

## Cisco Discovery Service FAQ

1. What is Cisco Discovery Service (CDS)?
2. How do Partners access CDS?
3. How do neteXpose DNA integrate with CDS?
4. What is required by the partner to make the connection to CDS?
5. Can you explain the Cisco.com Partner level access requirement in more detail?
6. Where can I see a demonstration and obtain training on the CDS process?
7. How do I get support if I have problems using CDS?
8. What devices will be discovered and what results will I see from a CDS-enabled tool?
9. Where can I see the results of the CDS processing?
10. Where can I see the results of the neteXpose Knowledge Base Server processing?
11. What happens to the customer data after CDS returns the results?
12. What happens to the customer data when using the neteXpose Knowledge Base Server?
13. Can network discoveries be done remotely?
14. What is the maximum number of devices that can be discovered and analyzed?
15. How long does it take to process a transaction?
16. What is the enhanced PSIRT feature that was added in CDS 1.1? Does it require any additional configuration?
17. What are Field Notices?
18. Can CDS-enabled tools discover Wireless Access Points and IP phones?
19. What can I do if a customer does not allow me to connect a non-company PC to their network for security reasons?
20. What information should customers provide for a successful discovery?
21. Is there a "Test/Lab" transaction for training or testing purposes?
22. What market segments can I select for CDS analysis?
23. Will I be able to tell which SmartNet contracts have expired on my customer's devices?
24. Why do I not see detailed Service Coverage (or PSIRT) reporting for all my discovered Cisco devices?
25. I went to CSCC and registered my missing service contracts. Do I need to re-submit my discovery data to see the results?
26. Is SSH is an option rather than Telnet?
27. Will network assessment tools discover Cisco Call Managers and other Unified Communications servers?
28. Is there any way to define multiple enable passwords?

29. Can I modify the collected IP addresses before uploading to Cisco in order to hide details about the customer networks?
30. Can I create discovery reports for non-Cisco equipment?
31. Is there a charge from Cisco for uploading a file to CDS?
33. Are Cisco IP phone serial numbers part of the information gathered for IP phones?
34. Will neteXpose DNA create network maps of the discovered devices?
35. Is the Network Assessment Information Transmission to Cisco encrypted?
36. Does neteXpose DNA work in an MPLS environment?
37. 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?
38. What is the reason for offering both the NAR and the ANSR as separate reports?
39. Is there a list of non-Cisco vendors and devices that neteXpose DNA can report on?
40. Which information neteXpose delivers on non-Cisco equipment, what information is reported?
41. If a customer does not allow their data to be uploaded through CDS to Cisco for analysis, what information will be omitted from reports?
42. Are Telnet/SSH credentials required for CDS analysis?
43. Are Cisco config files stored in the discovery PC in clear text or encrypted files?
44. Why do we need Telnet/SSH? Why isn't SNMP enough?
45. What are the specific CLI commands used, and what is their purpose?
46. What is the meaning of the Network Assessment Transaction Status messages?

### **Cisco Discovery Service FAQ**

#### **1. What is Cisco Discovery Service (CDS)?**

CDS is an advanced web service that enables network assessment tools to deliver detailed analysis and reporting on Cisco devices, including end-of-life milestones, security alerts, field notices and service coverage reports. This information can be used to assess upgrade and service opportunities, and to identify hardware, software & security vulnerabilities on existing equipment that could result in revenue opportunities from remediation. For more information, refer to the [Cisco Discovery Service Website](#).

## **2. How do Partners access CDS?**

CDS is a SOP API interface from Cisco to enable third-party discovery tools to correlate Cisco device information with the Cisco End-of-Life, KTN, and Security Knowledge base. A level 3 Cisco Partner login is required to upload device information so it can be correlated with the Cisco Knowledge Base.

## **3. How do neteXpose DNA integrate with CDS?**

The 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.

## **4. 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.

## **5. 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](#).

## **6. Where can I see a demonstration and obtain training on the CDS process?**

All general information you will find on [netexpose.com](http://netexpose.com). Registered Partners will have access to the neteXpose Partner web including product information and training material. neteXpose offers onsite training, software installation assistance and discovery analysis support. For more information please contact [sales@netexpose.com](mailto:sales@netexpose.com).

