Routing
Switching
Tigers
Forum

SWITCHING

www.rstforum.net

NETWORK TIME PROTOCOL (NTP)

Overview

IP-based networks are quickly evolving from the traditional best efforts delivery model to a model where performance and reliability need to be quantified and in many cases, guaranteed with SLAs. The need for greater insight to the network characteristics has led to significant research being targeted at defining metrics and measurement capabilities to characterize network behavior. The foundation of many metric methodologies is the measurement of time.

Keeping consistent time across the network devices will ensure that you can properly read log message and other information that is critical for troubleshooting.

Upon completing this lessons, you will be able to:

- Explain the need for accurate time and possible source of accurate time
- Manually configure a system clock on a Cisco device
- Explain idea behind NTP
- Describe NTP modes and their roles
- Secure NTP by using authentication and access lists
- Describe why and how would you configure NTP source interface
- Verify the configure NTP Version
- Configure NTPv4 in an IPv6 environment
- Compare SNTP with NTP
- Configure SNTP

The Need of Accurate Time

The Need Accurate Time

- Having accurate time on all devices in your network is crucial for troubleshooting and the PKI
- The system clock and be set in these ways:
  - NTP
  - SNTP
  - Manual Configuration

The heart of the time service is the system clock. The system clock runs from the moment the system starts and keeps the track of the current date and time. The system clock can be set from a number of source and, in turn, can be used to distribute current time through various mechanism to other system.

The system clock keeps track of time internally based on UTC. You can configure information about the local time zone and day light saving the time so that the time is displayed correctly relatively to the local time zone. The system clocks keeps track of whether time is authoritative or not. If it is not authoritative, the time is only available for display purpose and cannot be redistributed. Authoritative refers to trustworthiness of the source. Non-authoritative source do not guarantee accurate time. It is recommended to set clock on all network devices to UTC regardless of their location, and then configure the time zone to display the local time if desired.

Accurate time is needed for PKI that is based on X.509 certificates because they track validity: for example, the validity of a certificate expired on 10th of February 2011, but because of an incorrect time source your device still consider it valid. Accurate time is also essential consider for logging events in your network: for example, by using syslog, when devices are time synchronized, you can track the problem from device to another.

Configuring the System Clock Manually

Configuring the System Clock Manually

Switch# **show clock**

- Shows what the device think is the current time

Switch# clock set 12:13:00 10 January 2014

- Manually Configures the clock

Switch# **show clock details**

Time source is user configuration

- Verifies that the system clock changed; the **detail** keyword tells you the source of the clock configuration

To change the system clock manually, you need to use the **clock set** command from privileged EXEC mode and not global configuration mode. The date and time need to be set in UTC and not the local time zone.The local time zone and, if applicable, daylight saving time needs to be configured.

Configuring the System Clock Manually (Cont.)

Switch(config)# **clock timezone EDT -5**

Switch(config)# **clock summer-time EDT recurring**

- Changes the time zone and enables daylight saving time (in this example, EDT is used)

Switch# **show clock detail**

- Verifies how the clock setting reflects the local time.

Configuring the System Clock Manually (Cont.)

Switch# **Show calendar**

- **Shows the hardware clock on the device**

Switch# clock update-calendar

- Synchronizes the hardware clock with software clock

Switch# show calendar

- Verifies that the hardware clock is changed

A number of Cisco a battery-powered calendar system that tracks the date and time across system restarts and power outages. This calendar system is always used to initialize the system clock when the system is restarted. It can be also be considered as an authoritative source of time and redistributed through NTP. If no other source is available. Furthermore, if NTP is running, the calendar can periodically updated from NTP, compensating for the inherent drift in the calendar time. When a router with a system calendar is initialized, the system clock is set based on the time its internal battery-powered calendar. On models without a calendar, the system clock is set to predetermined time constant. The calendar is also called a hardware clock.

You can configure the hardware clock by using calendar set hh:mm:ss <1-31> month year.

Note: in absence of NTP or another reliable time source. Make sure that whenever you manually set the clock, you update the calendar with it to ensure continuity when the device restarts,

Note: Manually configuring time is neither accurate nor scalable. The better way to ensure accurate time is to use a protocol for time synchronization such as NTP.

Network Time Protocol

Network time protocol

- NTP synchronizes network devices to display the correct time.
- Accurate time is obtained from an external source:
  - Atomic clock
  - GPS receiver
  - Authoritative time source

NTP is designed to synchronize the time on a network of machines. NTP runs over UDP, using port 123 as both the source and destination, which in turn runs over IP. NTP is used to synchronize timekeeping among a set of distributed time servers and clients. A set of nodes on a network is identified and configured with NTP, and the nodes from a synchronization subnet, sometimes referred to as an overlay network. While multiple masters (primary severs) may exist, there is no requirement for an election protocol.

An NTP network usually gets its time from an authoritative time source, such as radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. An NTP client makes a transaction with its server over its polling interval (from 64 to 1024 seconds), which dynamically changes over time depending on the network conditions between the NTP server and the client. The other situation occurs when the router communicates to a bad NTP server (for example, an NTP server with a large dispersion). The router also increases the poll interval. No more than one NTP transaction per minute is needed to synchronize two machines. It is not possible to adjust the NTP poll interval on a router.

The communications between machines running NTP (associations) are usually statically configured. Each machine is given the IP address of all machines with which it should from associations. Accurate timekeeping is made possible by exchanging NTP message between each

pair of machines of an association. However, in an LAN, NTP can be configured to use IP Broadcast message instead. This alternative reduces configuration complexity because each machine can be configured to send or receive broadcast message. However, the accuracy of timekeeping is marginally reduced because the information flow is one-way only.

Network Time Protocol (cont.)

- NTP uses stratum values (1-16) to establish a hierarchy
- A lower stratum value equals a greater trust of accuracy.
- Stratum 1 devices use external clocks such as GPS.

NTP uses the concept of a stadium to describe how many NTP hops away a machine is from an authoritative time source. For example, a stratum 1 time server has a radio or atomic clock that is directly attached to it. It then send its time to Stratum 2 time server through NTP, and so on. A machine running NTP automatically chooses the machine with the lowest stratum number that is configured to communicate with using NTP as its time source. This strategy effectively builds a self-organizing tree of NTP speakers. NTP performs well over the nondeterministic path lengths of packet-switched networks, because it makes robust estimates of the following three key variables in the relationship between a client and a time server:

- **Network delay**
- **Dispersion of time packet exchanges**: A measure of maximum clock error between two hosts
- **Clock offset:** The correction that is applied to a client clock in order to synchronize it

Clock synchronization at the 10-millisecond level over long-distance WANs (124.27 miles [2000km]), and at the 1-millisecond level for LANs, is routinely achieved.

NTP avoids synchronizing to a machine whose time may not be accurate in two ways. First of all, NTP never synchronizes to a machine that is not synchronized itself. Second, NTP compares the time that is reported by several machines, and it will not synchronize to a machine whose time is significantly different from the others, even if its stratum is lower.

NTP Modes

NTP can operate in four different modes that provide you flexibility for configuring time synchronization in your network.

NTP Modes

- Server: Provides accurate time information to clients
- Client: Synchronizes it's time to the server. This mode is most suited for file-server and workstation clients that are no required to provide any form of time synchronization to other local clients. It can also provide accurate time to other devices.
- Peer: Peers exchange time synchronization information.
- Broadcast/multicast: Special "push" mode of NTP server; used only when time accuracy is not a big concern.

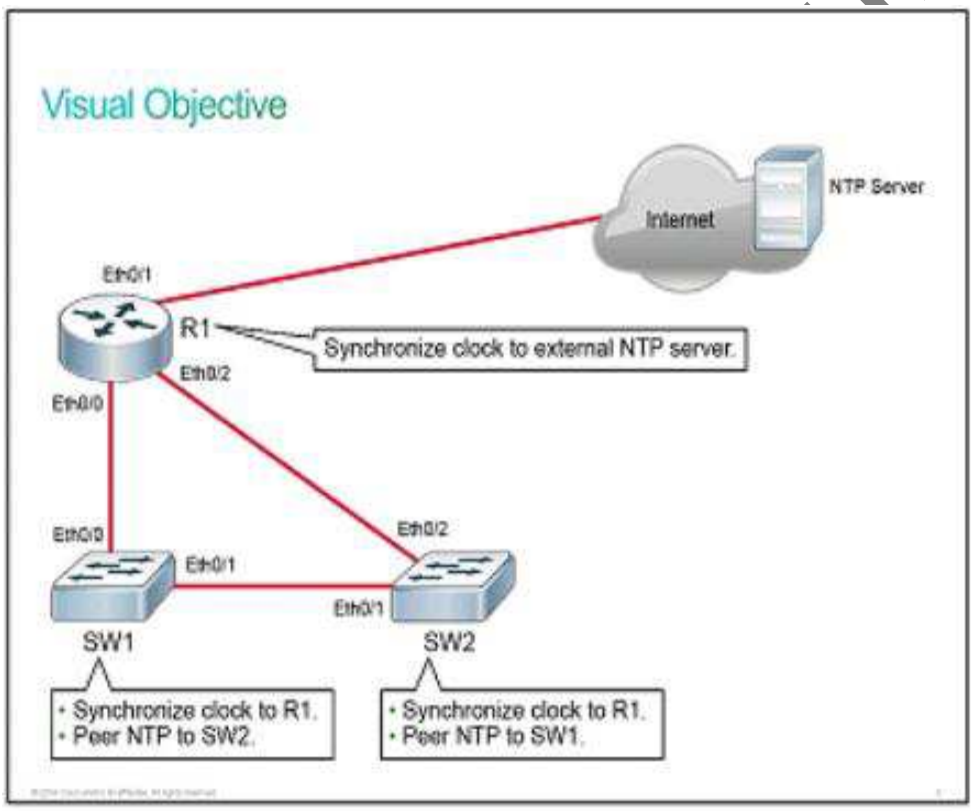
The server and client modes are usually combined with Cisco network devices. A device that is an NTP client can act as an NTP server to another device. The client/server mode is the most common Internet configuration. A client sends a request to the server and expects a reply at some future time. This process could also be called a poll operation because the client polls the time and authentication data from the server. A client is configured in client mode by using the server command and specifying the DNS name or address. The server requires no prior configuration. In a common client/server model, a client sends an NTP message to one or more servers and processes the replies as received. The server exchanges addresses and ports, overwrites certain fields in the message, recalculates the checksum, and returns the message immediately. The information that is included in the NTP message allows the client to determine the server time with respect to local time and adjust the local clock accordingly. In addition, the message includes information to calculate the expected timekeeping accuracy and reliability, as well as to select the best server.

The peer mode is also commonly known as symmetric mode. It is intended for configurations where a group of low stratum peers operate as mutual backups for each other. Each peer operates with one or more primary reference sources, such as a radio clock or a subset of reliable secondary servers. If one of the peers loses all the reference sources or simply ceases operation, the other peers automatically reconfigure so that time values can flow from the surviving peers to all the others in the group. In some contexts this operations described as push-pull, in that the peer either pulls or pushes the time and values depending on the particular configuration. Symmetric modes are most often used between two or more servers operation as a mutually redundant group. In these modes, the servers in the group members arrange the synchronization paths for maximum performance, depending on network jitter and propagation delay. If one or more of the group members fail, the remaining members automatically reconfigure as required.

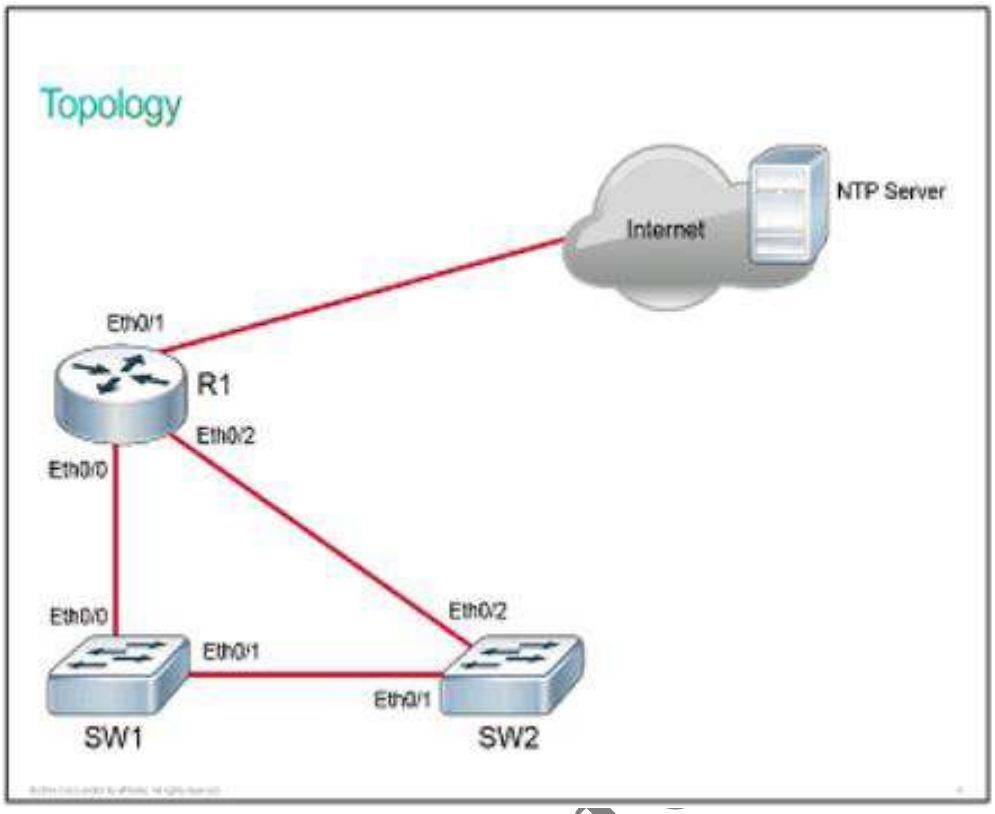
Where the requirements in accuracy and reliability are modest, clients can be configured to use broadcast or multicast modes. Normally, these modes are not utilized by servers with dependent clients. The advantage is that clients do not need to be configured for a specific server, allowing all operating clients to use the same configuration file. Broadcast mode requires a broadcast server on the same subnet. Because broadcast messages are not propagated by routers, only broadcast servers on the same subnet are used. Broadcast mode is intended for configurations that involve one or a few servers and a potentially large client population. A broadcast server is configured by using the broadcast command and a local subnet address. A broadcast client is configured by using the broadcast client command, allowing the broadcast client to respond to broadcast messages that are received on any interface.

