

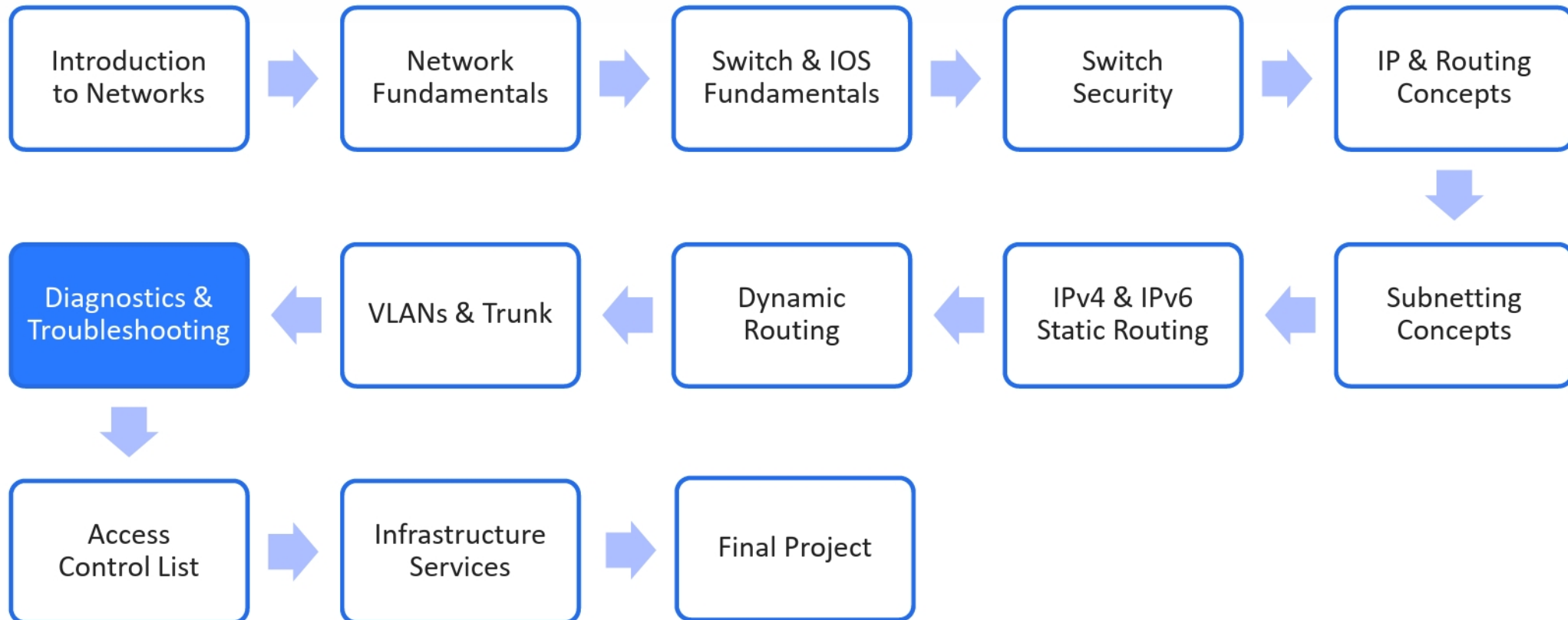
3D RENDERING PERSPECTIVE DESIGN VIEW

Cybersecurity Professional Program

Diagnostics & Troubleshooting

Computer Networking

Course Path



Overview

Lesson Objective

The object of this lesson is to understand how to diagnose network issues and troubleshoot them.

The lesson also introduces useful tools for troubleshooting and explains how CDP works, what log events are, syslog server operation, and the Network Time Protocol.



Troubleshooting Methods

Neighbor Discovery Protocols

Log Events & Syslog Server

Network Time Protocol

Diagnostics & Troubleshooting

Troubleshooting Methods

Troubleshooting Overview

What We Will Learn



Issues can and will arise, even in networks that were designed using the most advanced technologies.

This lesson covers the ways network issues can be resolved and the tools that can help resolve them quickly and efficiently.

An important aspect of network troubleshooting, also described in this lesson, is the usage of discovery protocols.



Troubleshooting

Documentation



Quick and efficient troubleshooting is based, in part, on continuous and detailed network-related documentation.



What Does Documentation Include?



Network documentation includes the following: physical and logical topological diagrams, network and end-device backup configuration files, IP and MAC addressing schemes, and network performance baselines.



