Cisco Discovery Service FAQ

1. What is Cisco Discovery Service (CDS)?
2. How do Partners access CDS with Netformx DesignXpert®?
3. How does the Navigate to Accelerate (N2A) program work?
4. What is the difference between DesignXpert, Enterprise AutoDiscovery (EAD) and Netformx Discovery (ND)?
5. How does DesignXpert integrate with CDS?
6. Does ND provide the same discovery analysis reports as the legacy DesignXpert EAD?
7. Will ND always be available at no cost to Cisco partners?
8. What is required by the Partner to make the connection to CDS?
9. Can you explain the Cisco.com Partner level access requirement in more detail?
10. Where can I see a demonstration and obtain training on the CDS process?
11. How do I get support if I have problems using CDS with DesignXpert?
12. What devices will be discovered by Netformx Discovery and what results will I see from this tool?
13. When I add CDS analysis to the DesignXpert results, what additional information will I receive?
14. Where can I see the results of the CDS Processing?
15. What happens to the customer data after CDS returns the results?
16. Can network discoveries be done remotely?
17. What is the maximum number of devices that can be discovered and analyzed?
18. How long does it take to process a transaction?
19. What information will the Partner get following a completed network assessment?
20. What enhancements were added with the 1.1 release of CDS?
21. What do you mean by enhanced PSIRT? Does it require any additional selection in Netformx Discovery Configurations?
22. What are Field Notices?
23. Can the Netformx Discovery discover Wireless Access Points and IP phones?
24. What can I do if a customer does not allow me to connect a non-company PC to their network for security reasons?
25. What information should customers provide for a successful discovery?
26. Is there a “Test/Lab” transaction for training or testing purposes, similar to the one in Cisco Discovery?
27. What market segments can I select for CDS Analysis?
28. Does ND provide the same Inventory Profile Report (IPR) as Cisco Discovery?
29. Will I be able to tell which SmartNet contracts have expired on my customer's devices?
30. Why do I not see detailed Service Coverage (or PSIRT) reporting for all my discovered Cisco devices?
31. I went to CSCC and registered my missing service contracts. Do I need to re-submit my discovery data to see the results?
32. Is SSH is an option in ND?
33. I understand that ND will discover IP Phones. Will this tool discover Cisco Call Managers and other Unified Communications servers as well?
34. Is there any way to define multiple enable passwords in ND?
35. Can I modify the collected IP addresses before uploading to Cisco in order to hide details about the customer networks?
36. Can you exclude certain items from the report, such as downloading Cisco config files?
37. Can I create discovery reports for non-Cisco equipment?
38. Is there a charge from Cisco for uploading a file to CDS?

40. Are Cisco IP phone serial numbers part of the information gathered for IP phones?
41. Can ND create a network map of the discovered devices?
42. Will ND hide the Telnet credentials?
43. Is the Network Assessment Information Transmission to Cisco encrypted?
44. How does ND collect the IP Phone serial number information?
45. Is DesignXpert tested in other language Operating Systems? Do their regional settings need to be set to English USA?
46. Does ND work in an MPLS environment?
47. 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 Know the Network (KTN) portal by following the embedded link in the NAR?
48. What is the reason for offering both the NAR and the ANSR as separate reports?
49. Is there a list of non-Cisco vendors and devices that ND can report on?
50. When ND discovers non-Cisco equipment, what information is reported?
51. If a customer does not allow their data to be uploaded through CDS to Cisco for analysis, what information will be omitted from the ND reports?
52. Are Telnet/SSH credentials required for CDS analysis?
53. Are Cisco config files stored in the discovery PC in clear text or encrypted files?
54. Why do we need Telnet/SSH? Why isn't SNMP enough?
55. What are the specific CLI commands used, and what is their purpose?
56. What is the meaning of the Network Assessment Transaction Status messages?
57. How do I obtain support for CDS related issues with Netformx Discovery? What is the escalation path?
58. Can CDS profile all discovered devices?
59. I can get EoX, PSIRT and Service Coverage data from Cisco.com. Why should I use a Cisco Discovery Service enabled tool?
60. Why do I sometimes see different serial numbers returned in different places for the same device?

