Network Documentation

13.1.1

Documentation Overview

As with any complex activity like network troubleshooting, you will need to start with good documentation. Accurate and complete network documentation is required to effectively monitor and troubleshoot networks.

Common network documentation includes the following:

- Physical and logical network topology diagrams
- Network device documentation that records all pertinent device information
- Network performance baseline documentation

All network documentation should be kept in a single location, either as hard copy or on the network on a protected server. Backup documentation should be maintained and kept in a separate location.

13.1.2

Network Topology Diagrams

Network topology diagrams keep track of the location, function, and status of devices on the network. There are two types of network topology diagrams: the physical topology and the logical topology.

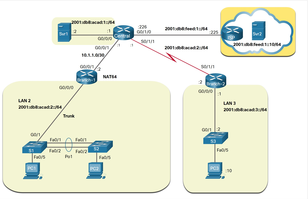
Click each button for an example and explanation of physical and logical topologies.

Physical Topology | Logical IPv4 Topology | Logical IPv6 Topology

Logical IPv6 Topology

Although IPv6 addresses could also be displayed in the same IPv4 logical topology, for the sake of clarity, we have created a separate logical IPv6 network topology.

The figure displays a sample IPv6 logical topology.



13.1.3

Network Device Documentation

Network device documentation should contain accurate, up-to-date records of the network hardware and software. Documentation should include all pertinent information about the network devices.

Many organizations create documents with tables or spreadsheets to capture relevant device information.

Click each button for examples of router, switch, and end device documentation.

Router Device Documentation | LAN Switch Device Documentation | End-system Documentation Files

Router Device Documentation

The table displays sample network device documentation for two interconnecting routers.

Device	Model	Description	Location	IOS	License
Central	ISR 4321	Central Edge Router	Building A Rm. 137	Cisco IOS XE Software, Version 16.09.04 flash:isr4300-universalk9_ias.16.09.04.SPA.bin	uiseven-security,k9
Interface	**Description**	**IPv4 Address**	**IPv6 Address**	**MAC Address**	**Routing**
G0/0/0	Connects to Net1 -	10.0.0.1/26	2001:db8:acad:1::1/64	a034.98e1.a180	OSPF
G0/0/1	Connects to Branch-1	10.1.1.1/30	2001:db8:acad:a001::1/64	a034.98e1.a181	OSPFv3
G0/1/0	Connects to ISP	209.165.200.226/30	2001:db8:feed:1::2/64	a034.98c3.a132	Default
S0/1/1	Connects to Branch-2	10.1.1.2/24	2001:db8:acad:2::1/64	n/a	OSPFv3
Device	**Model**	**Description**	**Site**	**IOS**	**License**
Branch-1	ISR 4221	Branch 2 Edge Router	Building B Rm. 102	Cisco IOS XE Software, Version 16.09.04 flash:isr4200-universalk9.16.09.04.SPA.bin	uiseven-security,k9
Interface	**Description**	**IPv4 Address**	**IPv6 Address**	**MAC Address**	**Routing**
G0/0/0	Connects to S1	Router-on-a-stick	Router-on-a-stick	a034.98e1.9d90	OSPF
G0/0/1	Connects to Central	10.1.1.2/30	2001:db8:acad:a001::2/64	a034.98e1.9d91	OSPF

13.1.4

Establish a Network Baseline

The purpose of network monitoring is to watch network performance in comparison to a predetermined baseline. A baseline is used to establish normal network or system performance to determine the "personality" of a network under normal conditions.

Establishing a network performance baseline requires collecting performance data from the ports and devices that are essential to network operation.

A network baseline should answer the following questions:

- How does the network perform during a normal or average day?
- Where are the most errors occurring?
- What part of the network is most heavily used?
- What part of the network is least used?
- Which devices should be monitored and what alert thresholds should be set?
- Can the network meet the identified policies?

Measuring the initial performance and availability of critical network devices and links allows a network administrator to determine the difference between abnormal behavior and proper network performance, as the network grows, or traffic patterns change. The baseline also provides insight into whether the current network design can meet business requirements. Without a baseline, no standard exists to measure the optimum nature of network traffic and congestion levels.

Analysis after an initial baseline also tends to reveal hidden problems. The collected data shows the true nature of congestion or potential congestion in a network. It may also reveal areas in the network that are underutilized, and quite often can lead to network redesign efforts, based on quality and capacity observations.

The initial network performance baseline sets the stage for measuring the effects of network changes and subsequent troubleshooting efforts. Therefore, it is important to plan for it carefully.

13.1.5

Step 1 – Determine What Types of Data to Collect

When conducting the initial baseline, start by selecting a few variables that represent the defined policies. If too many data points are selected, the amount of data can be overwhelming, making analysis of the collected data difficult. Start out simply and fine-tune along the way. Some good starting variables are interface utilization and CPU utilization.

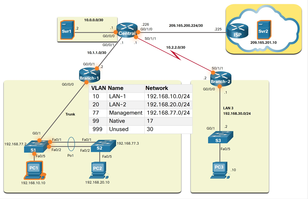
13.1.6

Step 2 – Identify Devices and Ports of Interest

Use the network topology to identify those devices and ports for which performance data should be measured. Devices and ports of interest include the following:

- Network device ports that connect to other network devices
- Servers
- Key users
- Anything else considered critical to operations

A logical network topology can be useful in identifying key devices and ports to monitor. In the figure, the network administrator has highlighted the devices and ports of interest to monitor during the baseline test.



