Network Documentation Checklist

Don Krause, Creator of NetworkDNA

NetworkDNA

This list has been created to provide the most elaborate overview of elements in a network that should be documented. Network Documentation is a BIG job with **BIG** rewards. Network administrators who utilize network documentation as a "living document" or "living process" reap the greatest of those rewards. Also, service providers can leverage this detailed of a binder as their project deliverable to rise above the competition.

It is advised that you step back and review this entire document before jumping in. This approach breaks common document grouping practices as it leverages the perspective of the entire network. There are concepts of NetworkDNA not explained that are valuable to a complete documentation strategy.

Non-Network Information

There are several items that have nothing to do with your network that are important to keep track

- € Overview of all location your organization consists of.
  - o Addresses, driving directions, pictures, contact name and phone number(s).
- € List of all major contractors who work on your network
- € List of all major vendors you purchase equipment from
  - o Identify who can authorize purchases, Organization purchase protocol
- € Resource (online) account management list
  - o Track all the URL, usernames and passwords for the web resources you utilize.
- € Network Documentation overview – Help the person looking for information find it fast!
  - o Outline the framework you are utilizing
  - o Hints to help find information fast
- € Network Purpose Statement
  - o Identify why the organization has a network and what its primary functions and responsibilities are. This may also include what the network is NOT.

Network Globals

These are the elements of the network that expand beyond being just hardware or software. NetworkDNA separates environments from hardware and software. We have found it to be more efficient to identify our resources as assets in sections 3 – 6. We then reference those assets within environments that encompass those assets. This section comes before the assets because it is accessed more often post completion.

- € ANTI Environments – What is protected (computers / servers), how is it configured, what is NOT protected, how are different components related – does one update from another, how is it managed – per device or centrally? Is this a hardware device? Configuration information for applications or device.

  - o Anti-Virus
  - o Anti-Spyware
  - o Anti-Spam

- € BACKUP Environment – What software is used, What hardware is used, How is it configured, what backup scheme (tape rotation) is being used, what is taken off site, is it encrypted, is it password protected, what is the password (also kept in the administrative section), When were tapes purchased, when was cleaning tape purchased, how often is the hardware cleaned, who swaps tapes daily, who takes the backup offsite, What revision is the backup software, Does the server backup an workstations,

  - o Workstation Based – elaborate specifically on workstations that have their own backup

solution

- o Server Based – elaborate each servers backup strategy

€ BUSINESS CONTINUITY – The plan to keep end users productive in the event of failure. This may take other network global environments and put them together to demonstrate how they help one another. For example the Power protection section may outline UPS for every user which helps ensure productivity in the event of minor power failures. The Backup plan may include 2 backups, a differential to NAS device and a full backup to tape – allowing very fast restore of yesterday's files. This section should have as many "What if…." Or "In the event…." Statements you can think of to ensure the purpose of the network can be fulfilled.

€ CELLULAR Environment – If the IT department is also responsible for the cellular phones, it makes sense to group them with the other hardware for asset management. This section allow elaboration as to the service plans in use and who has cell phones and why. What the purpose of each phone is and how it fills a business need.

€ DHCP – Identify what the dhcp server is OR state that there is none. If there is more than one or if bootp is being used on the network. Identify lease times, dhcp pool, global settings used. If the imaging section explains PXE, elaborate on the dhcp strings and supporting services needed to maintain the whole environment.

€ DIGITAL IMAGERY – A place to identify the total number of digital still cameras and digital video recorders. Who holds them, where they are mounted in the facility, who controls them, who can access the video footage for security purposes. For still cameras outline where pictures should be stored to help prevent losses in disk space on servers.

€ DISASTER RECOVERY – The outline of what will be done when hardware fails or nature disaster strikes.

€ DIRECTORY SERVICES – This is the central directory for the organization, how it synchronizes itself, what maintenance it performs, who has rights to add, delete from it.

€ DNS – Identify what the local dns server is OR state that there is none. If there is more than one, what the upstream dns servers are, if they hold live dns records or only local.

€ DOCUMENT HANDLING – Elaborate on the purpose and how it works. Who has access to it. What does it include – scanned in items (resumes), email, files on the network, workflow.