Troubleshooting Steps

Gather Information

The first and most important step is gathering information and symptoms from network devices, end systems, and users.

1

Implement a Solution

Consider the severity of the problem and the impact of the solution. Then, begin planning, testing, and documenting possible solutions.

3

Documentation

Document every step you took in the process for future reference.

5

Isolate the Problem

Based on the symptoms, eliminate variables until a single problem or a set of related problems is identified as the cause.

2

Problem Solved?

If the problem was not solved, repeat steps two and three again and deepen the research.

4

Gathering Information

01

Question end users

02

Protocol analyzers
(Wireshark, etc.)

03

Physical troubleshooting tools
(cable tester, others)

04

Network
management software

CMD network commands

05

show and ***debug*** commands

06

IP SLA: monitors network
performance in real-time

07

Neighbor Discovery Protocols

08

Open Systems Interconnection (OSI) Troubleshooting Methods

Bottom-Up



In this method, the starting point is at the bottom of the OSI model: the physical layer.

The examination starts from the network's infrastructure, such as cables and NICs.

Top-Down



In this method, the starting point is at the top of the OSI model: the application layer.

The examination starts from the application itself.

Divide & Conquer



In this method, the starting point is not predefined as in the other methods.

A particular layer is selected and examined; if the layer functions, then the next layer to examine is the one above it. If the layer is faulty, then the next one should be the one below it.

Software Tools

Software Troubleshooting Tools



Network Management Software (NMS) provides excellent tools for troubleshooting.

NMS continuously monitors network activity and establishes a clear baseline for reference purposes. This enables network administrators to promptly identify issues, and, in some cases, even predict the occurrence of such issues.



Top IOS Show Commands

show interfaces

1

show interfaces outputs a large volume of information, including interface errors, bandwidth utilization, and interface speed.

show ip route

2

show ip route verifies network reachability. It will indicate if routing protocols are operating as they should.

show ip interface brief

3

show ip interface brief presents only information about interfaces associated with the IP protocol. The command outputs a detailed summary of interface status and IP addresses.

show running-config

4

show running-config displays the complete device configuration that is being used at that time.

show startup-config

5

show startup-config displays the complete device configuration that is being used when it loads.

Extended *ping* & *traceroute* Commands

Extended Ping



Extended *ping* is used to perform advanced checks of network connectivity. It is also able to change the source IP on the packet leaving the router.



Traceroute



The *traceroute* command discovers the path packets take to a remote destination and where routing failures occur.



Extended Ping Example

```
R2#ping
Protocol [ip]:
Target IP address: 172.16.1.2
Repeat count [5]: 6
Datagram size [100]: 150
Timeout in seconds [2]: 4
Sending 6, 150-byte ICMP Echos to
172.16.1.2, timeout is 4 seconds:
!!!!!!
Success rate is 100 percent (6/6),
round-trip min/avg/max = 0/0/3 ms
```



Diagnostics & Troubleshooting

Neighbor Discovery Protocols

CDP Overview

Cisco Discovery Protocol



CDP (Cisco Discovery Protocol) is a Layer 2 Cisco proprietary protocol enabled by default on all Cisco devices. Its purpose is similar to the purpose of NDP.

CDP can be disabled on specific devices or interfaces for security reasons.



CDP Characteristics

Eavesdropping



Since CDP does not encrypt transmitted data, it is vulnerable to reconnaissance-type attacks (such as Sniffing).

Such attacks will allow the attacker to map the victim's network and more.

Information Gathering



CDP gathers information on the local device and periodically sends it to all directly connected devices.

Advertisements

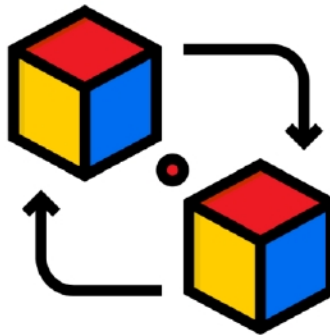


CDP advertisements are special packets that reveal device details to neighbors also running CDP.

When advertisements are received, they are stored in the neighbor table.

CDP Advertisement

CDP Packets



CDP includes the following data in advertised packets:

- Type of device (router, switch)
- Device name
- Interconnected interfaces
- IOS version
- Next-hop IP
- Connection's duplex mode (full, half)



Mismatch Detection

Mismatch Error Detection



CDP includes a unique feature that can detect a protocol-connection mismatch.

