload device IP addresses to Cisco (aids in remediation)	Device show version and show diagnostics helps validate PID	Specific show commands required to validate serial numbers	Configs required for advanced reports, may also reveal IP addresses
Additional Details	http://www.cisco.com/public/sw-center/netmg-mt/cmtk/mibs.shtml and http://www.cisco.com/en/US/docs/ios/12_1/configfun/command/reference/frd3001.html	http://en.wikipedia.org/wiki/IP_address	http://www.cisco.com/en/US/docs/ios/12_1/configfun/command/reference/frd2001.html	http://www.cisco.com/en/US/docs/ios/12_1/configfun/command/reference/frd2001.html See next slide for specific commands	http://www.cisco.com/en/US/docs/ios/12_1/configfun/command/reference/frd2002.html#wp1019218
EoX	Required	Recommended	Recommended	Not Required	Not Required
Field Notice	Required	Recommended	Required	Not Required	Not Required
Security (PSIRT)	Required	Recommended	Required	Not Required	Required
Service Coverage	Required	Recommended	Recommended	Required	Not Required
IPv6 Profile	Required	Recommended	Required	Not Required	Recommended
Cost Optimization	Required	Not Required	Recommended	Not Required	Not Required
Medianet Profile	Required	Recommended	Required	Not Required	Required
EnergyWise Profile (2012)	Required	Recommended	Required	Not Required	Required
Security Profile (2012)	Required	Recommended	Required	Not Required	Required
TN 360° Report (2012)	Required	Recommended	Required	Not Required	Required

IPv6 Profile

Q. What data is used for IPv6 analysis?

A. The following attributes are collected for each device:

- Device Name
- Sys Object ID
- OS Version
- Image Name
- Flash Memory
- DRAM Memory
- Free DRAM
- CPU Usage
- For line cards:
  - Device Name
  - Product ID

Q. What causes a device to be classified as Further Analysis Required?

A. If a transaction either is processed with an error or is incomplete, the devices will be categorized as Further Analysis Required. Examples of such cases include:

- **Missing system object ID (OID)** in collection (discovery) data.
- **Missing product identification ID (PID)** in processed data; **this can also be caused by incomplete collection data.**
- **Unsupported product:** Missing back-end product rules for the product system object ID. New products are continuously being added to the Advanced Services IPv6 tool that powers the Cisco Discovery Service IPv6 Profile report. The tool currently supports most common Cisco IOS® Software routers and switches. In 2012 Cisco expects to add new platforms, including Cisco IOS-XR, IOS-XE, security appliances (ASA), and Cisco Nexus® devices, among others.
- **Unidentified modules** and software features: If data collection is not sufficient to identify all of a device's hardware modules and software features, it may also be classified as Further Analysis Required.

Q. How does the tool determine IPv6 capability?

A. A device is defined as being IPv6 capable if the device can understand and process IPv6 packets. The IPv6 capability of a device is determined using three pieces of information: the chassis type, Cisco IOS Software version, and feature set. These pieces of information are compared to reach a decision about whether or not a device is capable of supporting IPv6.

Q. What logic does the tool use to determine whether a device, platform, or software is or is not IPv6 capable?

A. Table 2 shows this logic. The steps that follow the table describe the logic flow.

Table 2. Logic Used to Determine IPv6 Capability

Detailed Report	OID model	FeaureSet	IOS	DRAM	Flash
Devices Currently IPv6 Capable	C	C	C	C	C
Devices Requiring IOS Only Upgrade	C	U or U		C	C
Devices Requiring IOS and FLASH Upgrade	C	U or U		C	U

Detailed Report	OID model	FeaureSet	IOS	DRAM	Flash
Devices Requiring IOS and DRAM Upgrade	C	U or U		U	C
Devices Requiring IOS, DRAM and FLASH Upgrade	C	U or U		U	U
Devices NOT Capable of Supporting IPv6	Anything as N				
Devices Requiring Further Analysis	Anything as FA.. Or any remaining case				

C= Capable of supporting IPv6
U= Requires upgrade

1. The flow begins with a check for devices that are known to require further analysis. (This first check is new in IPv6-RA 1.2). Any devices matched here are marked as FA (further analysis).
2. The next check is for devices known to be capable; matching devices are marked C (capable).
3. The next check is for devices known to require upgrade; matching devices are marked U (upgrade).
4. The next check is for devices known not to be capable; matching devices are marked N (not capable).
5. The final stage of the flow takes all the remaining devices and marks them FA (further analysis).