€ FILE SYSTEM Structure – Identify what drive mappings will exist and there purpose. What groups have access to what area / server(s). Include

€ HAND HELD Computing – Who has them, For what purpose, how is synchronization configured, are passwords required to prevent identity theft, Are collaboration capabilities available,

€ IMAGING – What application (Novell Zenworks, Ghost, etc) Where are images stored, is PXE used, how are images taken, how are images restored, who can restore images, automation capabilities,

€ INTERNET – Who is the ISP, is there a backup ISP, What is the IP config – dhcp or static, how many static addresses (also documented in the protocol section), What technology is used: T1, DSL, cable, FTTP, dial up. If PPOE what is username and password, What is the support phone number, what is the circuit ID, What domain name are registered, who is the registrar, who is the live DNS (authoritive) hosting service provider, What domain name prefixes are used and what IP address do they reference, What DNS records exist – A, Mx, etc

€ MAIL – Is email stored in-house or outsourced, who provides outsourced services, who has a mailbox, how much does it cost, What server houses the in-house mail application, what is the mail application, what is the naming standard used for email addresses, who has an email address, what is corporate policy on what email can be used for – personal mail??? Can mail be checked from outside the office, what is available POP3 / IMAP,

€ MANAGEMENT – What application is used (Zenworks, SMS, etc), What helpdesk application is used, who can do what within the app, What client needs to be loaded onto managed PC's

€ PHONE SYSTEM – What hardware is used for call processing, What Phones are used, What type of line is used (T1, etc), What phones are used, Who has a phone, What extension does each user have, Are there Auto Attendants, What is the voice mail configuration, Backup process (should also be linked or documented under BACKUP)

€ POWER PROTECTION – Identify how power is isolated or UPSed for computer network, Does each PC have a UPS, Does each server have a UPS, Is the UPS monitoring software used, how is it configured, How long will the UPS(es) keep devices up if power is lost, Is there a backup generator, Is there a maintenance schedule for UPSes,

€ PRINTING – What printers are there, who can print to them, what are their responsibilities (color, billing, letter head, 11X17, ect.) Are local printers shared, who supplies printer cartridges, what is done with old cartridges, who services the printers, what printers are backups to other high priority printers, how are printers installed onto workstations, who can install printers onto workstations,

€ PROTOCOL – What protocols are running on the network, What addresses (network numbers) are assigned to each, For IP networks – what is the subnet, gateway, dns servers, what static addresses are assigned,

€ REMOTE – What technology is used to remote control workstations or servers, are KVM's used on servers, who can remote control workstations, what client needs to be installed onto workstations, what passwords are used

€ SECURITY – physical access to the infrastructure equipment and servers, password policy, backup encryption settings, who is authorized to access the NOC (server room), Is the default administrative username changed to something else on workstations / servers, Are all data jacks activated or only those with workstations connected, Are users required to lock their desktops when leaving their desk,

€ WAN – what locations are connected, how are locations connected together, what can be accessed from one location to another,

€ WIRELESS – Is wireless authorized in your organization, Is wireless used for point to point connection, Is wireless used for Wi-Fi within a location, if multiple access points exist in the same location how are they configured – map or diagram, what security is setup on the access points, who is authorized to connect to the wireless network, is the wireless network direct on the LAN or on the DMZ, Is wireless available for free to visitors to your organization,

Infrastructure

The hardware that "makes the network"
- € Data cabling
- € Switch / Hub gear
- € Routers
- € Firewalls
- € Patch cable management
- € Wireless access point(s)
- € Antennas

Devices

The hardware that connects to the network.
- € Servers
- € Workstation
- € Print Servers
- € Printers / Copiers
- € Hand Held(s)
- € PLC(s)
- € IP Camera's
- € IP Phones

Peripherals

The hardware that does NOT connect to the network.
- € Local Printers
- € USB Hubs
- € Keyboards
- € Mice
- € Monitors / Displays
- € Hand Helds
- € Removable storage devices
- € Digital Camera(s)
- € Docking Station(s)
- € Cell Phones

Software

- € Operating Systems
- € Productivity Applications
- € Support Applications
- € Device drivers
- € Services
- € Engines

Administrative

Information that makes the large amount of computer equipment a valuable networked system

- € Users
- € Passwords
- € Groups
- € Login Scripts
- € Licenses
- € Policies

Diagrams

The graphical representation of your network

- € Geographic outline of all organization locations / WAN diagram
- € Floor plan for each location
- € Data jack map
- € LAN diagram
- € Infrastructure map

This list is organized based on the NetworkDNA framework, for more information on the open source project dedicated to bringing to life an industry standard in network documentation please visit http://www.networkdna.org. Or to subscribe to the creators blog at ITToolbox, visit http://blogs.ittoolbox.com/networking/documentation