NTP Configuration

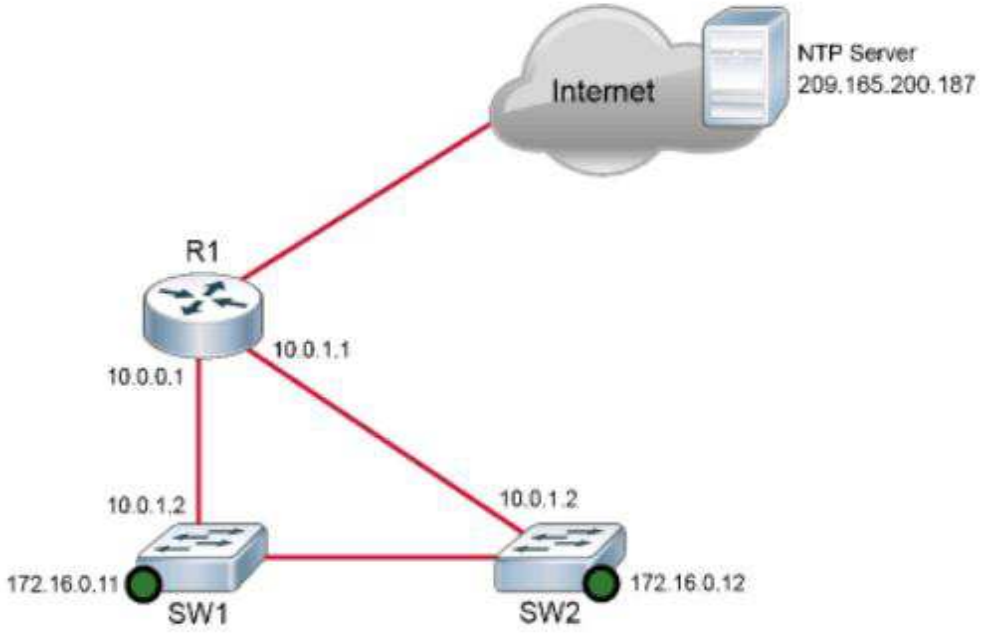
Configure devices in your network to synchronize their clocks via NTP.



Topology



IP Addresses Used For NTP Configuration



NTP

Step 1 Configure R1 to synchronize its clock to the public NTP server at 209.165.200.187.

R1(config)# **ntp server 209.165.200.187**

Before you can configure NTP, you will have to choose an NTP server for synchronization. A large organization has its own stratum 1 server. However, you will usually configure your devices to synchronize to a public NTP server.

NTP allows you to limit the maximum number of peer and client associations that your device will serve. This setup ensures that this NTP server is not overwhelmed by too many NTP command in global configuration mode.

When NTP is enabled on a device that in turn means that NTP is enabled on all interfaces. All interfaces will serve as NTP servers. You can use the ntp disable interface configuration command on interface that connect to external networks, because you do not want to provide a clock for them. NTP-disabled interfaces will turn off NTP server functionality but still allow the interface to act as an NTP client.

To configure a device to be an authoritative NTP server, use the ntp master stratum number command in global configuration mode. Configuring only an authoritative server in your network is recommended only if you do not have a reliable external reference clock. When using the ntp master command, you should choose a high stratum number, such as 10, so time associations through the inaccurate master clock are ignored if more trustworthy NTP information is made available. The local router should be also configured as a time source. This way the router will serve meaningful time to connected devices, even if it loses upstream connectivity. In that case approximately correct time is better than totally incorrect time.

It is recommended that you configure more than one NTP server for your devices to synchronize your device to. In that scenario, the device will associate itself with one server and mark the other one as an alternate. To specify a preferred NTP server, use the ntp server ip_address prefer command.

If you use an inbound access list on your internet interface, you will need to open up NTP communication for the NTP server that is selected:

access-list acl_number permit udp host NTP_host_IP eq ntp.

Note: The IP address that is used for the NTP server in this step is just an example-it will not work in real networks.

Step 2 On R1, issue the show ntp status command to investigate if the clock on the router has synchronized to the (public) NTP server.

R1# **show ntp status**

```
Clock is synchronized, stratum 2, reference is 209.165.200.187
nominal freq is 250.0000 Hz, actual freq is 250.000 Hz, precision is 2**10
ntp uptime is 1500 (1/100 of seconds), resolution is 4000
reference time is D67E670B.0B020C68 (05:22:19.043 PST Mon Jan 13 2014)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 630.22 msec, peer dispersion is 189.47 msec
loopfileter state is 'CRTL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 64, last update was 5 sec ago.
```

The output will tell you if NTP has successfully synchronized the clock on the device. The stratum will be +1 in comparison to the NTP source. Because the output shows that this device is stratum2, you can assume that you are synchronizing to a stratum 1 device.

NTP can be slow to synchronize. It can take up to 5 minutes for a device to synchronize with an upstream server. The NTP poll timer is 64 seconds.

Once a device is synchronized to an NTP source or configured to serve as a master, it will, in turn, act as an NTP server to any system that requests synchronization.

Step 3 Issue the show ntp associations command to verify the devices that R1 is associated with through NTP.

R1# **show ntp associations**

```
    address         ref clock       st   when   poll reach   delay   offset  disp
*~209.165.200.187   .LOCL.          1      24     64   17    1.000   -0.500   2.820
* sys.peer,  #  selected, + candidate, - outlier, x falseticker, ~ configured
```

The * before the IP address signifies that the devices are associated with that server. If you have multiple NTP servers defined, others will be marked with +, which signifies alternate options. Alternate servers are those that will become associated if the currently associated NTP server fails.

Step 4 On R1, investigate its current clock.

R1# **show clock**
04:56:17.655 PST Tue Jan 14 2014

R1 has its time zone set to PST. This behavior is IOL-specific. On real equipment, the time zone will be set to UTC by default. After you configure synchronization, you will also need to define the local time zone and, if applicable, enable summertime.

By default, NTP will synchronize only the software clock. If you want NTP also to synchronize the hardware clock, you need to issue the ntp update-calendar command in global configuration mode. Note that this command will not work in an IOL environment or on devices that do not have a hardware clock.

Step 5 On R1, configure the time zone that you are currently in, and enable summertime(if applicable) to the time zone that you are in.

In this example, the time zone is set to EDT and summertime is enabled. EDT is just a label. You can make it whatever you like. The -5 is the actual offset from UTC.

R1 (config)# clock timezone EDT -5
R1 (conifg)# clock summer-time EDT recurring

Step 6 On R1, verify that zone is now set to the zone that you are currently in and that summertime is enabled (if applicable).

R1# show clock detail
08:01:54.470 EDT Tue Jan 14 2014
Time source is NTP
Summer time starts 02:00:00 EDT Sun Mar 9 2014
Summer time ends 02:00:00 EDT Sun Nov 2 2014

In this example, R1 is configured with the EDT time zone and summertime is enabled.

Step 7 Configure SW1 to synchronize its clock to R1 via NTP. Configure SW1 with the same time zone and summertime configuration as R1.

Only a few devices in your network should synchronize to external NTP servers. All other devices in your networks will synchronize to those few devices.

SW1 (config)# ntp server 10.0.0.1
SW1 (config)# clock timezone EDT -5
SW1 (config)# clock summer-time EDT recurring

Step 8 Verify that the SW1 clock is synchronized to R1.

SW1# show ntp status
Clock is synchronized, sratum 3, reference is 10.0.0.1
Nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
Reference time is D67FD8F2.4624853F (10:40:34.273 EDT Tue Jan 14 2014)
Clock offset is 0.0053 msec, root delay is 0.00 msec
Root dispersion is 17.11 msec, peer dispersion is 0.02 msec

SW1 is considered a stratum 3 device because it synchronizes to a stratum 2 device, R1.

Step 9 Configure SW2 to synchronize its clock to R1 via NTP. Configure SW2 with the same time zone and summertime configuration asR1.

SW2 (config)# ntp server 10.0.1.1
SW2 (config)# clock timezone EDT -5
SW2 (config)# clock summer-time EDT recurring

Step 10 Verify that the SW2 clock is synchronized with R1.

SW2# **show ntp status**
Clock is synchronized, stratum 3, reference is 10.0.1.1
Nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
Reference time is D67FD974.17CE137F (10:42:44.092 EDT Tue Jan 14 2014)
Clock offset is 0.0118 msec, root delay is 0.00 msec

SW2 is considered a stratum 3 device because it synchronizes to a stratum 2 device, R1.

NTP Design Hierarchy

NTP Design Hierarchy

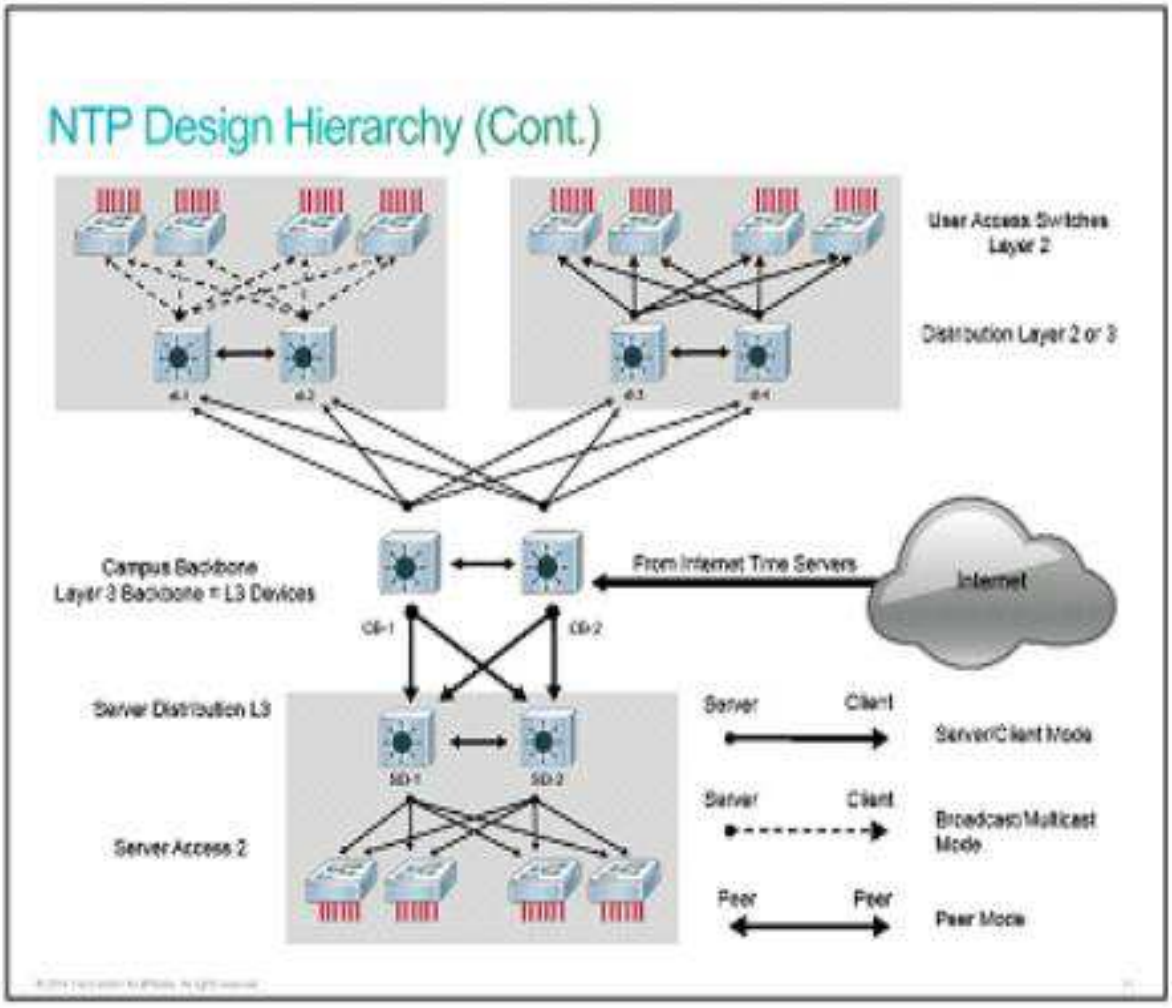
Flat versus hierarchical NTP design:

- Flat is more stable.
- Hierarchical is more scalable
- Hierarchical requires less administrative overhead

With a flat structure, you will configure all routers to be NTP peers for each other. Each router will act both as a client and server with every other router. Two or three routers should be configured to synchronize their time with external time servers. This model is very stable because each device synchronizes with every other device in the network. The disadvantages are difficulty of administration, slow convergence time, and poor scalability. If you add a device to the network, it can take you a good amount of time to identify all other devices and peer them with the new device. Because all devices in a peer-to-peer relationship have a say in selecting the best time, it can take a while to agree to what the accurate time is.

Do not use the flat model for large networks. You should implement NTP in a hierarchical manner. Every ISP uses this kind of model. Each ISP has multiple stratum 1 servers that synchronize other devices for the ISP. The later devices in turn provide time synchronization service to customer devices. That customer devices (or devices) then provide synchronization to the customer internal system. With a tiered model, there is less administrative overhead and time convergence is minimized. If you have a large network in your organization, it makes sense to implement a similar hierarchy of NTP synchronization.

There is also a star structure where all devices in a network have a relationship with few time servers in the core. This configuration is the middle ground between having a flat and hierarchical structure.



When you design NTP in a campus network, it is important to consider the broadcast association mode. The broadcast association mode simplifies the configurations for the LANs, but it reduces the accuracy of the time calculations. Therefore, the trade-off in maintenance costs must be considered against accuracy in performance measurements.

The high stratum campus network that is shown in the figure is taken from the standard Cisco Campus network design and contains three components. The campus core consists of two Layer 3 devices labeled CB-1 and CB-2. The server component that is located in the lower section of the figure has two Layer 3 devices labeled SD-1 and SD-2. The remaining devices in the server block are Layer 2 devices. In the upper left, there is a standard access block with two Layer 3 distribution devices labeled dl-1 and dl-2. The remaining devices are Layer 2 switches. In the client access block, the time is distributed by using the broadcast option. In the upper right, there is another standard access block that uses a client/server time distribution configuration.

Step 11 Configure SW1 and SW2 to be NTP peers for each other.