## **7. How do I get support if I have problems using CDS?**

Cisco Partners using neteXpose DNA can open a support case by contacting neteXpose Support Team via email <mailto:support@netexpose.com> or phone: +33 4 93 00 1274.

### **8. What devices will be discovered and what results will I see from a CDS-enabled tool?**

neteXpose DNA discovers IP network devices and end-stations from Cisco and other manufacturers. Discovered data include asset and configuration on hardware and operating system software, applications and services, as well as topology information on layer 2 and layer 3. The result is presented in automatically created inventory reports and network maps. After the discovery, external information such as product lifecycle and security information is added to the discovery data by using either the Cisco Discovery Services (CDS) API or the neteXpose Knowledge Base Server. In the case of Cisco equipment, the resulting CDS API analysis is quite extensive. 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. When using the neteXpose Knowledge Base Server the user receives product lifecycle information and security CVE information on Cisco and other DNA-supported network manufacturers.

### **9. 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 from within the network assessment tool application. Report formats include Microsoft Word and Microsoft Excel. They feature full color and graphics that are easily customized by the user. Visit the [Cisco Discovery Service Website](#) to see sample reports.

### **10. Where can I see the results of the neteXpose Knowledge Base Server processing?**

The neteXpose Knowledge Base Server provides data from external sources, such as manufacturers and private and public organizations. These data can be downloaded to the DNA PC's memory at any time, and are correlated with the discovery data shortly after the discovery has been finished. The result is presented in EOX reports on Cisco and other selected network manufacturers, as well as in EOX network maps. Report formats include Microsoft Word and Microsoft Excel. The user can also place its own Microsoft Office Word templates in the neteXpose DNA software to document the discovery results. The EOX maps display the devices of different network manufacturers which are EOX at any selected date. The maps are supplied in DNA, JPEG and Microsoft Office Visio format.

### **11. What happens to the customer data after CDS returns the results?**

The data is retained by Cisco in a secure database. The neteXpose DNA network assessment tool provides an option to purge the data after the transaction is completed.

### **12. What happens to the customer data when using the neteXpose Knowledge Base Server?**

Network discovery data and EOX data are stored only on the DNA station and can be deleted at any time.

### **13. Can network discoveries be done remotely?**

It is possible to perform a network discovery remotely using VPN. neteXpose DNA can be used in a multi-tenant security service environment . In this case the DNA software is installed on the central server, the discovery data is transmitted using VPN, and the data is stored to the customer-related secure database. It is up to the customer to agree with the partner how the discovery is performed.

### **14. 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.

### **15. 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.

### **16. What is the enhanced PSIRT feature that was added in CDS 1.1? Does it require any additional configuration?**

Enhanced PSIRTS (feature based PSIRTS) are based on the running configuration. Telnet enable passwords are required in the network assessment tool.

- 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”

### **17. 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.

### **18. Can CDS-enabled tools 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. While they may be discovered, they are not supported in the CDS analysis at this time (nor were 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.

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

neteXpose offers special licenses to install the DNA software on a customer's PC. The discovery and product lifecycle reports can be produced on the customer's DNA station, and the IBLM-related reports are then sent to Cisco by the Cisco Partner in accordance with the customer (neteXpose Knowledge Base Server Approach). Or the partner can initiate the Cisco CDS transfer from the customer's DNA PC. For more information please contact: [sales@netexpose.com](mailto:sales@netexpose.com).

### **20. 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

If you wish to retrieve Cisco configuration files or more detailed information on certain products you will also need one of the following:

- Telnet/SSH enable password (required to get enhanced PSIRT report).

### **21. Is there a "Test/Lab" transaction for training or testing purposes?**

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.

### **22. 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

### **23. 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](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](http://www.cisco.com/web/SCM/KTNx/html/CSCC_Contract_Management_Summary_Job_Aid.pdf)
- **CSCC:** <http://www.cisco.com/web/partners/services/resources/csc/index.html>

### **24. 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 Network Assessment Report (NAR) and/or failure of the ANSR report available from the KTN portal.

**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:** Available now in the CDS 1.4 release, there is 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 network assessment tool so that I receive complete raw data to process services coverage and PSIRT alerts?** Network assessment tool capabilities vary in this area. Check with the assessment tool vendor.

**25. 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.

**26. Is SSH is an option rather than Telnet?**

Yes, you can use Telnet or SSH or both.