Note: Within each stage of the flow, the rules are applied in order of descending length of string. Thus, in the check for capable devices, for example, the rule *this is a verylongrulecheck* will be applied before the rule *shortrule.*

Q. How does a device end up in the “not capable” category?
A. A device ends up in the “not capable” category if it cannot process and understand IPv6 packets. This rule extends to devices that support service modules and line cards. If a service module or line card is not capable of processing IPv6 packets, the whole device is marked as “not capable.” The reasoning behind this decision is that the service module or line card is being used by the device for IPv4 packet forwarding and therefore cannot be used for IPv6 packet forwarding.

Q. What is the difference between “not capable” and “further analysis required”?
A. The “not capable” category refers to the platform itself (including the line cards and service modules in the chassis). The “further analysis required” category is generally triggered by the following issues:

- A selected feature is not supported on that platform.
- The feature is supported, but the device is running a version of code that does not include that feature.
- Data is missing.
- An internal rule on the tool has not been properly set up.

Medianet Profile

Q. What are the data collection requirements for a Medianet Assessment?
A. When a customer initiates a Medianet Assessment, the assessment is performed for all the devices existing in the Cisco Discovery Service database for the customer’s inventory. If any device is not yet discovered, it will not be assessed by the Medianet Readiness Advisor.

Discovery (collection) requirements are:

- Hardware
- Software
- Feature configurations: Features configured and enabled in each device (possibly via Facility Information System [FIS])

To discover these requirements, Cisco Discovery Service collects the data required for the assessment, using the standard Cisco Discovery Service inventory collection commands:

- SNMP
- CLI/Telnet, show running config

Q. What are the different medianet reports? What is the difference between the customer reports and the sales reports?

A. The Final Analysis and Download screen displays the Medianet Assessment reports. A final Medianet Readiness Advisor report will automatically be generated by applying migration, upgrade, and replacement rules to the Cisco Discovery Service data and questionnaire data with Feature Identification results.

The screen is divided into three tabs:

Customer Medianet Hardware Report: This report displays the number of devices selected by the user. The graph is grouped by product family; that is, there will be a separate bar for each product family selected by the user. The x-axis denotes the number of devices, and the y-axis denotes the product family.

- If there are any medianet recommendations, a blue bar is displayed.
- If there are no medianet recommendations (that is, if the device is already medianet capable), a green bar is displayed.

Customer Medianet Software Report: This report displays the Cisco IOS Software versions for the (HW) devices selected by the user in previous screens. This graph is grouped by Cisco IOS version; that is, there will be a separate bar for each version. The x-axis denotes the number of devices, and the y-axis denotes the Cisco IOS version.

- If there are any medianet recommendations, a blue bar is displayed.
- If there are no medianet recommendations (that is, if the Cisco IOS version is already medianet capable), a green bar is displayed.

Customer Medianet Features Report: This report displays the number of devices that match the focus area selected by the user. There will be a separate bar for each focus area. The x-axis denotes the number of devices, and the y-axis denotes the focus area.

- If there are any medianet recommendations, a blue bar is displayed.
- If there are no medianet recommendations (that is, if the feature is already medianet capable), a green bar is displayed.

Downloadable Reports

The Medianet Readiness Advisor report provides HW recommendations, OS recommendations, and feature recommendations.

- The customer report displays only the selected devices.
- The sales report displays all the devices.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C67-704184-00 03/12

