Chapter 1 – Introduction to Network Maintenance
Objectives

- Describe network maintenance tasks
- Explain the difference between proactive and reactive network maintenance.
- Describe well-known network maintenance models.
- Identify common maintenance procedures.
- Describe tools required for network maintenance.

Maintenance Tasks

- *Device installation and maintenance:* Includes tasks such as installing devices and software and creating and backing up configurations and software.

- *Failure response:* Includes tasks such as supporting users that experience network problems, troubleshooting device or link failures, replacing equipment, and restoring backups.

- *Network performance:* Includes tasks such as capacity planning, performance tuning, and usage monitoring.

- *Business procedures*: Includes tasks such as documenting, compliance auditing, and service level agreement (SLA) management.

- *Security:* Includes tasks such as following and implementing security procedures and security.

Interrupt Driven Maintenance

- The most basic method of performing network maintenance, involves *responding* to problems as they arise (reactive).
- Disadvantages, including the following:
  - Tasks that are *beneficial* to the long-term health of the network might be ignored, *postponed*, or *forgotten*.
  - Tasks might not be executed in order of *priority* or *urgency*, but instead in the order they were requested.
  - The network might experience more downtime than necessary because problems are not prevented.

Structured Maintenance

- Structured network maintenance *predefines* and *plans* much of the processes and procedures (proactive).

- This proactive approach reduces the *frequency* and *quantity* of problems, and addresses them more *efficiently*.

- The structured approach to network maintenance has some clear benefits over the interrupt-driven approach, including:

  - Reduced network downtime
  - More cost-effectiveness
  - Better alignment with business objectives
  - Higher network security

Standards-Based Maintenance Methodologies

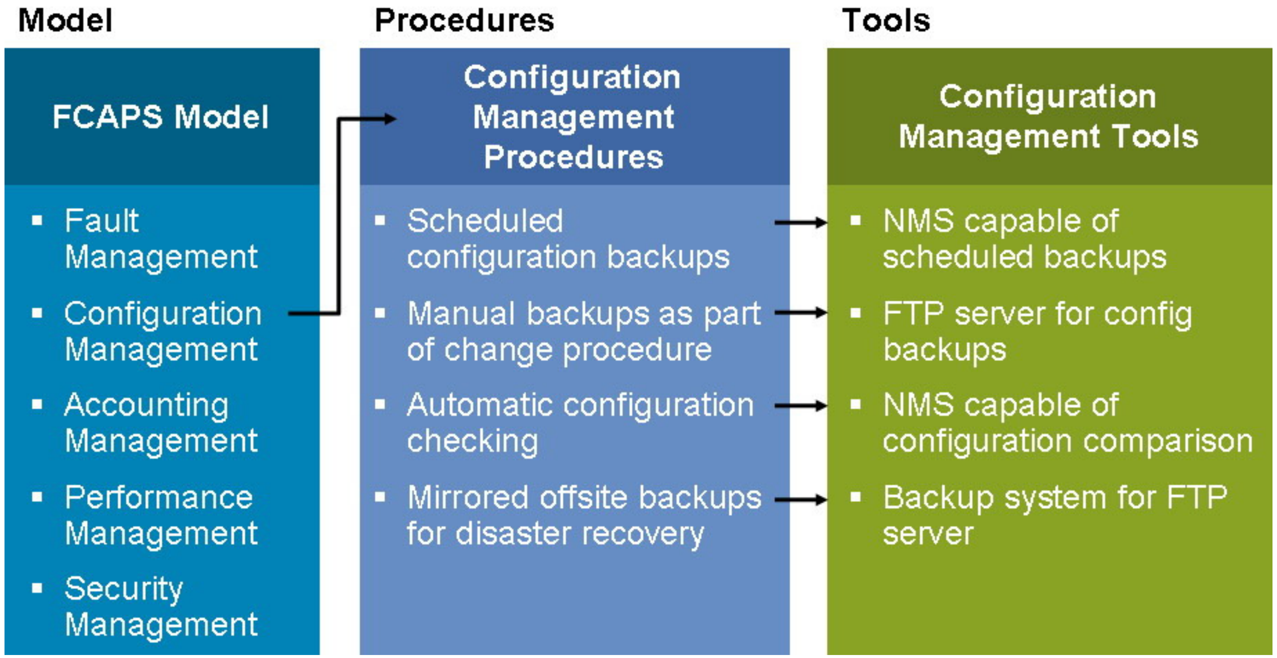
- Several well-known network maintenance methodologies have been defined by a variety of organisations:

1. IT Infrastructure Library (ITIL)
2. FCAPS
3. Telecommunications Management Network (TMN)
4. Cisco Lifecycle Services

- The choice of maintenance methodology will determine the type and variety of maintenance tools required.