SW1 (config)# ntp peer 172.16.0.12
SW1 (config)# ntp peer 172.16.0.11

NTP peers will exchange time information with each other, which will prevent single points of failure.

Step 12 On SW1 and SW2, verify the NTP associations.

SW1# **show ntp association**

address	ref clock	st	when	poll	reach	delay	offset	disp
*~10.0.0.1	209.165.200.187	2	22	128	377	0.0	0.02	0.0
+~172.16.0.12	10.0.1.1	3	1	128	376	0.0	-1.00	0.0

* master (synced), # master (unsynced), + selected, - candidate, ~ configured

SW2# show ntp association

address	ref clock	st	when	poll	reach	delay	offset	disp
*~10.0.1.1	209.165.200.187	2	18	128	377	0.0	0.02	0.3
+~172.16.0.11	10.0.0.1	3	0	128	17	0.0	-3.00	1875.0

* master (synced), # master (unsynced), + selected, - candidate, ~ configured

Now Sw1 and SW2 both have two sources of NTP information. If you look at the output from SW1, R1 is listed as an NTP source to which SW1 is synchronized. SW2 is listed as a candidate source and it will be considered if the first source fails.

Securing NTP

NTP can be an easy target in your network. Because device certificates rely on accurate time, you should secure NTP operation. You can secure NTP operation by using authentication and access lists.

Securing NTP

NTPServer (config)# ntp authentication-key 1 md5 MyPasswork
NTPServer (config)# ntp authenticate
NTPServer (config)# ntp trusted-key 1

- Configures NTP authentication on the NTP client

NTPServer (config)# ntp authentication-key 1 md5 MyPasswork
NTPServer (config)# ntp authenticate
NTPServer (config)# ntp trusted-key 1
NTPServer (config)# ntp server 10.0.1.22 key 1

- Configures NTP authentication on the NTP client

NTP authenticates the source of information, so it only benefits the NTP client.

Cisco devices support only MD5 authentication for NTP. To configure NTP authentication, follow these steps:

- Define the NTP authentication key or keys with the ntp authentication-key command. Every number specifies a unique NTP key.
- Enable NTP authentication by using the ntp authenticate command.
- Tell the device which keys are valid for NTP authentication by using the ntp trusted-key command. The only argument to this command is the key that you defined in the first step.
- Specify the NTP server that requires authentication by using the **ntp server** ip_address **key** key_number command. You can similarly authenticate NTP peers by using the **ntp server** ip_address **key** key_number command.

Not all clients need to be configured with NTP authentication. NTP does not authenticate clients- it authenticates the source. Because of that the device will still respond to unauthenticated requests, so be sure to use access lists to limit NTP access.

After implementing authentication for NTP, use the **show ntp status** command to verify that the clock is still synchronized. If a client has not successfully authenticated the NTP source, then the clock will be unsynchronized.

Securing NTP (Cont.)

Corel (config)# access-list 1 permit 10.0.1.0 0.0.255.255
Corel (config)# ntp access-group peer 1

- Configure Core1 to peer with only a specified IP address

Corel (config)# access-list 1 permit 10.1.0.0 0.0.255.255
Corel (config)# ntp access-group serve-only 1

- Configures Core1 to answer synchronization requests from only 10.1.0.0/16 subnet devices.

Configure NTP access lists on server, to ensure that only authorized clients can synchronize with it.

Once a router or switch is synchronized to NTP, the source will act as an NTP server to any device that requests synchronization. You should configure access lists on those devices that synchronize their name with external servers. Why would you want to do that? A lot of NTP synchronization requests from the Internet might overwhelm your NTP server device. An attacker could use NTP queries to discover the time servers to which your device is synchronized and then, through an attack such as DNS cache poisoning, redirect your device to a system under its control. If an attacker modifies time on your devices that can confuse any time-based security implementations that you might have in place.

For NTP, the following four restrictions can be configured through access lists:

- Peer: Time synchronization requests and control queries are allowed. A device is allowed to synchronize itself to remote systems that pass the access list.
- Serve: Time synchronization requests and control queries are allowed. A device is not allowed to synchronize itself to remote system that pas the access list
- Serve-only: it allows synchronization requests only.
- Query-only: it allows control queries only.

Let us say that you have a hierarchical model with two routers configured to provide NTP service to the rest of the devices in your network. You would configure these two routers with peer and serve-only restrictions. You would use the peer restriction mutually on the two core routers. You would use the serve-only restriction on both core routers to specify which devices in your network are allowed to synchronize their information with these two routers.
If your device is configured as the NTP master, then you must allow access to the source IP address of 127.127.x.1. The reason is because 127.127.x.1 is the internal server that is created by the ntp master command. The value of the third octet varies between platforms.

After you secure the NTP server with access lists, make sure to check if the clients still have their clocks synchronized via NTP by using the show ntp status command. You can verify which IP address was assigned to the internal server by using the show ntp associations command.

NTP Source Address

NTP Source Address

NTPServer (config)# ntp source Loopback 0

- Configures Loopback 0 to be used as the source for NTP communication

The source of an NTP packet will be the same as the interface that the packet was sent out on. When you implement authentication and access lists, it is good to have a specific interface set to act as the source interface for NTP.
It would be wise to choose a loopback interface to use as the NTP source. The loopback interface will never be down like physical Interfaces.
If you configured Loopback 0 to act as the NTP source for all communication, and that interface has, for example, an IP address of 192.168.12.31, then you can write up just one access list that will allow or deny based on the single IP address of 192.168.12.31.

NTP Versions

Currently NTP versions 3 and 4 are used. Some vendors of operating systems customize and deliver their own versions. Generally, older clients can talk with newer versions.

NTP Versions

- NTP versions 3 and 4 are used currently.
- Version 4 introduces support for IPv6.
- NTPv4 also introduces better security
- NTPv3 uses broadcast messages and NTPv4 uses multicast messages

NTPv4 is an extension of NTPv3. NTPv4 supports both IPv4 and IPv6 and is backward-compatible with NTPv3.
NTPv4 provides the following capabilities:

- NTPv4 supports IPv6, making NTP time synchronization possible over IPv6.
- Security is improved over NTPv3. NTPv4 provides a whole security framework based on public key cryptography and standard X.509 certificates.
- Using specific multicast groups, NTPv4 can automatically calculate it time-distribution hierarchy through an entire network. NTPv4 automatically configures the hierarchy of the servers in order to achieve the best time accuracy for the lowest bandwidth cost. This feature leverages site-local IPv6 multicast addresses.

NTPv3 support sending and receiving clock updates by using IPv4 broadcast messages. Many network administrators use this feature to distribute time on LANs with the minimum client

configuration. For example, Cisco corporate LANs use this feature over IPv4 on local gateways. End-user workstations are configured to listen to NTP broadcast messages and synchronize their clock accordingly. In NTPv4 for IPv6, IPv6 multicast messages instead of IPv4 broadcast messages are used to send and receive clock updates.

NTPv3 access group functionality is based on IPv4 numbered access lists. NTPv4 access group functionality accepts IPv6 named access lists as well as IPv4 numbered access lists. NTPv4 adds DNS support for IPv6.

NTP in an IPv6 Environment

NTP is designed to time synchronize a network of machines. NTP runs over UDP, which in turn runs over IP. NTPv4 is an extension of NTPv3, which supports both IPv4 and IPv6.

NTP in an IPv6 Environment

- NTPv4 provides IPv6 support.

Switch(config)# ntp server 2001:D08:0:0:8:800:200C:417A version 4

- Configures device to synchronize its clock to a specified server via NTPv4

Switch(config)# ntp peer 2001:D88:0:0:8:800:200C:417A version 4

- Configures the software clock to synchronize a peer or to be synchronized by a peer

Networking devices that run NTPv4 can be configured to operate in various association modes when synchronizing time with reference time sources. There are two ways in which a networking devices can obtain time information on a network: by polling host servers and by listening to NTPv4 multicasts.

Configuring polling host servers is done by using the ntp server ipv6_address version 4 command. Sometimes this mode is called the asymmetric active mode.
Authentication and access list configuration with IPv6 similar to that in IPv4.

NTP in an IPv6 Environment (Cont.)

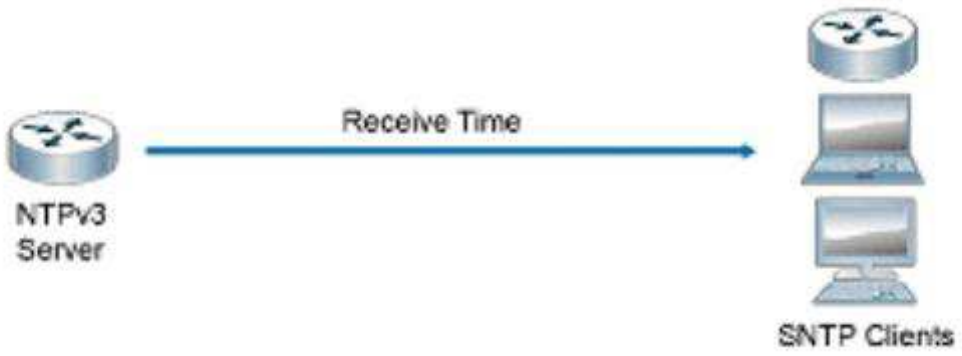
Switch# **show clock** *(Display the time and date from the system software clock)*
Switch# **show ntp associations [details]** *(Show the status of NTP associations)*
Switch# **show ntp status** *(Shows the synchronization information of NTPv4)*
Switch# debug ntp {adjust| authentication |events | loopfilter | packets | parans | refclock | select | sync | validity) *(Enables the debugging of NTP functionality)*

After you configure NTP in an IPv6 environment, the verification commands are very similar to those that are used in IPv4

Simple Network Time Protocol

SNTP is simplified, client-only version of NTP, SNTP can only receive the time from NTP servers; it cannot be used to provide time services to other systems.

Simple Network Time Protocol



- SNTP uses a subnet of NTP functionalities.
- It is a receive-only mechanism, usually for low-end devices.
- SNTP and NTP cannot coexist on the same device because they use the same port no.

SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanism of NTP.

You can configure SNTP to request and accept packets from configures servers or accept NTP broadcast packets from any source. When multiple sources send NTP packets, the server with the best stratum is selected. If multiple servers are at the same a configured server is preferred over a broadcast server. If multiple servers pass both tests, the first one to sends a packet is selected. SNTP will choose a new server only if it stops receiving packets from the currently selected server, or if a better server is discovered.

SNTP and NTP cannot coexist on the same machine because they use the same port. These two services cannot be configured on the system at the same time:

Switch(config)# **sntp server** 209.165.200.187

Sntp: cannot configure sntp as ntp is already running. Sntp: Unable to start sSNTp process

SNTP support for IPv6 address is available only if the image supports ipv6 addressing.

SNTP Configuration

There is little difference in the basis commands that are used between SNTP and NTP for end devices. The command **ntp server** server_ip is replaced with **sntp server** server_ip. The command **show ntp** is replaced with **show sntp**.

SNTP Configuration

Switch(config)# sntp authenticate

Switch(config)# sntp authentication-key 1 md5 cisco

Switch(config)# sntp trusted-key 1

Switch(config)# sntp server 172.16.22.44

- Allows the software clock to be synchronized by an SNTP time server

Switch# **show sntp**

SNTP server	Stratum	Version	Last Received	
209.165.209.187	1	4	00:00:00	Synced

Synced

- **Display information about SNTP that is available in cisco devices.**

To enable SNTP authentication, use the **sntp authenticate** command. To define an authentication key, use the command, **sntp authentication-key** number **md5** key. You can specify one or multiple keys. To mark key as trusted for SNTP, use the **sntp authentication-key** number **md5** key command. The last step is to tell the device to which server it should synchronize its time. You do that by using the **sntp server** server_ip command.

To verify whether the device has synchronized its time via SNTP, use the **show sntp** command. The output will show you the ip address of the SNTP server or servers it uses, the stratum number, the SNTP version number, when the last synchronization cycle was done, and whether time is synchronized or not.

If you need to troubleshoot SNTP server selection, issue the **debug sntp selec**t command. The debug will output messages that are related to both IPv4 and IPv6 servers.

If you need to troubleshoot the SNTP process, use the **debug sntp packets [detail]** command.

Summary

This topic summarizes the key points that were discussed in this lesson.

Summary

- Accurate time is essential for time-logging services and the PKI.
- To synchronize device to an external NTP source, use the ntp server ip_address command.
- NTP peers are same-stratum devices that exchange time synchronization information.
- The system clock is usually based on UTC. You need to configure the local time zone and summertime information (if applicable).
-
- When you use the **ntp master** command. You should choose a high stratum number, such as 10, so that time associations through the inaccurate master clock are ignored if more trustworthy NTP information is made available.
- **Show ntp status** will tell you if a device has its time synchronize via NTP.
- **Show ntp associations** will tell you which server a device is synchronized with.
- Configure NTP authentication on your devices to ensure that time source are credible devices.
- Configure access lists on an NTP server in order to prevent the server from answering NTP queries from devices that it should not answer.

SNMP

SNMP:

Modern communication networks are extremely complex. The reason for this complexity is partly due to a combination of different network technologies and techniques that are used to achieve their own specific goals. The trend of transporting different types of traffic (data, voice, and video) over the same IP infrastructure does not help to make your job as a network administrator an easy one.

In this environment, the need for network monitoring is important to effectively troubleshoot problems, track data, and plan for network upgrades.

SNMP exposes the environment and performance parameters of a network device, allowing an NMS to collect and process data. All modern versions of the NMS are based on SNMP.