Cisco Discovery Service FAQ

1. What is Cisco Discovery Service (CDS)?

CDS is a collection of web services that enables third-party network assessment tools to deliver detailed analysis and reporting on Cisco devices, including end-of-life milestones, security alerts, service coverage and product serial numbers. This information can be used to assess upgrade and service opportunities, and to identify Product Security Incident Response Team (PSIRT) advisories on existing equipment that could result in revenue opportunities from remediation. For more information, review the CDS At-A-Glance document.

2. How do Partners access CDS with Netformx DesignXpert®?

Netformx DesignXpert is the first CDS-enabled third-party tool, and is available free to partners for a limited time through the Cisco Partner Enablement program called Navigate to Accelerate (N2A). The N2A program provides Partners with access to the Netformx software to facilitate network discovery and CDS analysis of the Cisco devices discovered on the customer network. Partners may register to obtain DesignXpert through the N2A Program.

3. How does the Navigate to Accelerate (N2A) program work?

Upon submitting a request to Netformx, qualified Cisco Partners may receive a free 90 day evaluation license for full and unlimited use of *DesignXpert Silver Edition*, including Netformx Discovery. After 90 days, Partners may license DesignXpert directly from Netformx and continue using the full software suite. If the Partner elects not to purchase DesignXpert, his or her installation of DesignXpert automatically reverts to a standalone discovery tool called *Netformx Discovery (ND).* ND supports full enterprise auto discovery, but does not include pricing, advisors, ordering, and validation of devices or access to DesignXpert Favorites.

4. What is the difference between DesignXpert, Enterprise AutoDiscovery (EAD) and Netformx Discovery (ND)?

DesignXpert is an advanced, fully integrated software package that does everything from network discovery to design, configuration, validation and quoting, as well as generation of customizable bills-of-material (BoM) and statements of work (SOW).
EAD is the legacy network assessment and reporting module included in all versions of DesignXpert, and now enhanced with support for CDS.
ND is a standalone network discovery tool that includes full network assessment and reporting capabilities, but does not include the full capabilities of DesignXpert, such as configuration, validation, quoting, bill-of-materials, and statements of work.

5. How does DesignXpert integrate with CDS?

The DesignXpert user selects the option to submit the discovered data from his or her PC through the Internet to the secure CDS back-end. The receipt of the network information is acknowledged to the user and CDS begins to process the data using Cisco Advanced Services inventory profiling services. No other action is required by the user. The user and his or her PC are free to move to another task.

6. Does ND provide the same discovery analysis reports as the legacy DesignXpert EAD?

Yes, ND is designed to include the full discovery analysis reporting engine that supports the reporting of the enterprise assessment, with the addition of analysis and data from Cisco Discovery Service.

7. Will ND always be available at no cost to Cisco partners?

Cisco has teamed with Netformx to ensure a free version will be available through July 2011. It is possible the promotion will be extended, but we cannot commit to that. Note however, that the retail cost of Netformx Discovery is only $1000 per user, per year. Our hope is that partners would see this as a small investment compared with the tremendous returns they can gain through assessment led selling.

8. What is required by the Partner to make the connection to CDS?

Partners are required to have a Cisco.com account with Partner level access credentials. In addition, certain data fields must be entered properly for CDS to function properly.

9. Can you explain the Cisco.com Partner level access requirement in more detail?

The user must have a Cisco.com ID with Access Level 3; meaning it has to be associated with his or her 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 CDS access is not working, it may mean they are not associated with their Partner Company

and need 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.