Maintenance Procedures & Tools

- *Fault management:* network problems are discovered and corrected.
- *Configuration management:* installation, identification, and configuration of hardware and services.
- *Accounting management:* optimally distribute resources among enterprise subscribers.
- *Performance management:* managing the overall performance of the enterprise network.
- *Security management:* Security management is responsible for ensuring confidentiality, integrity, and availability (CIA).



Model

FCAPS Model

- Fault Management
- Configuration Management
- Accounting Management
- Performance Management
- Security Management

Procedures

Configuration Management Procedures

- Scheduled configuration backups
- Manual backups as part of change procedure
- Automatic configuration checking
- Mirrored offsite backups for disaster recovery

Tools

Configuration Management Tools

- NMS capable of scheduled backups
- FTP server for config backups
- NMS capable of configuration comparison
- Backup system for FTP server

- Upon selection of a network maintenance model, you must translate the theoretical model to *practical* procedures

Network Maintenance Task Identification

All network maintenance plans need to include procedures to perform the following tasks:

- Accommodating adds, moves, and changes.
- Installation and configuration of new devices.
- Replacement of failed devices.
- Backup of device configurations and software.
- Troubleshooting link and device failures.
- Software upgrading or patching.
- Network monitoring.
- Performance measurement and capacity planning.
- Writing and updating documentation.

Network Maintenance Planning

- You must build processes and procedures for performing your network maintenance tasks; this is called network maintenance planning.

- Network maintenance planning includes the following:

1. *Scheduling* maintenance
2. Formalizing *change-control* procedures
3. Establishing network *documentation* procedures
4. Establishing effective *communication*
5. Defining templates/procedures/conventions – standardisation.
6. Disaster Recovery.

Cisco Networking Academy

Scheduled Maintenance

BIRMINGHAM City University

- The benefits of scheduled maintenance include the following:
    - Network downtime is reduced.
    - Long-term maintenance tasks will not be neglected or forgotten.
    - Predictable lead times for change requests.
    - Disruptive maintenance tasks can be scheduled during assigned maintenance windows, reducing downtime during production hours.

Change Control

•In many companies, change control is formalised and answers the following types of questions:

1. Which types of change require authorisation and who is responsible for authorising them?
2. Which changes have to be done during a maintenance window and which changes can be done immediately?
3. What other actions (such as updating documentation) need to be taken after a successful change?
4. What conditions allow skipping some of the normal change procedures and which elements of the procedures should still be followed?

Network Documentation

- Typical elements of network documentation include the following:

1. *Network drawings:* Diagrams of the physical and logical structure of the network.
2. *Connection documentation:* Lists of all relevant physical connections, such as patches, connections to service providers, and power circuits.
3. *Equipment lists:* Lists of all devices, part numbers, serial numbers, installed software versions, (if applicable) software. Licenses, warranty/service information.
4. *IP address administration:* Lists of the IP subnets scheme and all IP addresses in use.
5. *Configurations:* A set of all current device configurations or even an archive that contains all previous configurations.
6. *Design documentation:* This is a document describing the motivation behind certain implementation choices.

Effective Communication

•Communication is *vital* both during troubleshooting and technical support and afterward.

•During troubleshooting, certain questions must be answered, such as the following:

1. Who is making changes and when?
2. How does the change affect others?
3. What are the results of tests that were done, and what conclusions can be drawn?

Standardisation

•One of the ways to streamline processes and make sure that tasks are executed in a *consistent* manner is to define and document procedures; this is called standardization.