**27. Will network assessment tools discover Cisco Call Managers and other Unified Communications servers?**

neteXpose DNA is capable of discovering Server and PC software through either the SNMP or WMI (Windows Management Information) protocol. A comprehensive list of software including any Cisco software is presented. In addition neteXpose DNA can provide EOX information on Cisco Call Manger and other Cisco software e.g. Cisco VPN Client to determine the latest versions.

**28. Is there any way to define multiple enable passwords?**

neteXpose DNA can run multiple enabled passwords by using it sequentially. If none of this is working, DNA provides a setup option to enable well-known communities (vendor's default password). In this case you will receive information on devices which use still the default password.

**29. 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. 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 tool the device ID is then mapped back to the appropriate IP address. neteXpose DNA offers the option to view the XML data before they get sent by opening the file with a XML browser.

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

Yes. neteXpose DNA is a vendor-independent discovery tool offering inventory reports on network devices and end-stations, as well as EOX reports on Cisco and selected other network equipment manufacturers. The report information depth relies on the information every single vendor supplies.

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

No.

**32. How does neteXpose DNA actually inventory devices?**

neteXpose DNA uses SNMP, SSH and WMI protocols to discover and interrogate network devices and end-stations. Using public MIBs such as System MIB and Entity MIB, it collects information on the devices. Neighboring devices are discovered using user inputs, routing tables, ARP cache tables, and CDP tables.

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

NeteXpose DNA uses the CDP protocol and MAC address information to find Cisco IP phones. The next version will use the HTTP interface on the phone to discover IP phones not connected to Cisco equipment.

**34. Will neteXpose DNA create network maps of the discovered devices?**

neteXpose automatically creates pre-defined network and EOX maps on different network layers. The network maps include network devices and end-stations of all discovered vendors. The EOX maps highlight network devices of different manufacturers which are EOX at any selected date. In addition to the pre-defined network maps, the user can create his own maps using the integrated full-featured DNA graph and layout application including device library and the option to integrate vendor or customer-specific icons.

**35. Is the Network Assessment Information Transmission to Cisco encrypted?**

Yes.

**36. Does neteXpose DNA work in an MPLS environment?**

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. Like all

network management activities the discovery of devices must be done from the point of view that the discovery station needs access to SNMP and SSH on all infrastructure devices. This must be established before a discovery is started.

**37. 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

### **38. 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/>.

### **39. Is there a list of non-Cisco vendors and devices that neteXpose DNA can report on?**

neteXpose DNA will discover and report on IP devices of all vendors as long as they support SNMP.

#### **40. Which information neteXpose delivers on non-Cisco equipment, what information is reported?**

For non-Cisco devices, there is no CDS analysis or reporting on Service Coverage, PSIRTs or Field Notices. End-of-Life data is provided for selected non-Cisco devices, e.g. from Avaya / Nortel, Brocade/Foundry; Extreme Networks, Hewlett Packard (HP), Juniper. neteXpose DNA will also discover information based on generic MIBs, such as IP and MAC addresses, and system description. It also retrieves data from the vendor's private MIBs. In addition neteXpose DNA reports on Windows Management Information (WMI) devices and NetBIOS devices. The following information can be supplied:

- SNMP devices: host name, IP address, vendor, type, model, serial number, number of slots, chassis, cards and modules, software and firmware
- WMI devices: name, IP address, vendor, model, serial number, OS, user, CPU, memory, disk, installed software, hot fixes and patches, services
- NetBIOS devices: name, IP address, type, model, manufacturer, description
- Link and topology data: link type, data rate, mode, link endpoint device data, VLAN and subnet addresses including members

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

By not submitting discovery data to Cisco for analysis, you will not get PSIRTs, Field Notices, Cisco validated Serial Numbers and Service Coverage (KTN) reports.

#### **42. Are Telnet/SSH credentials required for CDS analysis?**

SSH/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 SSH/telnet. You will get far better reporting with CLI data.

#### **43. Are Cisco config files stored in the discovery PC in clear text or encrypted files?**

Cisco configuration files are stored encrypted in the database but in clear text through the neteXpose interface and in the XML upload file in the DNA CDS interface.

#### **44. 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

#### **45. 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

#### 46. 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.
- ERROR: Usually caused by a CDS 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 that here is a backlog