10. Where can I see a demonstration and obtain training on the CDS process?

Please visit the Netformx Learning Center to access the complete DesignXpert Video on Demand (VOD) training series, including three brief Videos that focus on Netformx Discovery and CDS. You must first create a Logon ID and register to view these free videos.

11. How do I get support if I have problems using CDS with DesignXpert?

In addition to the training modules mentioned above, users can also open a support case by contacting Netformx Support.

12. What devices will be discovered by Netformx Discovery and what results will I see from this tool?

With SNMP and Telnet enabled in the network, ND will return data related to each IP device on the network. In the case of Cisco equipment, the data is quite extensive, based on the CDS analysis and the complete Netformx Knowledge Base of Cisco products as published weekly in the Cisco ERP system.

13. When I add CDS analysis to the DesignXpert results, what additional information will I receive?

CDS provides device inventory for core Cisco routing and switching devices, and many Advanced Technology devices, as well as device end-of-life (EoX) milestones, enhanced product security alerts (PSIRT), service coverage (KTN), field notices and validated Serial Number information. Most Cisco devices that support SNMP are supported by CDS, with the current exception of a few new high-end systems such as IOS-XR devices.

14. Where can I see the results of the CDS Processing?

The information processed by CDS is returned to the user's laptop and is available for reporting within DesignXpert. Report formats include Microsoft Word and Microsoft Excel. They feature full color and graphics that are easily customized by the user.

15. What happens to the customer data after CDS returns the results?

The data is retained by Cisco in a secure database. Netformx Discovery provides an option to purge the data after the transaction is completed.

16. Can network discoveries be done remotely?

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.

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

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, such as physical location and subnets. Larger device counts increase upload and download time, as well as processing time.

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

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. Future system enhancements are planned to improve processing time. Also, uploading and downloading of data can add to the overall time—usually very fast for a small network, but for larger networks in excess of 1,000 devices, it may take up to 30 minutes to upload or download using web service protocols.

NOTE (8.12.2010): *Currently CDS is frequently over capacity, frequently delaying processing by hours and in some cases days. In response to this, CDS will be migrating to a whole new infrastructure in August 2010, which should greatly enhance performance, accuracy and processing time.*

19. What information will the Partner get following a completed network assessment?

The immediate result will be the analysis provided by the Netformx tools, including a graphical representation of the network, network assessment reports such as Equipment Summary Report, analysis of EoX milestones, and other information that Netformx has in its Knowledge Base via ERP integration. Once processed with CDS, the level of detail increases.

20. What enhancements were added with the 1.1 release of CDS?

The 1.1 release of CDS enhances PSIRT reporting accuracy, improves serial number validation, adds Cisco Field Notices, and provides Service Contract reporting. The SmartNet service contract reporting is now included in the DesignXpert Network Assessment Report (NAR).

21. What do you mean by enhanced PSIRT? Does it require any additional selection in Netformx Discovery Configurations?

Enhanced PSIRTS (Feature based PSIRTS) are per the given configuration (running configuration). Enable passwords are required in the Netformx Discovery configurations.

- CDS 1.0 PSIRT Alerts were IOS based which is broader and may include PSIRT alerts that are not relevant (“Potentially Vulnerable”) in the current configuration.
- CDS 1.1 utilizes the Running Configuration data to match PSIRTs based on the features installed on the device. This extra validation means that there are more actionable (or “Vulnerable”) PSIRTS and fewer “Potentially Vulnerable”

22. What are Field Notices?

A field notices 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 can sometimes include fixes through a software upgrade. Unlike PSIRT alerts, devices usually have very few field notices if any.

23. Can the Netformx Discovery discover Wireless Access Points and IP phones?

Wireless Access Points (WAPs) (as slaves to a controller) and IP phones are not SNMP accessible and have to be inventoried using different means. Cisco IP phones are discovered by NND, and information from Netformx Library is retrieved for them. It will display the phone graphics, ports, and other catalog attributes. This information includes End of Life date, but does not necessarily include all EoX milestones. Most information arrives from Cisco ERP system. The slave Wireless Access Points (WAPs), like phones, are not supported in the CDS analysis at this time (nor are they supported in the legacy Cisco Discovery tool for the

same reason). We are currently working with the Cisco AS team to develop the best methodology for collection and reporting of these devices. The goal is to provide this functionality in a future release.