Upon completing this lesson, you will be able to:

- Describe the role of SNMP
- Compare different SNMP versions
- List the recommended practices for setting up SNMP
- Configure SNMPv3
- Verify an SNMPv3 configuration

SNMP Overview:

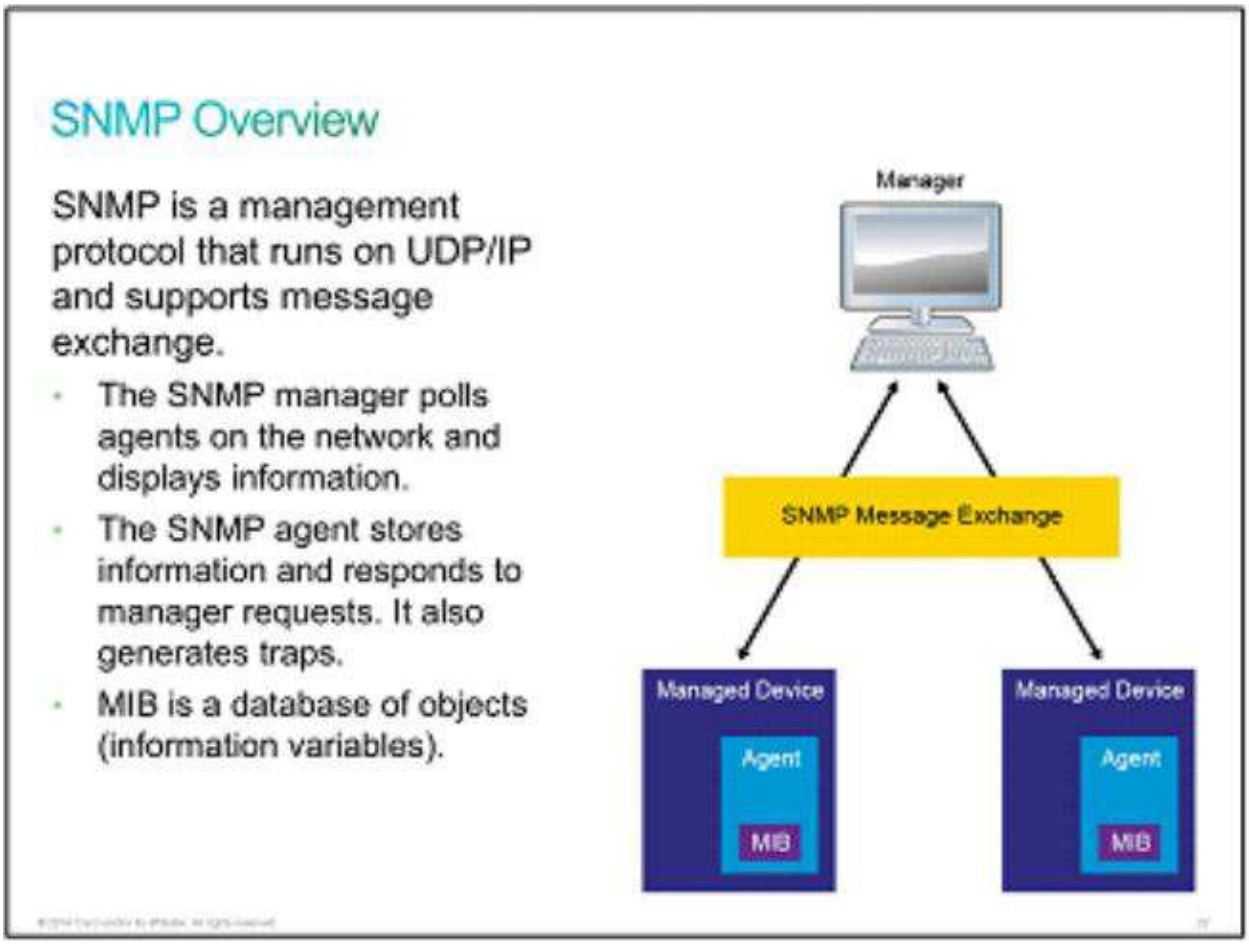
SNMP has become the standard for network management, SNMP is a simple, easy-to-implement protocol and is supported by nearly all vendors.

SNMP defines how management information is exchanged between SNMP managers and SNMP agents. SNMP uses the UDP transport mechanism to retrieve and send management information, such as MIB variables.

The SNMP manager periodically polls the SNMP agents on managed devices by querying the device for data. Periodic polling has a disadvantage: there is a delay between an actual event occurrence and the time at which the SNMP manager polls the data.

SNMP agents on managed devices collect device information and translate it into a compatible SNMP format according to the MIB. MIBs are collections of definitions of the managed objects. SNMP agents keep the database of values for definitions written in the MIB.

Agents also generate SNMP traps, which are asynchronous notifications that are sent from agent to manager. SNMP traps are event-based and provice almost real-time event notifications.

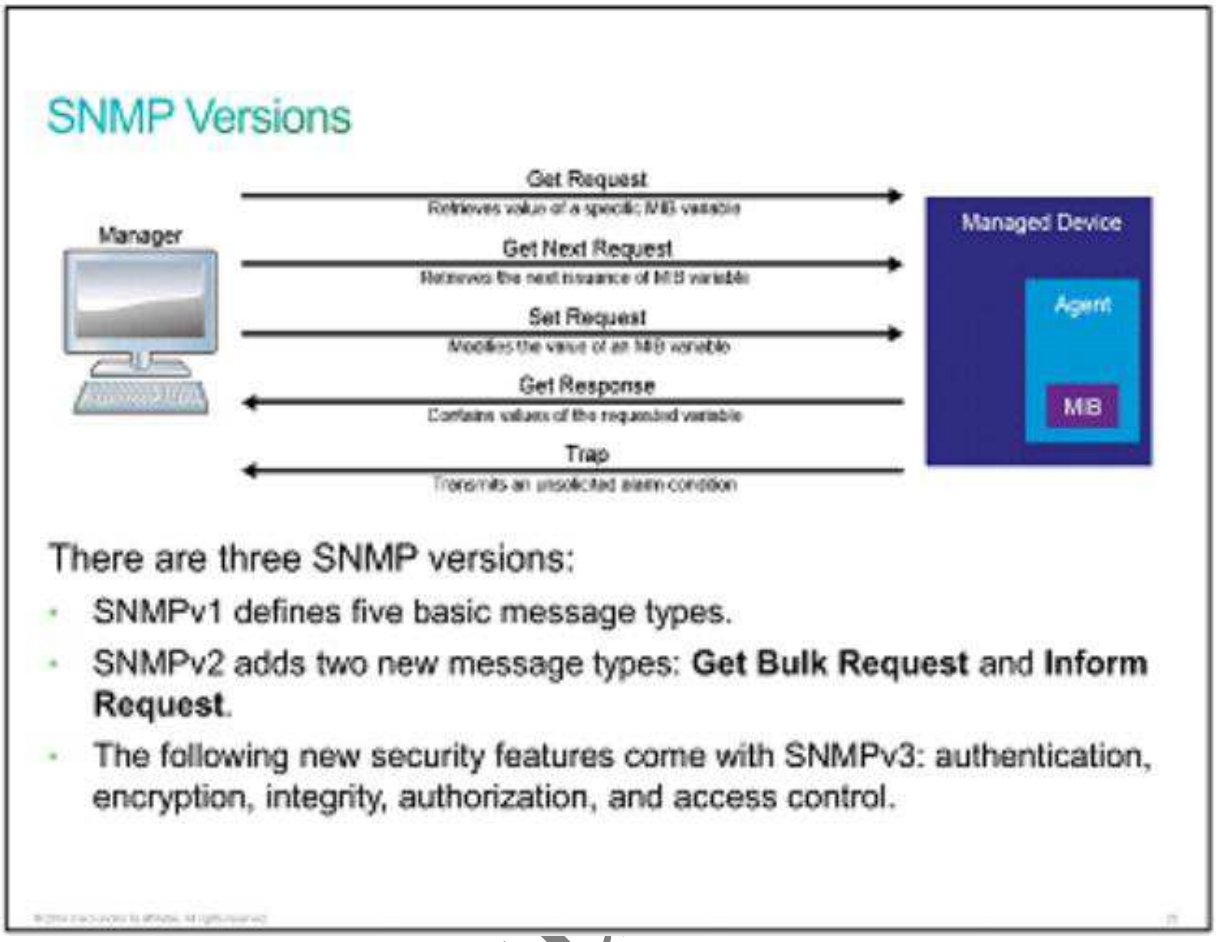


SNMP is typically used together environment and performance data such as device CPU usage, memory usage, interface traffic, interface error rate, and so on. Free and enterprise NMS software bundles provide data collection, storage, manipulation, and presentation. NMS offers a look into historical data, as well as anticipated trends. Based on SNMP values, NMS triggers alarms to notify network operators. The central view provides an overview of the entire network to easily identify irregular events, such as increased traffic and device unavailability due to a Dos attack.

NOTE: SNMP allows read/write access. A configuration of network devices can be applied with SNMP write access, so SNMP access must be configured with care and security in mind.

SNMP Versions

New functionalities were added to SNMP through time. There are currently three versions of SNMP.



SNMPv1 introduces five messages types: Get Request, Get Next Request, Set Request, Get Response, and Trap. SNMPv1 is rarely used today.

SNMPv2 introduced two new message types: Get Bulk Request, which polls large amounts of data, and Inform Request, a type of trap message with expected acknowledgment on receipt. Version 2 added 64-bit counters to accommodate faster network interfaces.

SNMPv2 added a comples security model, which was never widely accepted. Instead a community-based SNMPv2, known as Version 2c, draft standard was introduced and is now, due to its wide acceptance, considered the de facto version 2 stardard.

NOTE: Neither SNMPv1 nor SNMPv2 offers security features. Specially SNMPv1 and SNMPv2c cannot authenticate the source of a management message or provide encryption.

In SNMPv3, methods to ensure the secure transmission of critical data between the manager and agent were added. It provides flexibility in defining security policy. You can define a secure policy per group, and you can optionally limit the IP addresses to which its members can belong. You have to define encryption and hashing algorithm and password for each user.

SNMPv3 introduces three levels of security:

- noAuthNoPriv: No authentication is required, and no privacy (encryption) is provided.
- authNoPriv: Authentication is based on MD5 or SHA. No encryption is provided.
- authPriv: In addition to authentication, CBC-DES encryption is used.

SNMP Recommendations

There are some basic guidelines and best practices you should follow when setting up SNMP in your network.

SNMP Recommendation

- Restrict access to read-only.
- Set up SNMP views to restrict the manager to access only the needed set of MIBs.
- Configure ACLs to restrict SNMP access to only known managers.

Use SNMPv3 authentication, encryption, and integrity if possible.

NMS systems rarely need SNMP write access, so it is good practice to configure SNMP access as read-only. Separate community credentials should be configured for systems that require write access.

The command that sets up the SNMP view can block the user with access to only limited MIB. By defalult, there is no SNMP view entry. It works similar to an access list in that if you have any SNMP view on certain MIB trees, every other tree is implicitly denied.

Access lists should be used to limit SNMP access to only known SNMP managers.

SNMPv3 is recommended whenever possible. It provides authentication, encryption, and integrity. Be aware that the SNMPv1 or SNMPv2c community string was not designed as a security mechanism and is transmitted in clear text. Nevertheless, community strings should not be trivial and should be changed at regular intervals.

SNMPv3 Configuration

When you configure SNMPv3, there are a few mandatory steps you should implement first to get it to work properly.

SNMPv3 Configuration

1. Configure access lists for SNMP.
2. Configure the SNMPv3 view
3. Configure the SNMPv3 group
4. Configure the SNMPv3 user
5. Configure the SNMP trap receiver.
6. Configure the interface index persistence

```
SW(config) # access-list 99 permit 10.1.1.0 0.0.0.255
SW(config) # snmp-server view OPS sysUp7ize included
SW(config) # snmp-server view OPS ifDeser included
SW(config) # snmp-server view OPS ifAdminStatus included
SW(config) # snmp-server view OPS ifOperStatus included
SW(config) # snmp-server group group8  v3 priv read OP8 write OPS access 99
SW(config) # snmp-server user userZ groupZ v3 auth sha itasecret priv aes 256
anothersecret
SW(config) # snmp-server enable traps
SW(config) # snmp-server host 10.1.1.50 traps version 3 priv userZ cpu port-security
SW(config) # snmp-server ifindex persist
```

- SNMPv3 Configuration example

As shown in the example, you first have to configure a standard access list (**access-list 99**) which will be further used to limit SNMP access to a local device to SNMP managers with address in the subnet 10.1.1.0/24 (**permit 10.1.1.0 0.0.0.255**)

Next, configure the OPS view that will be used as both read and write view for the group Z. You can include or exclude specific OIDs from the view. In the example, ODIs for the system uptime, interface status, and description were added.

Then you configure SNMPv3 security policy. The SNMPv3 group is configured with the authPriv security level (**snmp-server group groupZ v3 priv**) and user for that group (**snmp-server userZ userZ**) with passwords for both authentication (**auth sha itasecret**) and encryption (**priv aes 256 anothersecret**).

You can also enable SNMP traps with the **snmp-server enable traps** command. Traps are sent by a local device, so receiving the SNMP manager has to be configured. SNMPv3 traps will be sent to the address 10.1.1.50 (**snmp-server host 10.1.1.50 traps**) by using the user with the authPriv

security level (**priv**). You can also limit event for which traps are sent. In the example, these are the CPU and port security-related events (**cpu port-security**).

SNMP does not identify object instances, such as network interface, by their names; instead, object instance are identified by their numerical indexes. Whenever the number of the instances changes (for instances, when a new loopback interface in configured), index number may shuffle. As a consequence, the NMS may mismatch data from different interfaces. To prevent an index shuffle, the snmp-server ifindex persist minor software upgrades.

Command	Description
snmp-server enable traps [notification-type}	Enables SNMP notification types that are avialable on your system.
Snmp-serve group group-name {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** context-name] [**read** read-view][**write** write-view] [**notify** notify-view][**access** [acl-number |acl-name]]	Configure a new SNMP group with specified authentication and optionally with specified associated SNMP context, read, write, notify view, and associated ACL.
Snmp-server host {ip-address} [**informs** | **traps**] **version** {**1** |**2c** |**3** {**auth** | **noauth**}}}	Specifies the recipient of an SNMP notification operation.
Snmp-server ifindex persist	Enables interface index persistence
Snmp-server user username group-name {**v1** | **v2c** | **v3** [**encrypted**][**auth** {**md5** | **sha**} auth-password}} [**access**[**priv** {**des** | **3des** |**acs** {**128** |**192** |**256**}} privpassword] | {acl-number | acl-name}]	Configures a new user to an SNMP group.
Snmp-server view view-name old-tree	Creates a view entry.

Verifying the SNMPv3 Configuration

Verifying the administrative and operational state of SNMP is a very important step in the overall process of setting up SNMPv3 in your network.

The command **show snmp** provides you with basic information about the SNMP configuration. You can see if the SNMP agent is enabled. You can verify whether the device is configured to send traps and, if so, to which SNMP manager the traps are sent. The SNMP traffic statistics are also provided.