VLAN Name	Network
10 LAN-1	192.168.10.0/24
20 LAN-2	192.168.20.0/24
77 Management	192.168.77.0/24
99 Native	17
999 Unused	30

The devices of interest include PC1 (the Admin terminal), and the two servers (i.e., Svr1 and Svr2). The ports of interest typically include router interfaces and key ports on switches.

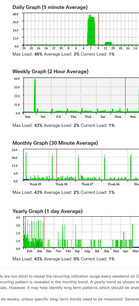
By shortening the list of ports that are polled, the results are concise, and the network management load is minimized. Remember that an interface on a router or switch can be a virtual interface, such as a switch virtual interface (SVI).

13.1.7

Step 3 – Determine the Baseline Duration

The length of time and the baseline information being gathered must be long enough to determine a "normal" picture of the network. It is important that daily trends of network traffic are monitored. It is also important to monitor for trends that occur over a longer period, such as weekly or monthly. For this reason, when capturing data for analysis, the period specified should be, at a minimum, seven days long.

The figure displays examples of several screenshots of CPU utilization trends captured over a daily, weekly, monthly, and yearly period.



In this example, notice that the work week trends are too short to reveal the recurring utilization surge every weekend on Saturday evening, when a database backup operation consumes network bandwidth. This recurring pattern is revealed in the monthly trend. A yearly trend as shown in the example may be too long of a duration to provide meaningful baseline performance details. However, it may help identify long term patterns which should be analyzed further.

Typically, a baseline needs to last no more than six weeks, unless specific long-term trends need to be measured. Generally, a two- to four-week baseline is adequate.

Baseline measurements should not be performed during times of unique traffic patterns, because the data would provide an inaccurate picture of normal network operations. Conduct an annual analysis of the entire network, or baseline different sections of the network on a rotating basis. Analysis must be conducted regularly to understand how the network is affected by growth and other changes.

13.1.8

Data Measurement

When documenting the network, it is often necessary to gather information directly from routers and switches. Obvious useful network documentation commands include **ping**, **traceroute**, and **telnet**, as well as **show** commands.

The table lists some of the most common Cisco IOS commands used for data collection.

Command	Description
show version	Displays uptime, version information for device software and hardware.
show ip interface [brief] **show ipv6 interface [brief]**	• Displays all the configuration options that are set on an interface. • Use the **brief** keyword to only display up/down status of IP interfaces and the IP address of each interface.
show interfaces	• Displays detailed output for each interface. • To display detailed output for only a single interface, include the interface type and number in the command (e.g. Gigabit Ethernet 0/0/0).
show ip route **show ipv6 route**	• Displays the routing table content listing directly connected networks and learned remote networks. • Append **static**, **eigrp**, or **ospf** to display those routes only.
show cdp neighbors detail	Displays detailed information about directly connected Cisco neighbor devices.
show arp **show ipv6 neighbors**	Displays the contents of the ARP table (IPv4) and the neighbor table (IPv6).
show running-config	Displays current configuration.
show vlan	Displays the status of VLANs on a switch.
show port	Displays the status of ports on a switch.
show tech-support	• This command is useful for collecting a large amount of information about the device for troubleshooting purposes. • It executes multiple show commands which can be provided to technical support representatives when reporting a problem

Manual data collection using **show** commands on individual network devices is extremely time consuming and is not a scalable solution. Manual collection of data should be reserved for simple networks or limited to individual network devices. For simpler network designs, baseline tasks typically use a combination of manual data collection and simple network protocol inspectors.

Sophisticated network management software is typically used to baseline large and complex networks. These software packages enable administrators to automatically create and review reports, compare current performance levels with historical observations, automatically identify performance problems, and create alerts for applications that do not provide expected levels of service.

Establishing an initial baseline or conducting a performance-monitoring analysis may require many hours or days to accurately reflect network performance. Network management software or protocol inspectors and sniffers often run continuously over the course of the data collection process.

13.1.9

Check Your Understanding – Network Documentation

Check your understanding of network documentation by choosing the BEST answer to the following questions.

1. Which topology diagram displays IP addresses?
   - ( ) ip topology
   - (•) logical topology
   - ( ) physical topology
   - ( ) port topology

2. Which document could be referenced to identify the OS on a server?
   - (•) End-system Documentation
   - ( ) LAN Switch Device Documentation
   - ( ) Router Device Documentation

3. Which three statements tell a network baseline answer? (Choose three.)
   - [x] How does the network perform during a normal or average day?
   - [ ] How much did the network cost?
   - [ ] What are the network policies?
   - [x] What part of the network is least used?
   - [x] What part of the network is most heavily used?
   - [ ] Who is responsible for managing the network?

4. True or False? A network baseline never ends and continually gathers information on a yearly basis.
   - ( ) True
   - (•) False

5. Which command could be used to get detailed information about directly connected Cisco neighbor devices?
   - (•) show cdp neighbor
   - ( ) show ip interface
   - ( ) show ip route
   - ( ) show version

Check | Show Me | Reset