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

Please contact Netformx and request to receive a copy of Netformx Discovery which you can provide to your customer to facilitate their enterprise discovery. They will not have access to CDS and must transfer the data to the Cisco Partner for analysis. The list price for the 30 day use of ND by the Enterprise Customer is $150.

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

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

- IP ranges, Subnets, and/or 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 also need one of the following:

- SNMP Read-Write community string, TFTP access, username and password
- Telnet/SSH enable password (required to get enhanced PSIRT report)

26. Is there a "Test/Lab" transaction for training or testing purposes, similar to the one in Cisco Discovery?

Yes. To identify a Test/Lab transaction (recommended for non-Customer engagements), please choose "Test/Lab" in the Market Segment pull-down menu in the "Submit Network Assessment Request" screen.

27. What market segments can I select for CDS Analysis?

Market segments and vertical market selections are mapped to most standard Cisco Sales markets. Market segments include:

- Commercial
- Enterprise
- Managed Services
- Other
- Public Sector (for Government)
- Service Provider
- SMB (Small/Medium Business)
- Test/Lab for training and lab transactions

28. Does ND provide the same Inventory Profile Report (IPR) as Cisco Discovery?

Cisco and Netformx have worked to ensure ND reporting is on par with or better than the IPR. Early user feedback has been very positive in this area. DesignXpert also offers users the ability to easily customize reports.

29. Will I be able to tell which SmartNet contracts have expired on my customer's devices?

The Partner may need to do some work in advance to obtain complete service coverage data in their CDS reports. Specifically, the Partner must use the Cisco Service Contract Center (CSCC) tool to associate themselves with their customer contracts. Here are three important links that can help Partners through this process:

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

30. Why do I not see detailed Service Coverage (or PSIRT) reporting for all my discovered Cisco devices?

Default Operation: To protect partner proprietary information, Cisco has implemented procedures to ensure partners have visibility to information in the Service Coverage Report that pertains only to the contracts registered to their Cisco.com user ID. Service contract related 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 visibility to their service coverage data, partners should ensure all their contracts are properly registered to the appropriate Cisco.com user ID's within the partner company. More information about how to register contracts can be found on the Cisco Service Contract Center (CSCC) training website.

Troubleshooting Error-derived Empty Service Coverage Reports & KTN ANSR Report Generation: There are a few known issues that can result in either empty Service Coverage details in the NAR and/or failure of the ANSR report available from the KTN portal. The most common is incorrect Discovery Configuration in DesignXpert, in addition to other system issues.

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

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

   NOTE (8.12.2010) Issue Resolution./ Enhancement: Coming in October 2010 will be a new routine to avoid KTN Service Coverage being excluded from NAR data. With this enhancement, Service Coverage data will be added to the NAR data as soon as it finished processing, without regard for the CDS time window. In those cases—after the enhancement is introduced—the user 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 or PSIRT data cannot be processed due to incorrect Discovery Configuration (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 mis-configuration of the Telnet/SSH settings in the Discovery Configuration screen. Both KTN Service Coverage and accurate PSIRT mapping/reporting require specific CLI commands be issued, which requires that Telnet/SSH be enabled (in addition to checking the "Enable Cisco Discovery Services" checkbox). If this step is missed, KTN will not be able to validate serial numbers—and resulting

contract mapping, and you will likely get an empty Service Coverage tab in the NAR and a mostly empty KTN ANSR report, if the ANSR generates at all (it's possible that ANSR is not even generated)—or the user may receive a KTN Error in the Network Assessment Status screen. **To reiterate, without enabling Telnet/SSH in Discovery Configuration, 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 PSIRTs 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 Discovery Configuration should also be included for PSIRT reporting. Otherwise, the user may have to follow the trail of hundreds (and some cases thousands) of PSIRTs to manually determine which devices are vulnerable and which are not.