When such a mismatch is detected, CDP notifies the network administrator by recording the incident in a log.

Examples of mismatch types include:

- Native VLAN mismatch
- Duplex mismatch



CDP Intervals

CDP Packet Timer



CDP sends advertisement packets every **60 seconds** by default to all directly connected devices.



CDP Hold Timer



If a device does not receive CDP packets from a neighbor for **180 seconds**, it will consider that neighbor "dead" and remove it from its neighbor table.



CDP Show Command Output

```
S1#show cdp
Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled
```



The timers can be modified.

CDP Configuration

Command

```
cdp run \ enable
```



Because CDP is not secure or encrypted, it is easy to eavesdrop. If necessary, the protocol can be turned off entirely on the device or on selected interfaces.

Recommended: Enable CDP only for port interconnection with other network devices.

Command Examples

#Enable\Disable on Device:

```
S1(config)#cdp run  
S1(config)#no cdp run
```

#Enable\Disable on Port:

```
S1(config)#interface range fastEthernet 0/1-24  
S1(config-if-range)#cdp enable  
S1(config-if-range)#no cdp enable
```



CDP Usage

The `show cdp neighbors` command displays all connected devices that CDP can communicate with.

The `show cdp neighbors detail` command displays more information on each device, such as IP address and IOS version.

Example Topology



Command Output on S1

```
S1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce    Holdtme    Capability    Platform    Port ID
R1               Gig 0/1          127        R             C1900       Gig 0/0
```

LLDP

Link Layer Discovery Protocol



LLDP is a Neighbor Discovery Protocol similar to CDP that was developed by the IEEE.

LLDP is an industry standard protocol, meaning it is not proprietary and can operate on any network device, and even on PCs and servers. Although LLDP is not enabled by default on Cisco devices, it is fully supported.



LLDP Intervals

LLDP Packet Timer



LLDP sends advertisement packets every **30 seconds** by default to all directly connected devices.



LLDP Hold Timer



If a device does not receive LLDP packets from a neighbor for **120 seconds**, it will consider that neighbor "dead" and remove it from its neighbor table.



LLDP Show Command Output

```
S1#show lldp
Global LLDP Information:
Status: ACTIVE LLDP advertisements are
sent every 30 seconds
LLDP hold time advertised is 120 seconds
```



The timers can be modified.

LLDP Configuration

Command

```
lldp run \ receive \ transmit
```



LLDP is also not secure or encrypted, like CDP. If necessary, it can be turned off entirely on the device or for a specific **direction** on selected interfaces.

Recommended: Enable LLDP only on ports interconnected with other network devices.

Command Examples

#Enable\Disable on Device:

```
S1(config)#lldp run  
S1(config)#no lldp run
```

#Enable\Disable on Port:

```
S1(config)#interface range fastEthernet 0/1-24  
S1(config-if-range)#lldp transmit  
S1(config-if-range)#no lldp transmit  
S1(config-if-range)#lldp receive  
S1(config-if-range)#no lldp receive
```



LLDP Usage

LLDP **show** commands are similar to CDP **show** commands but can display additional information.

The commands include *show lldp neighbors* and *show lldp neighbors detail*.

Example Topology



Command Output on S1

```
S1#show lldp neighbors
```

Capability codes:

(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device

(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID	Local Intf	Hold-time	Capability	Port ID
R1	Gig0/1	120	R	Gig0/0

Total entries displayed: 1



Diagnostics & Troubleshooting

Log Events & Syslog Server

Overview

What Is Syslog?



Syslog is a standard for logging messages.

Each device records actions and events that occur like a private diary.

Among other tasks, network administrators need to monitor the network to ensure smooth, errorless functionality.

Monitoring the network improves troubleshooting capability and helps identify issues such as device health and network load.



The syslog protocol is documented in RFC 5424.

System Log Events

Why Are Logs Useful?



System notification logging increases a network administrator's awareness of hardware or software malfunctions, service status, and security accountability.

In some cases, logs can be used to predict component failures.

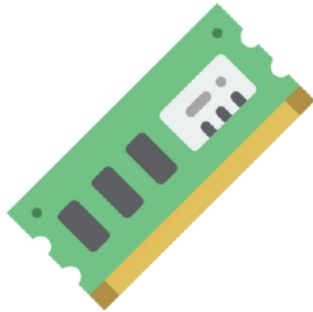
Log analysis can help administrators troubleshoot the system and can be useful to information security experts when investigating security breaches.