Verifying the SNMPv3 Configuration

SW# show snmp
Chassis: F0C1322V1P5
0 SNMP packets input
0 Get-request PDUs
0 Get-next PDUs
0 Set-request PDUs
0 Input queue packet drops (Maximum queue size 1000)
476 SNMP packets output
0 Response PDUs
476 Trap PDUs
SNMP global traps: enable

SNMP logging: enabled
Logging to 10.1.1.50 162, 0/10, 476 sent, 0 dropped.
SNMP agent enabled

- Verify the basic SNMPv3 configuration

Verifying the SNMPv3 Configuration

SW#1 **show snmp view**
OPS sysUPTime – included nonvolatile active
OPS ifDescr – included nonvolatile active
OPS ifAminStatus – included nonvolatile active
OPS ifOperStatus – included nonvolatile active
Vldefault iso – included permanent active
Vldefault internet – include permanent active
Vldefault snmpUsnMIB – excluded permanent active
Vldefault snmpVacnMIB – excluded permanent active
Vldefault snmpCommunityMIB – excludded permanent active
Vldefault ciscoNgnt.252 – excluded permanent active
<. . . . Output omitted. . . .>

- Verify theSNMPv3 views

The command **show snmp view** gives you information about configured SNMP views. You can verify for each group OIDs are included. Also, there is default read view (**vl default**) displayed, which used if you do not configure any custom read views.

Verifying the SNMPv3 Configuration

SW# **show snmp group**

Groupname: Group 1 security model: v3 priv

Readview: OPS writeviewa: OPS

Notifyview: *tv.00000000.00000000.10000000.0

Row status: active access-list 99

- Verify the SNMPv3 group

The command **shows snmp user** gives you information about configured SNMP users. The most impotant parameter to notice are the username (userZ) and group name to which user belongs (groupZ). Aside from that, authentication (SHA) and encryption (AES-256) algorithms are displayed, which tells you that the group that the user belongs to is configured with the authPriv security level.

Summary

This topic summarizes the key points that were discussed in this lessons.

Summary

- SNMP can monitor and control devices.
- There are three SNMP Version.
- SNMPv3 provides the best security and should be used whenever possible.
- SNMP write access should be limited.
- SNMP views limit access to certain MIBs.
- SNMP access should be limited to known managers using ACLs.

IMPLEMENTIGN THE CISCO IOS IP SLA

CISCO IP SLA:

Cisco IOS IP SLA features can gather realistic information about how specific types of traffic are being handled when they flow across the network. The IP SLA device generates traffic that is destined to a far end device. When the far-end device responds, the IP SLA device gathers data about what happened to the traffic along the way.

Upon completing this lesson, you will able to:

- Describe the purpose of IP SLA
- Describe the roles of IP SLA source and responder
- Configure the ICMP echo IP SLA to test the availability of a remote device
- Describe the operation of IP SLA with the responder
- Explain the role of IP SLA responder time stamps
- Configure authentication for the IP SLA
- Configure the IP SLA UDP jitter testing

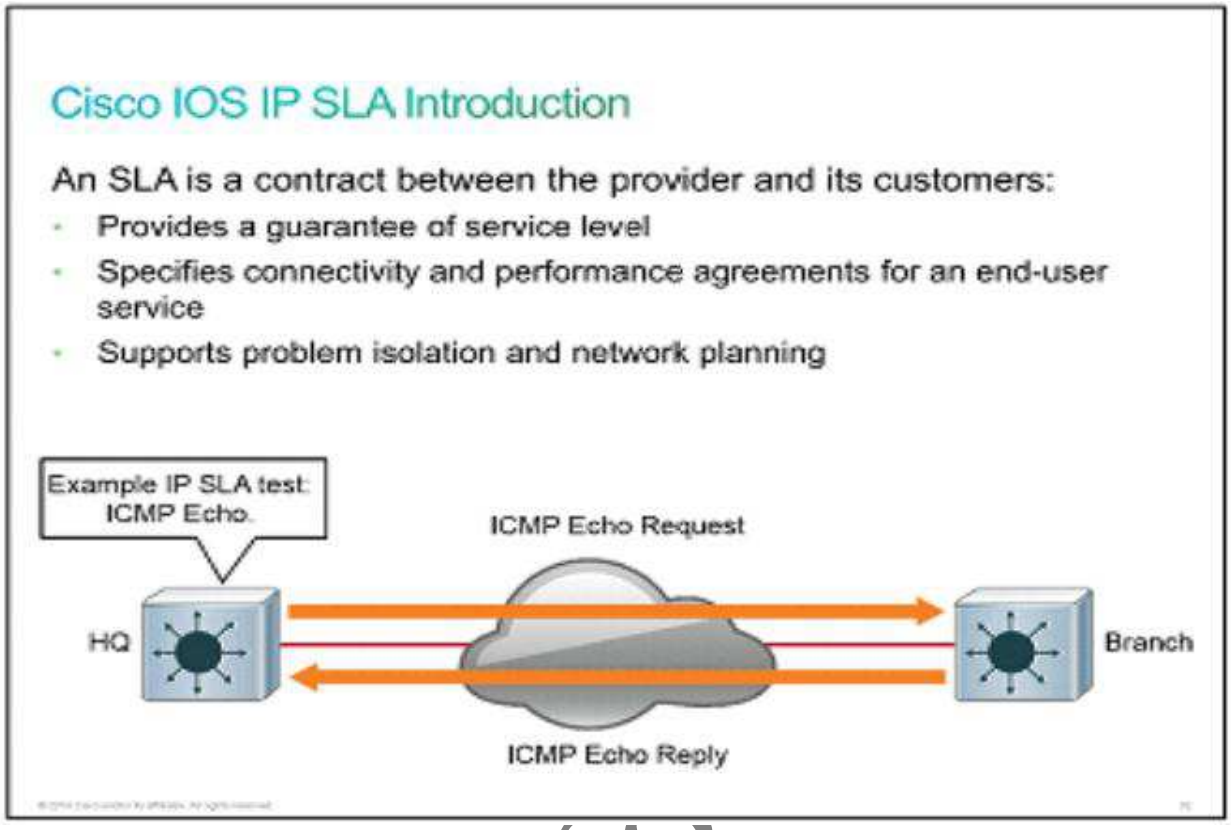
CISCO IOS IP SLA Introduction

The network has become increasingly critical for customers, and any downtime or degradation can adversely affect revenue. Companies need some form of predictability with IP Service. An SLA is contract between the network providers and its customers, or between a network department and integral corporate customers. It provides the form of guarantee to customers about the level of user experience.

An SLA specifies connectivity and performance agreements for an end-user service from a service provider. The SLA will typically outline minimum level of service and the expected level of service. The networking department can use the SLAs to verify that the service provider is meeting its own SLAs or to define service levels for critical business applications. An SLA can also be used as the basis for planning budgets and justifying network expenditures.

Administrator can ultimately reduce the MTTR by proactively isolating network issues. They can change the network configuration, based on optimized performance metrics.

Typically, the technical components of an SLA contains a guaranteed level for network availability, network performance in terms of RTT, and network response in terms of latency, jitter and packet loss. The specifics of and SLA vary depending on the applications that an organization is supporting in the network.



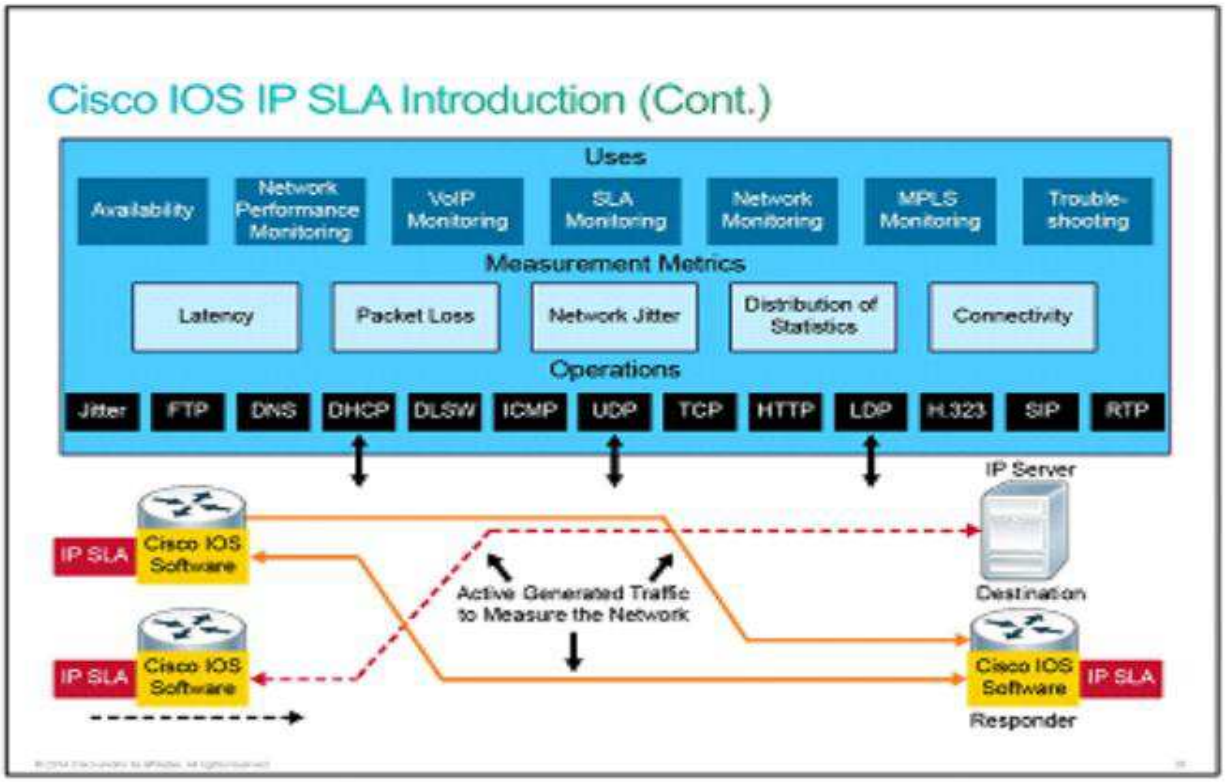
A simple example of an IP SLA test is the ICMP echo test. The IP SLA uses the ICMP echo request and response packets to test the availability of the far-end devices. The far-end devices can be any devices with IP capabilities, such as a router, switch, PC, server, and so on.

When you use the IP SLA features in the network, you can take advantage of the following features:

- Gather information about VoIP quality.
- Track interface to influence the behavior of first-hop redundancy protocols (HSRP, VRRP, GLBP)
- When thresholds are breached, scheduled further IP SLA test that will tell you more about your network
- When the threshold is breached, send an SNMP trap.

Multiple IP SLA operations (measurements) can run in a network at any given time. Reporting tools use SNMP to extract the data into a database and then report on it.

IP SLA measurement allow the network manager to verify service guarantees, which increases network reliability by validating network performance, proactively identifying network issues, and easing the deployment of new IP Service



There are several common function for the IP SLA measurement:

- Edge-to-edge network availability monitoring
- Network performance monitoring and network performance visibility
- VoIP, video, VPN, MPLS Network monitoring
- SLA monitoring
- IP Service network health
- Troubleshooting of network operations

Determining which test you can perform on the IP SLA source is platform-dependent:
Switch (config-ip-sla) # ?
IP SLA entry configuration commands:

dhcp	DHCP Operation
dns	DNS Query Operation
exit	Exit Operation Configuration
ftp	FTP Operation
http	HTTP Operation
icmp-echo	ICMP Echo Operation
path-echo	Path Discovered ICMP Echo Operation
path-jitter	Path Discovered ICMP Jitter Operation
tcp-connect	TCP Connect Operation
udp-echo	UDP Echo Operation
udp-jitter	UDP Jitter Operation

IP SLA Source and Responder

IP SLA Source and Responder

IP SLA Source:

- Cisco IOS Software device that sends data for operation
  - Target device may not be a Cisco IOS Software device
  - Some operations require an IP SLA responder
- IP SLA source stores result in MIB

IP SLA responder:

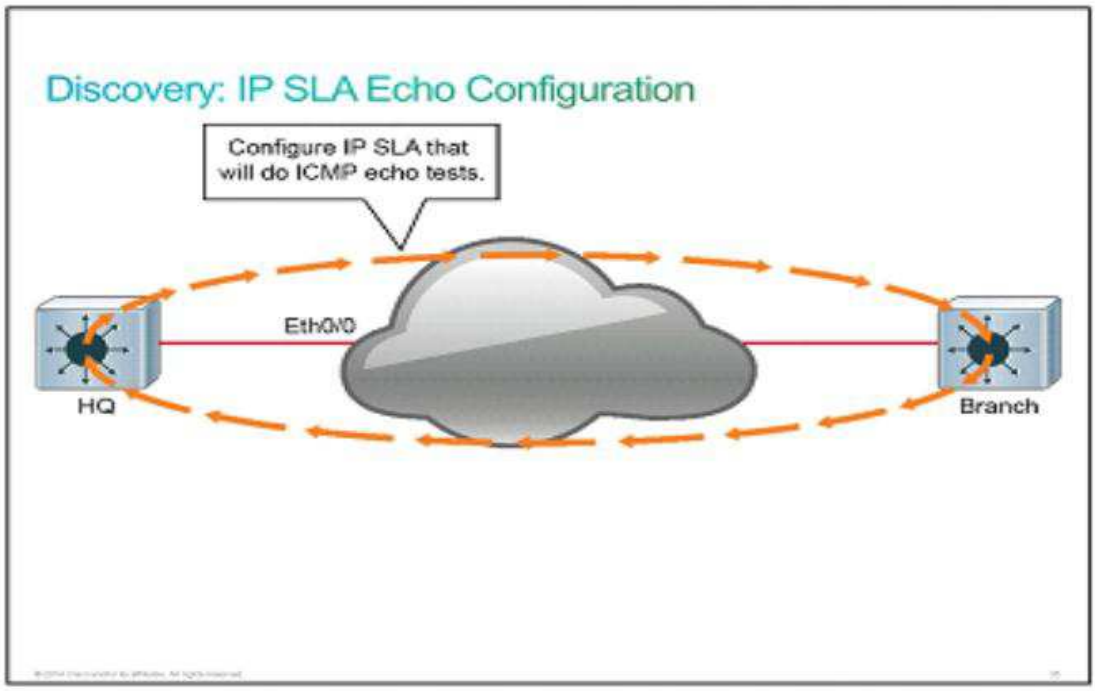
- Greater measurement Accuracy is available between an IP SLA source and responder.
- The IP SLA responder is a Cisco IOS Software device that is configured to respond to IP SLA packets that are based on the ip sla responder configuration command.