- **IMPORTANT TIP: How do I determine if the Discovery Configuration was properly set up for Telnet/SSH collection? I am missing my contract data, but there are apparently multiple reasons?** The first thing users usually notice are empty Service Coverage details, or in the ANSR report the majority if not all devices 'un-validated.' But that in itself doesn't tell you for sure. To double check this you need to check the PSIRT Details tab in the NAR (the PSIRT reporting must have been enabled in the upload screen). Go to the NAR PSIRT Details Excel tab and scan through the Vulnerability column results. If all, or nearly all PSIRTS are listed as Potentially Vulnerable and there are no or almost no reported as Vulnerable (and sometimes if you have an inordinate # of PSIRTs), then Telnet/SSH likely was not enabled and the collection must be re-run. ***The combination of missing contract data and all "Potentially Vulnerable" PSIRTs is a sure indicator of the CLI commands not being enabled.***

- **How do I enable Telnet/SSH in the Netformx Discovery so that I receive complete raw data to process services coverage and PSIRT alerts?** Open a discovery project (Project Menu → New → Discover Network → Blank Project → Provide "Project Name" → click Ok). On the Netformx Discovery window click on Configure button which will open Netformx Discovery Configuration Window. Select Telnet/SSH Tab, here you can check Telnet or SSH or both and provide username/password and enable password and add them into right pane. Please do not forget to check "Query Devices using Telnet/SSH.

31. I went to CSCC and registered my missing service contracts. Do I need to re-submit my discovery data to see the results?

If you previously submitted your discovery data (and all the device data was there), you can just click the existing Service Coverage Report URL in the Network Assessment Report (NAR) to go to the KTN portal and retrieve the full report (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 re-submit.

32. Is SSH is an option in ND?

Yes, you can use Telnet or SSH or both while working with Netformx Discovery.

33. I understand that ND will discover IP Phones. Will this tool discover Cisco Call Managers and other Unified Communications servers as well?

Not at this time; however this capability is part of the Netformx roadmap.

34. Is there any way to define multiple enable passwords in ND?

Yes, Under AutoDiscovery Configuration window, go to the Telnet Tab; here you can enter multiple enable passwords. To import a list of addresses and their specific Telnet/SSH credential, go to the Network Tab and click on the Excel icon under Include Subnets/Address options.

35. Can I modify the collected IP addresses before uploading to Cisco in order to hide details about the customer networks?

There is no need to modify collected IP addresses as they are automatically removed before submitting to Cisco for analysis. ND internally maps IP addresses to a locally generated device ID, which is sent to Cisco. After the analyzed data is returned to ND the device ID is then mapped back to the appropriate IP address in the DesignXpert project file.

36. Can you exclude certain items from the report, such as downloading Cisco config files?

Yes, by un-checking the "Download Cisco Configuration File" option under Cisco Specific Tab you will exclude it.

37. Can I create discovery reports for non-Cisco equipment?

Yes, ND will capture and allow you to create reports for non-Cisco network equipment. (With the Discovery Project open, go to Reports Menu → Auto Discovery → Equipment Summary).

38. Is there a charge from Cisco for uploading a file to CDS?

No.

39. How does ND actually discover devices?

ND uses Telnet, SSH and SNMP protocols to interrogate the network devices. Using public MIBs such as System MIB and entity MIB, ND collects information on the device and matches Netformx Knowledge Base to get additional device information and additional interrogation directions. Neighboring devices are currently being discovered using user inputs, routing tables, ARP cache tables, and CDP tables.

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

Yes. ND discovers the following information about Cisco IP Phone: Model Number, MAC Address, Serial Number, Host Name, Phoned, SysDesc & Subnet Mask.