•Defining and using templates is an effective method of network documentation, and it helps in creating a consistent network maintenance process:

1. Are logging and debug time stamps set to local time or coordinated universal time (UTC)?
2. Should access lists end with an explicit "deny any"?
3. In an IP subnet, is the first or the last valid IP address allocated to the local gateway?

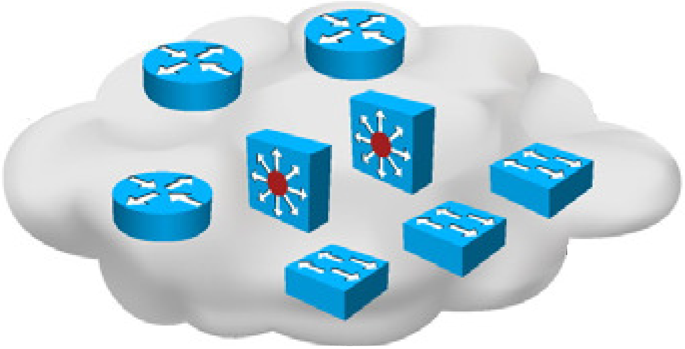
Disaster Recovery

- The quicker you can replace failed devices and restore functionality, the quicker your network will be running again. To replace a failed device, you need the following items:

1. Replacement *hardware*.
2. The current *software* version for the device.
3. The current *configuration* for the device.
4. The *tools* to transfer the software and configuration to the device.
5. *Licenses* (if applicable).
6. Knowledge of the *procedures* to install software, configurations, and licenses.

- Missing any of the listed items severely affects the time it takes to replace the device.