Syslog messages can be stored locally on the device or on a syslog server in the network.

Device Logs

Log Storage



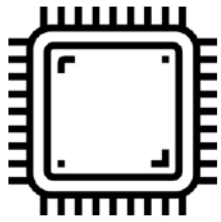
Log storage takes up space, and can, in some cases, degrade system performance.

- Log message count is limited due to buffer size.
- Collecting logs from separate devices can take a long time.
- RAM is erased upon device power off.



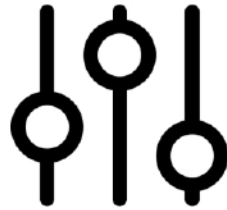
Syslog Storage Methods

Logging Buffer



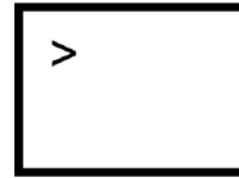
A logging buffer is a predetermined storage space allocated on RAM for syslog messages.

Console Line



Console line is a method of viewing messages locally via the console window.

Terminal Line



Terminal line is a method of viewing messages via a CLI program (such as Putty).

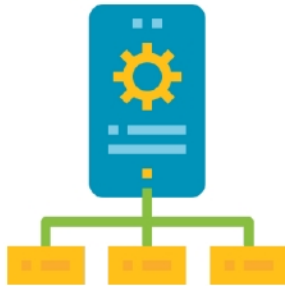
Syslog Server



If a syslog server is configured on the device, the device will send all syslog messages to the server over the UDP 514 port.

Syslog Server

What Is a Syslog Server?



A syslog server is a computer that runs syslog software.

The syslog software concentrates logs from all devices (PC, router, etc.) on the network into one centralized location, which makes management and log backup easier.

It also offers a convenient user interface.

This way of working is more efficient than storing logs in RAM.



Many free and enterprise versions of syslog exist, such as the Kiwi Syslog Viewer.

Severity & Facility

Syslog messages include several pieces of information, of which the most important are:

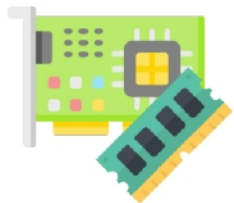
Message Severity



The urgency of the log message is represented by its severity level, which is a number value from 0 to 7. Level 0 indicates emergencies, and 7 indicates system debugging. The values also represent critical malfunctions and system warnings.



Message Facility



The facility parameter indicates the source that generated the message, which, for example, can be a network card or routing protocol. The facility can be a hardware component, protocol, or system service.



Syslog Message Severity Levels

The following table lists syslog severity levels with their number values. The lower the number, the higher the severity.

Severity Levels

Message Type	Severity Level	Explanation
Emergency	Level 0	System unusable
Alert	Level 1	Immediate action is required
Critical	Level 2	Critical condition
Error	Level 3	Error condition
Warning	Level 4	Warning condition
Notification	Level 5	Normal, but important
Information	Level 6	Informative message
Debugging	Level 7	Debugging message



Log Message Format

Log Event

```
*Dec 28 19:01 | %LINK | -5- | CHANGED: | Interface GigabitEthernet0/1, changed state to up |
```

1 2 3 4 5



1. **Timestamp:** records the time and date of the log (this service is disabled by default and should be enabled once so the system has the correct time info)
2. **Facility:** The category of the source that created the log message. In the example above, **link** represents the state of the router's hardware ports.
3. **Severity:** The severity level, which, in the example above, indicates that it is a notification message.
4. **Mnemonic:** a device-specific code that identifies the log message
5. **Text Description:** the log/event description and other details

Enable Gig0/1 Log

```
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#no shutdown
*Dec 28 19:01 %LINK-5-CHANGED: Interface
GigabitEthernet0/1, changed state to up
```



Syslog Configuration Commands

Typical configuration commands used to set up syslog on a Cisco device:

Cisco Syslog Commands

Command	Description
<i>logging host</i>	Sets the destination syslog server
<i>logging trap</i>	Determines what log severity levels to send to the server
<i>service timestamps log datetime msec</i>	Attaches time information to the alerts
<i>logging console</i>	Shows system messages on the screen of the console connection (enabled by default)
<i>terminal monitor</i>	Shows system messages on the screen of a remote connection (Telnet, SSH)
<i>login buffered</i>	Saves system messages to the RAM (enabled by default)



Syslog Config Example

The **logging host** command sets the destination IP of the syslog server, to which all logs are sent.