41. Can ND create a network map of the discovered devices?

Yes, by default ND will create a topological map of discovered devices.

42. Will ND hide the Telnet credentials?

Yes, this feature is available in current version of ND.

43. Is the Network Assessment Information Transmission to Cisco encrypted?

Yes.

44. How does ND collect the IP Phone serial number information?

ND uses **http** to collect configuration information for IP Phones.

45. Is DesignXpert tested in other language Operating Systems? Do their regional settings need to be set to English USA?

Yes, DesignXpert is also tested in additional European languages, although the full test is performed for the English US edition only. Other languages are tested for specific features and general product validation.

46. Does ND work in an MPLS environment?

Yes. 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, the user will have to discover each site separately (using seed router) or by address ranges. With DesignXpert 12.0, users can assign multiple seeds, so MPLS discovery will become easier.

47. 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 Know the Network (KTN) portal by following the embedded link in the NAR?

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

The NAR provides a summary view of the full Actionable Network Snapshot Report (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 / Partner Company, and therefore Contract Number, Service Level, and Coverage Start/End 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:

- PID
- Location
- Chassis (parent) and/or Card (child)
- LDoS: CDS reports all lifecycle milestones, including:
    - EoX CCO Bulleting URL
    - LDoS Announcement Date
    - End of Sale
    - End of Engineering
    - End of Contract Renewal Date
    - End of SW Maintenance
    - LDoS

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

- Instance ID (specific to ANSR report)
- Parent Instance ID (specific to ANSR report)
- PCS
- Item Type (covered in CDS by chassis/card)
- Installed Site ID (this could be added in the future as we provide the data in CDS data stream)
- Installed at Customer
- Installed at Customer Address
- Contract Bill to Name
- Contract Bill to ID
- Part Confidence

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

There are a number of reasons, including:

- Many users will want just one report that includes Inventory, EoX, PSIRT, Field Notice, Validated Serial Number and Contract Data, without the more detailed service coverage reporting provided by the ANSR
- Time—CDS provides a 4-hour SLA, compared to full ANSR's longer SLA. This means a user can get the combined NAR report fast (sometimes within minutes)
- The ANSR report is generated for Cisco's Service Contract Management (SCM) team to track customer assets deployed in the field. The internal ANSR report for Cisco users will provide ALL contract data, whereas a partner will only receive data for contracts they "own". In these cases, a partner may want to work with their Cisco Channel SE or CAM to address the service coverage gaps where they do not have visibility
- Some partner or customers users may be accustomed to full ANSR and want that level of service coverage reporting detail
- ANSR reports are constantly evolving. By including the ANSR report option, 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 install base data
- Before using the KTN portal, users must register. To get started, go to http://tools.cisco.com/ktn/.

49. Is there a list of non-Cisco vendors and devices that ND can report on?

ND will discover devices of all vendors as long as they support SNMP.

50. When ND discovers non-Cisco equipment, what information is reported?

For non-Cisco devices, ND does not report on Service Coverage, PSIRTs or Field Notices. End-of-Life milestones are provided for some non-Cisco devices including Nortel (now Avaya) and Juniper. With most of the vendors, ND will discover information based on generic MIBs, such as IP and MAC addresses, and system description. With Entity MIB supported equipment it will discover cards, ports, etc. With Cisco and to some extent Nortel, Juniper, and HP (ProCurve), it will also discover internal device configuration, memory used, configuration files (Cisco device only) and some other data which is stored in the vendor private MIBs.

51. If a customer does not allow their data to be uploaded through CDS to Cisco for analysis, what information will be omitted from the ND reports?

By not submitting discovery data to Cisco for analysis, ND only provides End of Life milestones from its local Knowledge Base. You will not get PSIRTs, Field Notices, Cisco validated Serial Numbers and Service Coverage (KTN) reports.