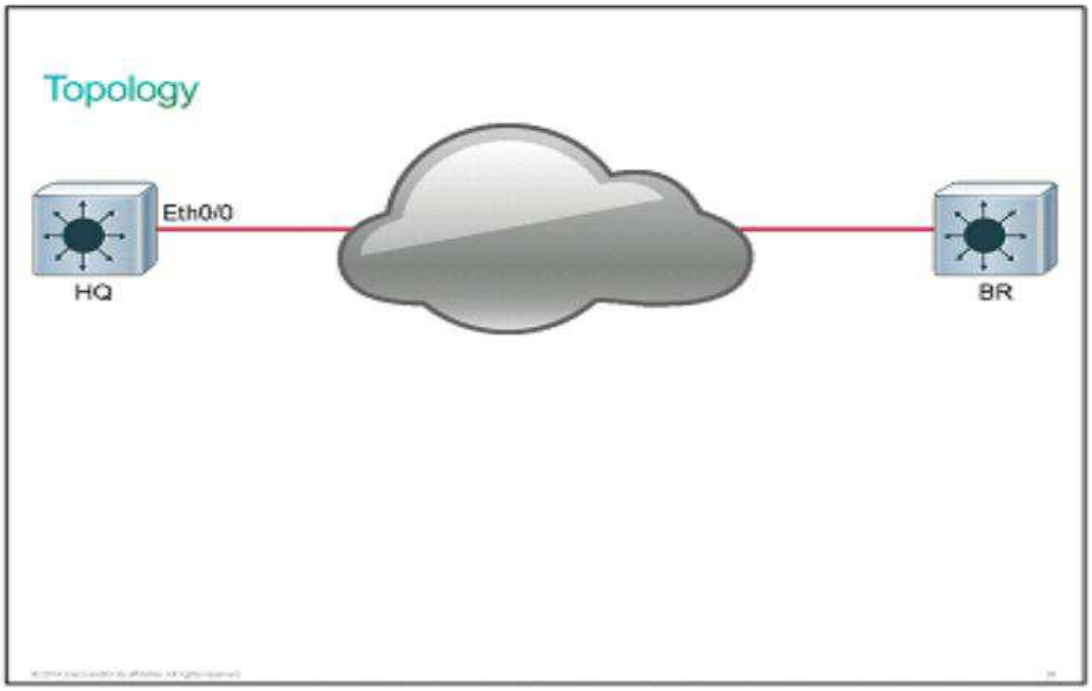
The IP SLA is where all IP SLA measurement probe operations are configured either by CLI or through an SNMP tool that supports IP SLA operation. The source is also the Cisco IOS device the sends probe packets. The destination of the probe may be another Cisco device or another network target such as a web server or IP host.

Although the destination of the majority of the tests can be any IP device, the measurements accuracy of some of the tests can be improved with an IP SLA responder. An IP SLA responder is a device that runs Cisco IOS Software. The responder adds a time stamp to the packets that are sent so the IP SLA source can take in to account any latency that occurred while the responder is processing the test packets. For this test to work properly, both clocks on the source and responder need to be synchronized through NTP.

IP SLA Echo Configuration

In this discovery, you will learn how to configure and verify the Cisco IOS IP SLA
HQ is local Layer 3 switch that you will configure as the IP SLA source. BR is a remote Layer 3 switch thazt will respondto the ip sla pings.





Note: if you shut down an interface on a real router or switch, the connected device will see it as "down/down". Due to virtualization specifics, IOL behavior is slightly different. If you shut down an interface on a router or switch. The connected device will see it as "up/up". In IOL, the status of an interface can only be "up/up" or "administratively down/down".

Device Information

Device	Interface	IP Address
HQ	Ethernet 0/0	192.168.1.1/24
BR	Ethernet 0/0	172.16.1.1/24
BR	Loopback 0	172.16.22.254/24

IP SLA Echo Configuration

Step 1. On the HQ switch, define the IP SLA with the number 1.

HQ(config)# **ip sla 1**

This step defines the IP SLA operation number. The operation number is an arbitrarily chosen number that uniquely identifies an IP SLA test

Step 2. Configure IP SLA 1 on HQ to perform ICMP echo tests to the BR ip address of 172.16.22.254.

HQ(config-ip-sla)# **icmp-echo 172.16.22.254**

Configuration the test to perform start with the **test-type** keyword. In this example, the test type is **icmp-echo.** the test type is followed by a list of parameters. In the icmp echo example, the mendatory parameter is the destination IP address. In this example, the destination ip address that is that of BR- 172.16.22.254.

Note: With Cisco IOS Software releases prior to 12.2(33), you have to use the keyword **type** before defining the test type**.** So this example would be **type icmp-echo 172.16.22.254.**

Step 3. Schedule IP SLA 1 on HQ to perform an ICMP echo test.

HQ(config)# **ip sla schedual 1 life forever start-time now**

The ip sla schedule command schedules the IP SLA test. It specifies when the test starts, for how long it runs, and for how long the collected data is kept.

Switch(config)# **ip sla schedule** operation-number[**life** {**forever** | seconds}] [**start-time**{hh:MM[:ss] [month day | day month] | **pending** |**now**|**after** hh:mm:ss}] [**ageout** seconds] [**recurring**]

With the **life** keyword, you set how long the IP SLA test will run. If you chose **forever**, the test will run until you manually remove it. By default, the IP SLA test will run for 1 hour.

With the **start-time** keyword, you set when the IP SLA test should start. You can start the test right away by issuing the **now** keyword, or you can configure a delayed start.

With **ageout** keyword, you can control how long the collected data is kept.

With the **recurring** keyword, you can schedule a test to run periodically- for example, at the same time each day.

Note: After an IP SLA test is scheduled to run, you will not be able to modify it.

Step 4. On HQ, verify the IP SLA configuration.

HQ# **show ip sla configuration**

Ip sla infrastructure Engine-III

When you verify the IP SLA configuration on HQ, you should see IP SLA 1 enabled to perform ICMP echo tests from the local device to the ip address of 172.16.22.254. the operation frequency is set to 60 seconds and that test will run forever, and collected entries will n out.

Step 5. On HQ, verify the IP SLA statistics.

Sh ip sla statistics

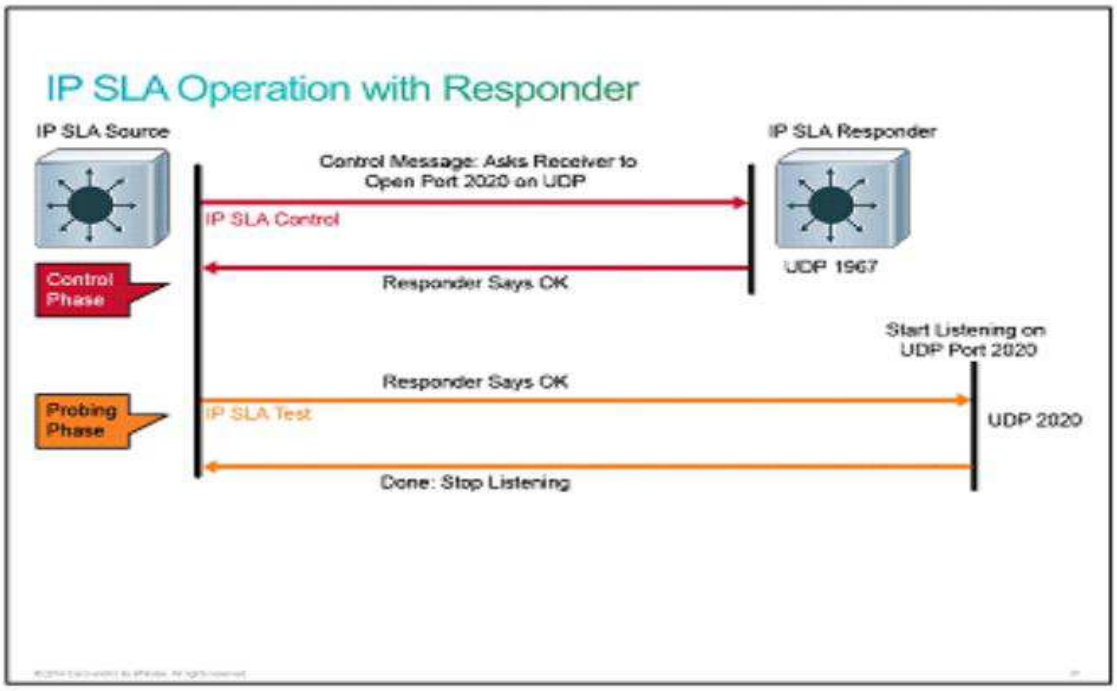
Use the **show ip sla statistics** command to investigate the result of the rest. In this example, the IP SLA 1 test on HQ was successfully performed 32 times and the test has never failed.

You can add the aggregated keyword to view a more summarized output of the **show ip sla statistic** command.
You can add the **details** keyword to view a more detailed output of the **show ip sla statistics** command.

Note: the **show ip sla application** command will show you which operations are supported on the platform and how many operations are configured or active.

IP SLA Operation with Responder

Specific IP SLA measurements, such as ICMP echo, Telnet. Or HTTP, can be performed against a destination device that is running standard network services. However the accuracy of the measurements can be greatly improved by using the IP SLA responder. The IP SLA responder is a component that is embedded in the destination Cisco device that allows the system to anticipate and respond to IP SLA request packets.



Switch and routers can take tens of milliseconds to process incoming packets due to other high-priority processes. This delay affects the responds times because the test-packet reply might be in a queue while waiting to be processed. In this situation, the response times would not accurately represent true network delays IP SLA minimizes these processing delays on the source device as well as on the target device (if the responder is being used) to determine true round-trip times. IP SLA test packets use time stamping to minimize the processing delays.

The network manager configure an IP SLA operation by defining a target device, protocol, and port number on the IP SLA source. The network manager can also configure reaction conditions. The operation is schedules to be run for a period of time to gather statistics. The following sequence of events occurs for each IP SLA operation that requires a responder on target:

1. At the start of the control phase, the IP SLA source sends a control message with the configured IP SLA operation information to IP SLA control port UDP 1967 on target router. The control message carries information such as protocol, port number, and duration.

- If MD5 authentication is enabled, the MD5 checksum is sent with the control message.
- If the authentication of the message is enabled, the responder verifies it;

if the authentication fails, the responder returns an authentication failure message.
If the IP SLA measurement operation does not receive a response from a responder, it tries to retransmit the control message and eventually times out.

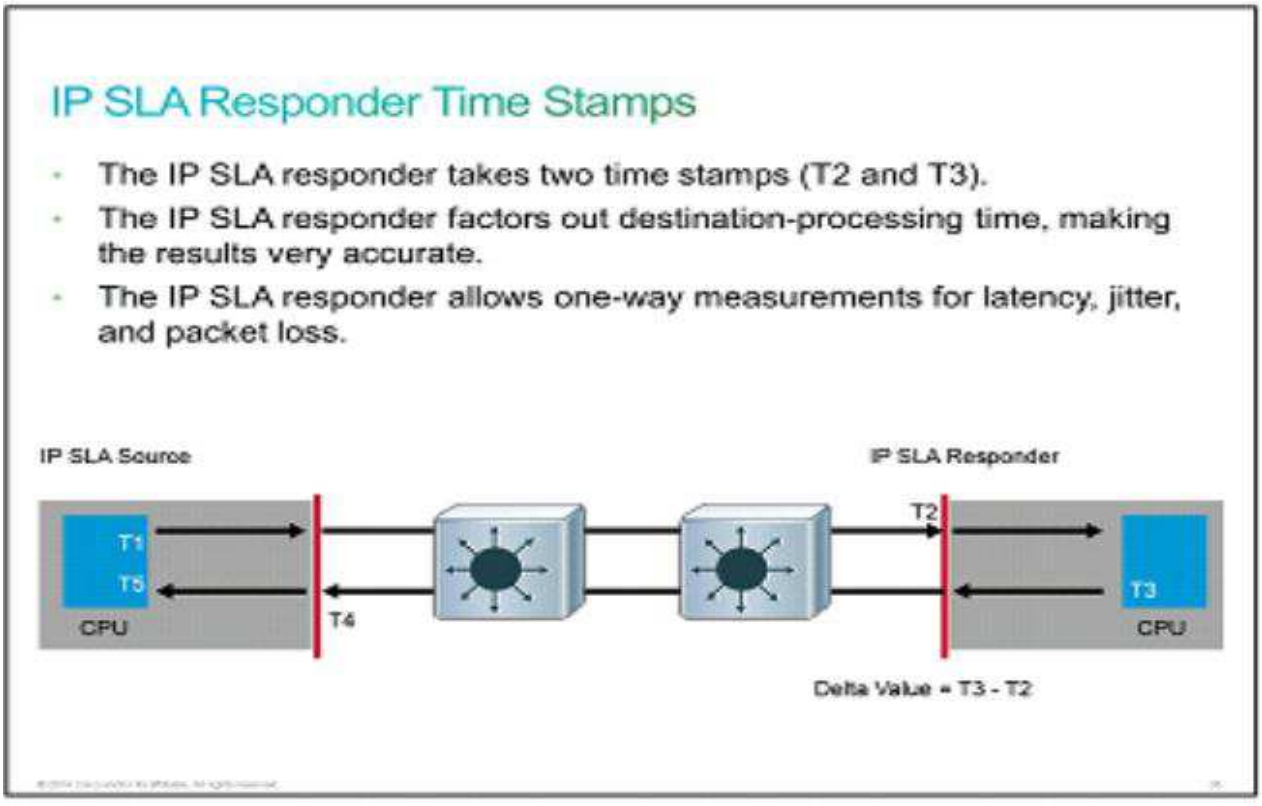
2. If the responder processes the control message, it sends an OK message to the source router and listens on the port that is specified in the control message for a specified duration. If the responder cannot process the control message, it returns an error. In the figure, UDP port 2020 is used for IP SLA test packets.

NOTE: The responder is capable of responding to multiple IP SLA measurement operation that try to connect same port number.

3. If the return code of the control message is OK, then the IP SLA operation moves to the probing phase, where it will send one or more test packets to the responder for response-time computations. The written code is available with the **show ip sla statistics** command. In the figure, these test messages are sent on control port 2020.