The **logging trap** command sends all severity log levels to the server (levels 7 and above).

The remaining commands in the example on the right are used to add time records.

Set Logging to Syslog Server on R1

```
R1(config)#logging host 172.16.0.250
R1(config)#logging trap debugging
R1(config)#logging userinfo
R1(config)#service timestamps log datetime msec

R1(config)#do show logging
<Output Omitted>
ESM: 0 messages dropped
  Trap logging: level debugging, 9 message lines logged
  Logging to 172.16.0.250 (udp port 514, audit disabled,
    authentication disabled, encryption disabled, link up),
    2 message lines logged,
    0 message lines rate-limited,
    0 message lines dropped-by-MD,
    xml disabled, sequence number disabled
    filtering disabled
```



Diagnostics & Troubleshooting

Network Time Protocol



NTP Overview

What is NTP?



NTP (Network Time Protocol) is responsible for the synchronization of the time and date across all devices on the network.

NTP is a simple client-server protocol and is implemented in networks everywhere.

It is very easy to set up and even has an authentication mechanism for security.



NTP operates on UDP port 123 and is defined in RFC 1305.

Time Configuration

Date and time for network devices can be set in one of two ways:

Manual Configuration



This method requires manual setting of the time and date on each device on the network.

It is not recommended to work this way for various reasons, among which is the lack of scalability for large networks. (Setting the clock in every device will waste valuable time.)



Automatic Configuration



This method requires an available and configured NTP server.

Only the server's IP address needs to be set on network devices.

This ensures that all devices on the network will be set to the most accurate time and date automatically.

Cisco routers can be configured to act as NTP servers.



NTP Operation

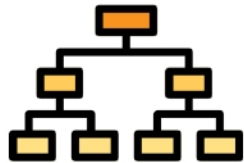
NTP Usage



Cisco routers and switches (and many other devices around the world) use NTP to determine the date and time, although routers and switches can also act as NTP servers.



Stratum Model



Stratum levels define the distance from high-precision reference clocks, which begin with stratum 0, to devices connected hierarchically. Servers linked to the reference clock are stratum 1, devices that receive the time from the servers are stratum 2, and so on. To avoid delays, a maximum of 15 levels are allowed.



Services



Accurate time settings are crucial for many protocols and device functions. For example, DHCP leases and syslog events are time-sensitive services. Timestamps are extremely important for troubleshooting, management, and network security.



Manual Time and Date Setting

Command

```
clock set <hh:mm:ss> <day> <month-name> <year>
```



Set R1 Time Settings

```
R1#clock set 09:21:14 16 January 2019
```



Setting the clock manually has two drawbacks: a device can get out of sync if it is shut down, and setting every device clock can waste valuable time.

NTP Configuration

To make R1 set the clock with an external NTP server, use the **ntp server** command together with the server's IP.

Verify the device time information using the **show clock** command or **show ntp status**.

Once the device clock is tuned correctly, run **log timestamp**, which logs device messages and events with a time and date.

Enable NTP on R1

```
R1(config)#ntp server 10.0.0.250
R1(config)#do show clock
18:58:46.855 UTC Sat Dec 28 2019

R1(config)#service timestamps log datetime msec
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#no shutdown
*Dec 28 19:01:46:100 %LINK-5-CHANGED: Interface GigabitEthernet0/1,
changed state to up
```



NTP Master

Command

```
ntp master <1-15>
```



Set R1 as NTP Server

```
R1(config)#ntp master
```

```
R1(config)#do show run ntp
```



A network device such as a router or switch can act as an NTP server. The main command requires only a stratum value and the number of hops from an accurate time source (such as an atomic clock).

Lab NET-10-L1

Configure NTP and Syslog
30–60 Min.



Mission

The objects of this lab are to answer questions based on material covered in the lesson and understand how to configure NTP and syslog servers.

Steps

- Answer the questions.
- Configure Syslog.
- Configure NTP.

Environment & Tools

- OS: All platforms
- Tools: Cisco Packet Tracer 7.2.2 or higher

Related Files

- Lab document
- *NET-10-L1.pka*



QUESTIONS?



THANK YOU