52. Are Telnet/SSH credentials required for CDS analysis?

Telnet enable passwords, for access to configs, are highly recommended for accurate PSIRT and Service Coverage reporting. Without the CLI commands, this resulting data is far less accurate. For example, all "possibly vulnerable" PSIRTs are not reported, and Service Coverage is best effort only. EoX data is also far more reliable with telnet. You will get far better reporting with CLI data.

53. Are Cisco config files stored in the discovery PC in clear text or encrypted files?

Cisco config files found during discovery are stored locally in clear format.

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

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

- CLI data improves PID validation, which can improve EoX data
- Accurate PSIRT reporting requires CLI commands that return configuration information for the purpose of identifying features enabled on each device. This results in fewer ambiguous "Potentially Vulnerable" PSIRT warning, and more "Vulnerable" warnings
- KTN Service Coverage reporting requires specific CLI commands to validate the S/Ns that enable matching of the contracts. Without the Telnet/SSH enabled, KTN results in a failure to process

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

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 CDS & KTN:

Basic CDS 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

56. What is the meaning of the Network Assessment Transaction Status messages?

The following is a list of the Transaction Status messages and their meanings:

CDS "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 CDS
- 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 KTN error, meaning either KTN had an error processing, or it missed the window to include in the CDS 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

57. How do I obtain support for CDS related issues with Netformx Discovery? What is the escalation path?

To ensure you get the proper attention and resolution, please take the following steps:

Step 1. Open a support case with Netformx:

• Email support@netformx.com, or

• Visit http://support.netformx.com to open a case online or start a live chat session with an agent

• Normal support hours are 6am – 6pm Pacific, Mon – Fri.

Step 2. If more than 3 business days have elapsed and you feel you are not getting satisfactory response, and you wish to escalate:

• Assemble the following information and email to nfx-supportmgmt@netformx.com

1. Support case #
2. CDS transaction ID
3. Description of issue
4. Reason for escalation

Step 3. If after 3 additional business days you are still not satisfied and wish to escalate further:

• Assemble the above information and email to your Cisco AM or SE, asking that they forward this information to the Cisco internal mailing list cds-support (partners should not email this list directly)

58. Can CDS profile all discovered devices?

No. For example, CDS 1.4 cannot profile 3750 stacks. However, this is not really CDS issue, rather it is an issue that exists across all of Cisco Services. Some tools can discover 3750 stacks, but automated stack processing does not exist yet. Stack children don't have their own IP address, they communicate through the parent stack device (usually a 3750). Without the IP address there is no way to inventory them and pull data (you see a similar problem with clusters and some device architectures such as wireless LAN access points). CDS will be introducing new discovery methods and profiling engine later in 2011 that will support stacks and many other unsupported device architectures and product lines. Stacks are *currently not supported by any service*.

59. I can get EoX, PSIRT and Service Coverage data from Cisco.com. Why should I use a Cisco Discovery Service enabled tool?

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, CDS 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 EoX 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 EoX data is significantly different.
- Product Security Incident Response Team (PSIRT) alerts – this is a significant differentiator, highly valued by customers, and usually only accessible 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 CDS enhanced PSIRT capability (requires CLI collection)
- Cisco Field Notices – similar value to PSIRT alerts
- Service coverage – quickly identify devices that are not covered by a service contract
- Seamless integration with best of breed third party tools that bring additional value to partners and customers
- Cisco recommended migration/replacement products for obsolete devices
- Powerful and customizable reporting capabilities through CDS-enabled vendor tools

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

60. Why do I sometimes see different serial numbers returned in different places for the same device?

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. When using a CDS-enabled network assessment tool, serial numbers are obtained and validated in a number of ways, including:

- The tool itself may provide a serial number mapping algorithm, irrespective of CDS or KTN. It is possible to derive different serial numbers based on different SNMP MIBs being utilized
- CDS 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
- CDS 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 CDS and then the vendor tool.