Fundamental Tools & Applications

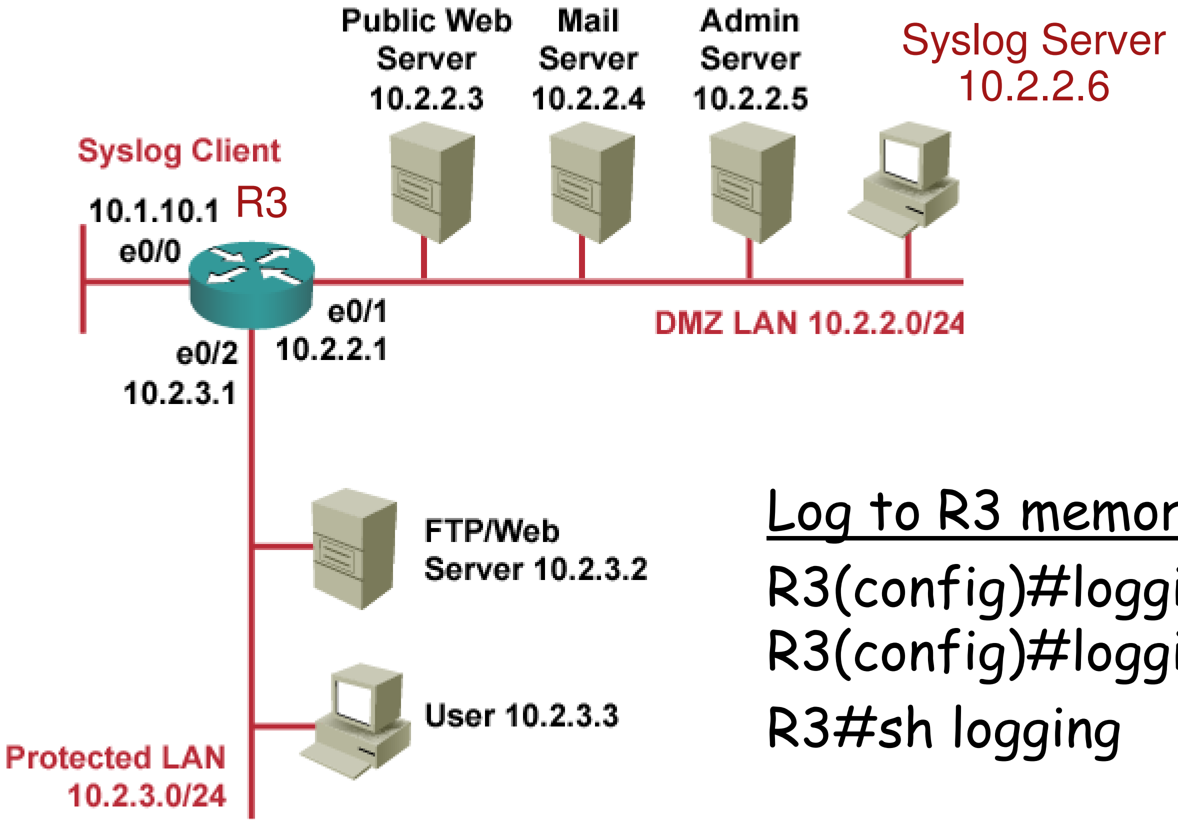


Chapter 1

Cisco Log Severity Levels

Syslog Level and Name	Definition	Example
0 LOG_EMERG	A panic condition normally broadcast to all users	Cisco IOS software could not load
1 LOG_ALERT	A condition that should be corrected immediately, such as a corrupted system database	Temperature too high
2 LOG_CRIT	Critical conditions; for example, hard device errors	Unable to allocate memory
3 LOG_ERR	Errors	Invalid memory size
4 LOG_WARNING	Warning messages	Crypto operation failed
5 LOG_NOTICE	Conditions that are not error conditions but should possibly be handled specially	Interface changed state, up or down
6 LOG_INFO	Informational messages	Packet denied by ACL
7 LOG_DEBUG	Messages that contain information that is normally used only when debugging a program	Packet type invalid

Configure Logging



Log to R3 memory:

```
R3(config)#logging buffered 16384
R3(config)#logging console warning
R3#sh logging
```

Log to Syslog server:

```
R3(config)#logging 10.2.2.6
R3(config)#logging trap informational
R3(config)#logging source-interface loopback 0
R3(config)#logging on
R3(config) #service timestamps log datetime
```

Network Time Protocol (NTP)

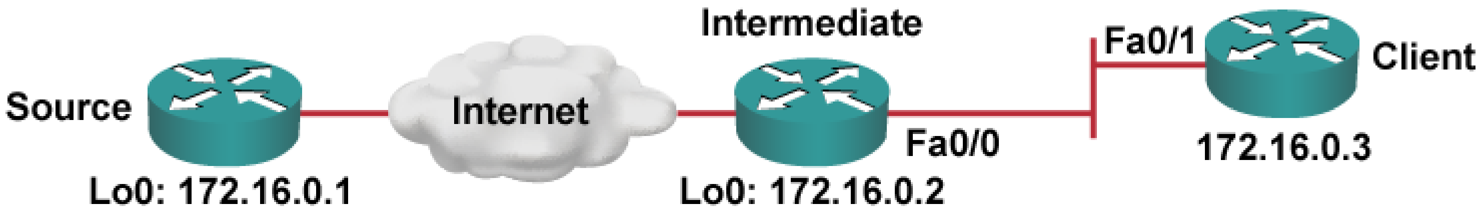
- Many features in a computer network depend on time synchronisation, such as accurate time information in syslog messages, certificate-based authentication in VPNs, ACLs with time range configuration, and key rollover in routing protocol authentication (EIGRP and RIP).
- Most Cisco routers have two clocks: a battery-powered system calendar in the hardware and a software-based system clock - These two clocks are managed separately.
- When a router with a system calendar is initialised or rebooted, the system clock is set based on the time in the internal battery-powered system calendar.
- The system clock can then be set manually or by using the Network Time Protocol (NTP) - an Internet protocol used to synchronise the clocks of network connected devices to some time reference.
- NTP is an Internet standard protocol currently at v3 and specified in RFC 1305.

NTP Configuration

- NTP is extremely efficient; no more than one packet per minute is necessary to synchronise two machines to within 1mS of one another.

- A stratum 1 time server typically has a radio or atomic clock directly attached to the server; a stratum 2 time server receives the time via NTP from a stratum 1 time server, etc, etc.