4. The responder accepts the test packets and responds. Based on the type of operation, the responder may add an "in" time stamp and an "out" time stamp in the response packet payload to account for the CPU time that is spent in measuring unidirectional packet loss, latency and jitter to a Cisco device. These time stamps help the IP SLA Source to make accurate assessments on one-way delay and the processing time in the target routers. The responder disables the user-specific port after it responds to the IP SLA measurements packets or when a specified time expires.

IP SLA Responder Time Stamps



The Figure illustrates the use of IP SLA responder time stamps in round-trip calculations. The IP SLA source will use four times stamps for the RTT calculation. The IP SLA source sends a test packet at time T1.

The IP SLA responder includes both the receipt time (T2) and transmit time (T3). Because of other high-priority processes, routers can take tens of milliseconds to process incoming packets. The delay affects the response times as the reply to test packets might be sitting in a queue while waiting to be processed. This time stamping is made with a granularity of sub-milliseconds. At times of high network activity, an ICMP ping test often shows a long and inaccurate response time, while an IP SLA-based responder shows an accurate response time. The IP SLA source subtracts T2 from T3 to produce the time that is spent processing the test packet in the IP SLA responder. This time is represented by a delta value.

The delta value is then subtracted from the overall RTT. The same principle is applied by the IP SLA source where the incoming T4 is also taken at the interrupt level to allow for greater accuracy, as compared with T5 when the packets is processed.

An additional benefit of two time stamps at the SLA responder is the ability to track one-way delay, jitter and directional packet loss. These statistics are critical, because a great deal of network behavior is asynchronous. To capture one-way delay measurements, you must configure both the IP SLA source and the IP SLA responder with the NTP.

Both the source and destination must be synchronized to the same clock source. The IP SLA responder provides enhanced accuracy for measurements, without the need for dedicated third-party external probe devices. It also provides additional statistics, which are not otherwise available via standard ICMP-based measurement.

The key chain should be configured on the source router as well as on the destination router. Only the source device will be allowed to interact with the destination router.

Multiple authentication strings can be configured for the key chain. When multiple strings are configured, then MD5 alternates between the strings during communication.

Once a key chain is configured, it has to be tied to Cisco IOS IP SLAs, so that it could use these authentication strings for authenticating control messages.

Summary

Implementing Port Mirroring for Monitoring Support

Overview

Cisco switches provide various information, such as resource utilization, traffic counts, error counts, and so forth, however, certain traffic information can be acquired only by specialized traffic sniffers and analyzers. To feed the traffic sniffer with traffic flows, you can use the SPAN features.

Upon completing this lesson, you will be able to:

- Describe SPAN
- Describe SPAN terminology
- Describe different version of SPAN
- Configure SPAN
- Verify the local span configuration
- Configure RSPAN
- Verify the RSPAN configuration

What is SPAN?

A traffic sniffer can be a valuable tool for monitoring and troubleshooting a network. Properly placing a traffic sniffer to capture a traffic flow but not interrupting it can be challenging.

When LANs were based on hubs, connecting a traffic sniffer was simple. When a hub receives a packet on one port, the sends out the packet on all ports except on the one where the hub received the packets. A traffic sniffer that connected a hub port could thus receive all traffic in the network.

Modern local network are essentially switched networks. After a switch boots, it starts to build up a Layer 2 forwarding table on the basis of the source MAC address of the different packets that the switch receives. After this forwarding table is built, the switch forwards traffic that is destined for a MAC address directly to the corresponding port, thus preventing a traffic sniffer that is connected to another port from receiving the unicast traffic.

The SPAN features introduced on switches.

The SPAN feature allows you to instruct a switch to send copies of packets seen on one port to another port on the same switch.

If you would like to analyze the traffic flowing from one PC1 to PC2, you need to specify a source port. You can either configure the GigabitEthernet 0/1 interface to capture the ingress traffic or the GigabitEthernet 0/2 interface to capture the egress traffic. Second specify the GigabitEhternet 0/3 interface as a destination port. Traffic that flows from PC1 to PC2 will then be copied to that interface and you will be able to analyze it with a traffic sniffer.

Besides the traffic on ports, you also monitor the traffic on VLANs.

SPAN Terminology

SPAN features two different port types. The source port is a port that is monitored for traffic analysis. SPAN can copy ingress, egress, or both types of traffic from a source port. Both Layer 2 and Layer 3 ports can be configured as SPAN source ports. The Traffic is copied to the destination (also called monitor) port.

The association of source port and a destination port is called a SPAN session. In a single session you can monitor at least one source port. Depending on the switch series you might be able to copy session traffic to more than one destination port.

Alternative you can specify a source VLAN, where all ports in the source VLAN become sources of SPAN traffic. Each SPAN session can have either ports or VLANs as sources, but not both.

Remote SPAN

The SPAN feature is limited, because it allows for only a local copy on a single switch. A typically switched network usually consist of multiple switches, and it is practical to monitor ports spread all over the switched network with a single packet sniffer. This setup is possible with RSPAN.

While local SPAN support source and destination ports on one switch only, remote SPAN supports source and destination ports on different switches.

RSPAN consist of following:

- RSPAN source session
- RSPAN VLAN
- RSPAN destination session

You separately configure the RSPAN source and destination sessions on different switches. Your monitored traffic is flooded into an RSPAN VLAN that is dedicated for the RSPAN session in all participating switches. The RSPAN destination port can then be anywhere in that VLAN.

On some of the platforms, a reflector port needs to be specified together with an RSPAN VLAN. A The reflector port s is physical interface that acts as a loopback and reflects the traffic that is copied form the Source Port to an RSPAN VLAN. No traffic is actually send out of the interface that is assigned as the reflector port. The need for the reflector port. The need for a reflector is caused by a hardware design limitation on some platforms. The reflector port can be used for only one session at a time.

Local SPAN Configuration

When you configure the SPAN feature, you must know the following facts:

- The destination port cannot be the Source Port, or vice versa.
- The number of destination ports is platform-dependent; some platforms allow for more than one destination port.
- The destination port is no longer a normal switch port-only monitored traffic passes through that port.

In the example in the figure, the objective is to capture all the traffic that is sent or received by the PC that is connected to the GigabitEthernet 0/1 port on switch. A packet sniffer is connected

to the GigabitEthernet 0/2 port. The switch is instructed to copy all the traffic that is sends and received on GigabitEthernet 0/1 to GigabitEthernet 0/2 by configuring the SPAN session.
The SPAN session is identified by a session number; in our example it is 1. The first step is then that you associate the SPAN session with source ports or VLANs by using following command:
monitor **session** number **source** interface/vlans
Similary, you associate the destination port with the SPAN session number by using the following command:
monitor **session** number **destination** interface/vlans

Verifying the Local SPAN Configuration

You can verify the configuration of the SPAN session by using the **show monitor** command.

As shown in the figure, the **show monitor** command returns the type of the session, source ports for each traffic direction, and the destination port. In the example, information about session number 1 is presented – the source port for both traffic directions is GigabitEthernet 0/1 and the destination port is GigabitEthernet 0/2. The ingress SPAN is disabled on the destination port, so only traffic that leaves the switch is copied to it.

In case you have more than one session configured, information about all sessions is shown after using the **show monitor** command.

RSPAN Configuration

These are some differences between the configuration of RSPAN and the configuration of local SPAN.

Because the port are now on two different switches, use a special RSPAN VLAN to transport the traffic from one switch to the other. You configure this VLAN like any other VLAN, but in addition you enter the **remote-span** key word in VLAN configuration mode. You need to define this VLAN on all switches in the path.

Remote SPAN uses two session – the source and the destination.
Use the following commands to define the port that traffic is captured from and the traffic is copied to:

- **monitor sessions** number **source interface** slot/number
- **monitor sessions** number **destination remote vlan** vlan-number

These two sessions need to be defined on both the local and remote switches.
Session number are local to each switch, so they do not need to be the same on every switch.

Verifying the RSPAN Configuration

As with the local SPAN configuration, you can verify the RSPAN session configuration by using the **show monitor** command.

The only difference is that on the source switch the session type is now identified as "Remote Source Session", while on the destination switch the type is marked as "Remote Destination Session".

In addition to verifying the correct configuration, it is also important that you verify that the VLAN is configured correctly as an RSPAN VLAN on both switches. Use the **show vlan remote-span** command to verify the configuration.

Summary

This topic summarizes the key points that were discussed in this lesion.

Verifying Switch Virtualization

Overview

Redundant topologies often introduce overhead in terms of management, resiliency, and performance. To reduce the number of logical network devices and simplify the Layer 2 and Layer 3 network topology, you can use two switch virtualization technologies - Cisco Stack Wise & VSS.

Upon completing this lesson, you will be able to:

- Describe the need and basic idea behind switch stacking and VSS
- Describe Stack Wise
- Describe the benefits of Stack Wise
- Verify the Stack Wise Configuration
- Explain supervisor redundancy modes
- Describe VSS
- Describe VSS benefits

- Verify the VSS configuration

The Need of Logic Switching Architectures

This figure shows a typical switch topology at the access and the distribution layer. Two (or more) access switches are sitting next to each other in the same rack to provide enough ports for all the network devices, each one with two redundant connections to each of distribution switches.

This topology introduces certain overhead in terms of management, resiliency and performance.

Every switch demands its own configuration and management, even though you can clearly identify only two different roles – access and distribution. Every access switch needs its own uplink to each of the distribution switches in order to satisfy the redundancy requirements, but one of the STP has to be blocked by STP to prevent a loop, thus cutting the bandwidth in half. Configuring per-VLAN STP will unequally utilize both uplinks, but with additional management overhead. Hosts that are connected to ASW1 can communicate with only in the same VLAN connected to ASW2 via one of the distribution switches.

What is StackWise?

The Cisco Stack Wise technology provides a method for collectively utilizing the capability of a stack of switches. Configuration and routing information is shared every switch in the Stack, creating a single switching unit. Switches can be added to and deleted from a working stack without affecting the stack performance.

The switches are united into a single logical unit with special stack interconnect cables that create a bidirectional closed-loop path. The bidirectional path acts as a switch fabric for all the connected switches. The network topology and routing information is updated continuously through the stack interconnect cables. All stack members have full access to the stack interconnect bandwidth. The stack is managed as a single unit by a master switch, which is elected from one of the stack member switches. Up to nine separate switches can be joined.

Each stack of switches has a single IP address and is managed as a single object. This single IP management applies to activities such as fault detection, VLAN creation and modification, security and QOS controls. Each stack has only one configuration file, which is distributed to each member in the stack. Each switch in the stack can share the same network topology, MAC address and routing information. In addition, it allows for any member to become the master if the master ever fails.

Stackwise Benefits

Uniting switches into a stack has multiple benefits.

Cisco Stack Wise typically unities access switches that are mounted in the same rack. Multiple switches are used to provide enough access ports. The stack, containing up to nine switches, is managed as single unit, reducing the number of units you have to manage in your network. Switches can be added to and removed from a working stack without affecting the stack performance. When a new switch is added, the master switch automatically configures the units with the currently running IOS image and the configuration of the stack, you do not have to do anything to bring up the switch before it is ready to operate.

The switches are united into a single logical unit by using special stack interconnect cables that creates a bidirectional closed-loop path. This bidirectional path acts as a switch fabric for all the connected switches. When a break is detected in a cable, the traffic is immediately wrapped back across the remaining path to continue forwarding.

Multiple switches in a stack can create an EtherChannel connection. STP can thus be avoided, doubling the available bandwidth of the existing distribution switch uplinks.

Verifying Stackwise

You can verify the status if your stack by using the **show switch** command with different parameters.

The **show switch** command without additional parameters returns the shared stack MAC address and lists all the switches in a stack with their stack number, stack role, MAC address, hardware priority, hardware version, and current state. The hardware priority is used in the stack master election and can be configured. The hardware version if they support the same system-level features. The hardware version number is not used in the stack master election.

Each stack switch uses two ports to connect to other switches to form a bidirectional ring. You can verify the state of a stack port with the **show switch stack-port** command.

The **show platform stack manager all** command offers an in-depth view into the Stack Wise status. It reveals the stack status, status of stack port, stack manager version, different counters and so on.

Redundant Switch Supervisors

The Cisco Supervisor Engine module is the heart of the Cisco modular switch platforms. The supervisor provides centralized forwarding and processing. All software processes of a modular switch are run on a supervisor.

Platform such as the Catalyst 4500, 6500 and 6800 Series can accept two supervisor modules that are installed in a single chassis, thus removing a single point of failure. The first supervisor module to successfully boot becomes the active supervisor chassis. The other supervisor remains in a standby role, waiting for the active supervisor to fail.

All switching function are provided by the active supervisor. The standby supervisor, however, is allowed to boot up and initialize only to certain level. When the active module fails, the standby module can proceed to initialize any remaining functions and take over the active role.

Supervisor Redundancy Modes

Redundant supervisor modules can be configured in several modes. The redundancy mode affects how the two supervisor handshake and synchronize information. Additionally, the mode limits the state of readiness for the standby supervisor. The more ready the standby module is allowed to become, the less initialization and failover time will be required.

You can use the following redundancy modes on Catalyst switches:

- **RPR:** The redundant supervisor is only partially booted and initialized. When the active module fails, the standby module must reload every other module in the switch, the initialize all the supervisor functions.
- **RPR+:** The redundant supervisor is booted, allowing the supervisor and route engine to initialize. No Layer 2 or Layer 3 functions are started. When the active module fails, the standby module finishes initializing without reloading other switch modules. Switch port can retain their state.
- **SSO:** The redundant supervisor is fully booted and initialize. Both the startup and running-configuration content are synchronized between the supervisor modules. Layer 2 information is maintained on both supervisor so that hardware switching can continue during a failover. The state of the switch interface is also maintained on both supervisor so that links do not flap during a failover.

Cisco Nonstop Forwarding

You can enable another redundancy feature along with SSO. Cisco NFS is an interactive method that focuses on quickly rebuilding the RIB table after a supervisor switchover. The RIB is used to generate the FIB table for Cisco Express Forwarding, which is downloaded to any switch module that can perform Cisco Express Forwarding.

What is VSS?

The VSS is a network system virtualization technology that combines a pair of Cisco Catalyst 4500 or 6500 Series Switches into one virtual switch, increasing the operational efficiency, booting nonstop communications, and scaling the system bandwidth capacity. The VSS simplifies network

configuration and operation by reducing the number of Layer 3 routing neighbors and by providing a loop-free Layer 2 topology.

The VSS is made up of two Catalyst switches and a VSL between them. The VSL is made up of up to eight 10 Gigabit Ethernet bundled into an EtherChannel. The VSL carries the control plane communication between the two VSS members, as well as regular data traffic.

Once the VSS is formed, only the control plane of one of the member is active. The data plane and switch fabric of both member are active. Both chassis are kept in sync with the inter-chassis SSO mechanism along with Cisco NFP to provide nonstop communication even in the event of a failure of one of the member supervisor engines or chassis

VSS Benefits

The VSS increases operational efficiency by reducing switch management overhead and simplifying the network. It provides a single of management, IP address, and routing instance.

You see a single management point from which you configure and manage the VSS as a single layer Layer 2 switching or Layer 3 routing node, thus reducing the control protocol traffic. The VSS provides a single VLAN gateway IP address, removing the need for a first-hop redundancy protocol (HSRP, VRRP, and GLBP). The MEC allows you to bundle links to two physical switches in the VSS, creating a loop-free redundant topology without the need for STP.

An inter-chassis stateful failover result is no disruption to applications that rely on network state information (for example, forwarding table info, Net flow, NAT, authentication and authorization). The VSS eliminates Layer 2 and Layer 3 protocol convergence if a virtual switch member fails, resulting in deterministic sub second virtual switch recovery.

Verifying VSS

You can verify the status of your stack using the **show switch virtual** command with different parameters.

To display configuration and status information for a VSS, use the **show switch virtual** command. Active and standby switches will be displayed, together with a virtual switch domain number.

Summary

This topic summarizes the key point that were discussed in this lesson.

Implementing DHCP

Overview

DHCP is a network protocol that enables network administrator to manage and automatic IP configuration assignment. Without DHCP, administrator must manually assign and configure IP addresses, subnet mask, default gateways, and so on, which can, in large environments, become an excessive administrative problem, especially if devices are moved from one internal network to another. In an enterprise environment, a DHCP server is usually a dedicated devices, whereas in smaller deployments or some branch offices, it can be configured on a Cisco Catalyst switch or a Cisco router.

Upon completing this lesson, you will be able to:

- Explain DHCP
- Configure a DHCP server and configure manual bindings
- Configure a DHCP relay
- Configure DHCP options

DHCP Overview

DHCP provides configuration parameters to Internet hosts. It consist of two components: a protocol for delivering host-specific configuration parameter from a DHCP server to a host, and a mechanism for allocating network addresses to hosts. It is built on the client/server model where designated DHCP servers allocate network addresses and deliver and IP configuration parameters to dynamically configured hosts. By default, Cisco multilayer switches that are running Cisco IOS Software include DHCP server and relay agent software.

Distribution multilayer switches often act as Layer 3 gateways for clients that are connecting to the various VLANs of access switches. Therefore, DHCP service can be provided directly by the distribution switches. Alternatively, DHCP services can be concentrated in an external, dedicated DHCP server. In that case, distribution switches must redirect the incoming client DHCP request to external DHCP server.

Exploring DHCP

Overview

In this discover, you will learn how to configure a DHCP service on a switch. You will also configured a manual binding for one of the DHCP clients.

Topology

Device Information

Device	Interface	IP Address
DSW1	VLAN 1	10.0.1.1/24
DSW2	VLAN 10	10.0.10.1/24

Exploring DHCP

Step 1 Access DSW1. Configure a DHCP server for VLAN 10 devices.

After the switch has a Layer 3 address, which is preconfigured in this example, you can configure a DHCP server on the switch. The switch acting as a DHCP server will intercept broad cast packets from client machines within a VLAN.

```
DSW1 (config)# ip dhcp excluded-address 10.0.10.1
DSW1 (config)# ip dhcp pool VLAN10POOL
DSW1 (config-dhcp)# network 10.0.10.0 255.255.255.0
DSW1 (config-dhcp)# default-router 10.0.10.1
DSW1 (config-dhcp)# lease 2
```

Command	Description
ip dhcp excluded-address start-ip end-ip	If there are addresses within the IP subnet that should not be offered to DHCP clients, this command will make sure that the specified addresses are not offered. In the example, 10.0.10.1 was excluded from the DHCP pool because this is the IP address of the Layer 3 interface on DSW1
ip dhcp pool pool-name	The pool-name parameter defines a DHCP pool. Using this command, you enter the DHCP configuration mode.
network ip-address subnet-mask	Specifies the address range through the IP subnet and subnet mask. The network command will bind the DHCP

	server to a matching Layer 3 interface. In the example, the DHCP server "VLAN10POOL" is bound to the "VLAN 10" interface. Broadcast and network IPs are not offered to clients. You can assign multiple subnets per pool.
default-router ip-address [ip-address2] address3] …	Sets the default router address that will be offered to [ip-offered to clients. The example uses the IP address of the Layer 3 interface on the switch.
Lease {infinite | {days [hours[minutes]]}}	Sets the IP address lease duration. By default, the IP address is leased to a client for 1 day. In the example, it is set to 2 days.

Step 2 On DSW1, verify the configured DHCP pool using the show ip dhcp pool command.

```
DSW1# show ip dhcp pool

Pool VLAN10POOL :
Utilization mark (high/low)          :100 / 0
Subnet size (first/next)             : 0 / 0
Total addresses                      : 254
Leased addresses                     : 0
Excluded addresses                   : 1
Pending event                        : none
1 subnet is currently in the pool    :
Current index        IP address range                    Leased/Excluded/Total
10.0.10.1            10.0.10.1   -   10.0.10.254         0     /   1     /   254
```

Notice that no addresses are leased to the clients right now.
Excluded IP addresses are not part of the show ip dhcp pool output.

Step 3 Enable DHCP packet debugging on DSW1.

```
DSW1# debug ip dhcp server packet
DHCP server packet debugging is on.
```

Step 4 Configure PC1 interface Ethernet 0/0 to acquire an IP address via DHCP and observe the CLI output on DSW1.

The port on SW1 to which PC1 is connected is already assigned to VLAN 10, so PC1 will get an IP address from the VLAN 10 subnet.

PC1 (config)# interface ehternet 0/0
PC1 (config-if)# ip address dhcp
PC1 (config-if)# no shutdown

As soon as you enable the interface on PC1, it will send a broadcast, requesting an IP address.

DSW1#
*Oct 3 11:21:52.364: %SYS-5-CONF_I: Configured from console by console
DSW1#
*Oct 3 11:23:09.256: DHCPD: Reload workspace interface Vlan10 tableid 0.
*Oct 3 11:23:09.256: DHCPD: tableid for 10.0.10.1 on Vlan10 is 0.
*Oct 3 11:23:09.256: DHCPD: client's VPN is
*Oct 3 11:23:09.256: DHCPD: using received relay info.
*Oct 3 11:23:09.256: DHCPD: DHCPDISCOVER received from client 0063.6973.636f.2d61.6162
622e.6363.3030.2e34.3830.302d.4574.302f.30 on interface Vlan10.
*Oct 3 11:23:09.256: DHCPD: using received relay info.
DSW1#
*Oct 3 11:23:11.265: DHCPD: Sending DHCPOFFER to client 0063.6973.636f.2d61.616
w.622e.6363.3030.2e34.3830.302d.4574.302d.4574.302f.30 (10.0.10.2)
*Oct 3 11:23:11.265: DHCPD: on option 125
*Oct 3 11:23:11.265: DHCPD: broadcasting BOOTREPLY to client aabb.cc00.4800.
*Oct 3 11:23:11.265: DHCPD: Reload workspace interface Vlan10 tabled 0.
*Oct 3 11:23:11.265: DHCPD: tableid for 10.0.10.1 on Vlan10 is 0
*Oct 3 11:23:11.265: DHCPD: client's VPN is.
*Oct 3 11:23:11.265: DHCPD: DHCPREQUEST received from client 0063.6973.636f.2d6
1.6162.622e.6363.3030.2e34.3830.302d.4574.302f.30.

The debug shows you the whole DHCP negotiation process.

DHCP Negotiation

In the DHCP process, the client sends a DHCPDISCOVER broadcast message to locate a Cisco IOS DHCP server. A DHCP server offers configuration parameters to the client in a DHCPOFFER unicast message. Typical configuration parameters are an IP address, a domain name, and a lease for the IP address.

A DHCP client may receive offers from multiple DHCP servers and can accept any one of the offers; however, the client usually accepts the first offer that it receives. Additionally, the offer from the DHCP server is not a guarantee that the IP address will be allocated to the client;

however, the server usually reserves the address until the client has had a chance to formally request the address.

The client returns a formal request for the offered IP address to the DHCP server in a DHCPREQUEST broadcast message. The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client.

In addition to these four messages, you can also see these DHCP messages with debug output:

- **DHCPDECLINE:** This message sent from the client to the server indicates that the address is already in use.
- **DHCPNAK:** The server sends a refusal to the client for its request for configuration.
- **DHCPRELEASE:** The client tells a server that it is giving up a lease.
- **DHCPINFORM:** A client already has an IP address but is requesting other configuration parameters that the DHCP server is configured to deliver,such as DNS address.

Step 5 Configuration PC2 and PC3 to obtain an IP address through DHCP.

```
PC2(config)# interface etherner 0/0
PC2(config-if)# ip address dhcp
PC2(config-if)# no shutdown

PC3(config)# interface ethernet 0/0
PC3(config-if)# ip address dhcp
pC3(config-if)# no shutdown
```

Step 6 On DSW1, investigate the DHCP binding table.

```
DSW1# show ip dhcp binding
Binding# from all pools not associated with VRF:

IP address          Client-ID/                  Lease expiration        Type
                    Hardware address/
                    User name
10.0.10.2           0063.6973.636f.2d61.        Oct 05 2013 03:23 AM    Automatic
                    6162.622e.6363.3030.
                    2e34.3830.302d.4574.
                    302f.30
```

10.0.10.3 0063.6973.636f.2d61. Oct 05 2013 04:04 AM
Automatic
6162.622e.6363.3030.
2e34.3830.302d.4574.
302f.30

10.0.10.4 0063.6973.636f.2d61. Oct 05 2013 04:04 AM
Automatic
6162.622e.6363.3030.
2e34.3830.302d.4574.
302f.30

Notice that the DHCP server leased three IP address.
You could also verify that the three clients acquired IP addresses by issuing the show ip interface brief command on each client.

Note:
There are times when a manually assigned IP address is preferred. For example, it is beneficial for your server to have an IP address that does not change.

Because you are using DHCP and assigning all IP addresses from a control point, it would be efficient if you could also assign a specific address to a specific device. You can do that with DHCP.

Step 7 Find out the client identifier of PC3.
When a cisco router sends a DHCP Discover message, it will include a client identifier to uniquely identify the device. You can use this value to configure a static binding.

DSW1# **show ip dhcp binding 10.0.10.4**

IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
10.0.10.4	0063.6973.636f.2d61. 6162.622e.6363.3030. 2e34.3830.302d.4574. 302f.30	Oct 05 2013 04:04 AM	Automatic

If you do not like this long client identifier, you can also assign PC3 to use the MAC address as the client identifier. You can do so by using the **ip address dhcp client-id Ethernet 0/0** command.

Step 8 On DSW1, clear the IP DHCP binding table.

If you already have a binding for a client and you want to manually set its IP address, you have to

Clear the DHCP binding table.

DSW1# **clear ip dhcp binding 10.0.10.4**

You could also delete all automatic address binding. Because you will manually set only the IP

Address for PC3, you only need to delete its current IP address from the binding table.

Step 9 On DSW1, assign an IP address of 10.0.10.200 to PC3.

You might have examples where it is necessary for a client to have the same IP address all the

Time because of some application requirements.

DSW1(config)# **ip dhcp pool client 3**
DSW1(dhcp-config)# **host 10.0.10.200 255.255.255.0**
DSW1(dhcp-config)#**client-identifier**
0063.6973.636f.2d61.6162.622e.6363.3030.2e30.3630.302d.4574.302f.30

To configure a manual binding, you first need to create a host pool, then specify the IP address

Of the client and client identifier. Only a client with the specified client identifier will be Assigned this IP address.

At this moment, Client3 will not acquire the specified IP address. Client3 will only request an IP

Address after its lease expires or if it request a renewal.

Note
Some devices, usually those running Linux, do not send client identifiers with DHCP messages. In these cases, you can bind an IP address to a device using the client MAC address. Instead of using the **client-identifier** number command, use the **hardware-address** MAC-address command.

Step 10 Force PC3 to request a new lease from the DHCP server.

PC3(config)# **interface Ethernet 0/0**

PC3(config-if)# **shutdown**
PC3(config-if)# **no shutdown**
*Oct 3 18:25:17.680: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP address 10.0.10.200, mask 255.255.255.0, hostname PC3

You are notified that the client acquired the address 10.0.10.200, the IP address to which it was

Bound to by using the **client-identifier** identifier command.

DHCP Relay

The DHCP service does not have to reside directly on the multilayer switch. Many network use a centralized DHCP server, in this case, the multilayer switch can redirect DHCP request to the corporate DHCP server.

In this configuration , serval elements are involved:

- The multilayer switch must have a Layer 3 IP address that will receive the client DHCP request. This address may be a router port or an SVI.
- An **ip helper-address** command must be configured on the multilayer switch Layer 3 interface.

When the switch receive a DHCP request in the form of broadcast message from a client, the switch forwards this request, as a unicast message, to the IP address that is specified in the **ip helper-address** command. With this feature, the switch relays the dialog between the DHCP client and the DHCP server.

DHCP Options

Advanced configuration parameter and other control information are carried in tagged data items, also known as DHCP options.

You can use DHCP option to “expand” the basic DHCP commands. For example, the **lease** command is one of the basic command that is used to set the duration of lease validity. With DHCP option, you can modify the behavior of leasing out IP addresses. For example, you can change the lease renewal time using the **dhcp-renewal-time** option.

Using option, you can also provide clients with additional information that cannot be passed down to the clients through basic configuration.

Some common examples include the following:

- Option 43: Vendor-encapsulated options, which enable vendors to have their own list of options on the server. For example, you can use it to tell a lightweight AP where the WLC is.
- Option 69: SMTP server, if you want to specify available SMTP servers to the client.
- Option 70: POP3 server, if you want to specify available POP3 server to the client.
- Option 150: TFTP server, which enables your phones to access a list of TFTP server.

Summary

This topic summarizes the key points that were discussed in this lessons