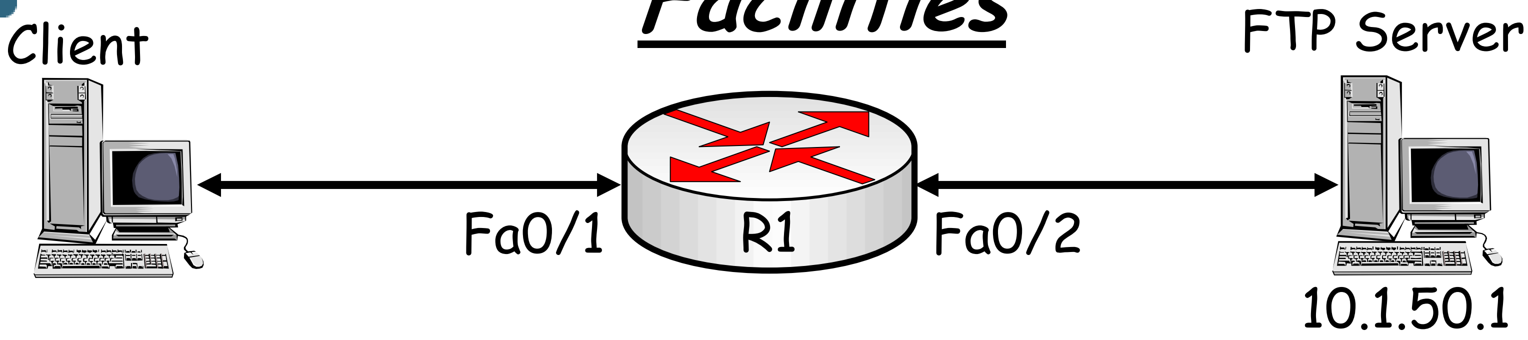
- A machine that runs NTP automatically chooses the machine with the lowest stratum number to communicate with via NTP as the machine's time source.



```
Source(config)#ntp master 5
Source(config)#ntp source loopback 0
Source(config)#clock timezone  cet -1

Intermediate(config)#ntp server 172.16.0.1
Intermediate(config)#ntp source loopback 0
Intermediate(config)#ntp update-calendar
```

Implementing Backup & Restore Facilities



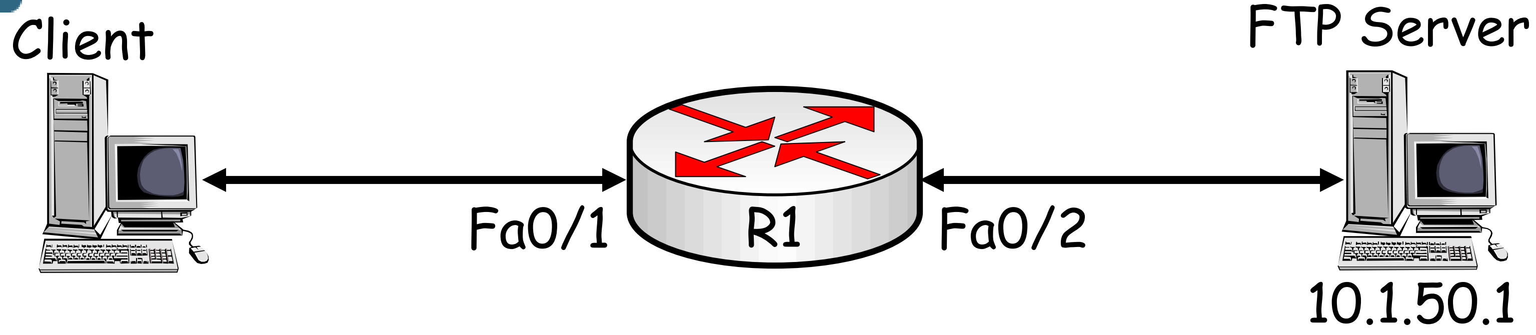
- More-secure protocols such as FTP, SCP, and HTTP or HTTPS can be used as a means of transferring configurations and software.

- To use any of these more-secure protocols, the username and password must be provided to authenticate to the server.

- The username and password are specified by placing the username and password as username:password@ before the server name or IP address in the URL:

```
R1# copy startup-config ftp://backup:san-fran@10.1.50.1/R1-test.cfg
Address or name of remote host [10.1.50.1]?
Destination filename [R1-test.cfg]?
Writing R1-test.cfg !
2323 bytes copied in 0.268 secs (8668 bytes/sec)
```

Username & Password Configuration

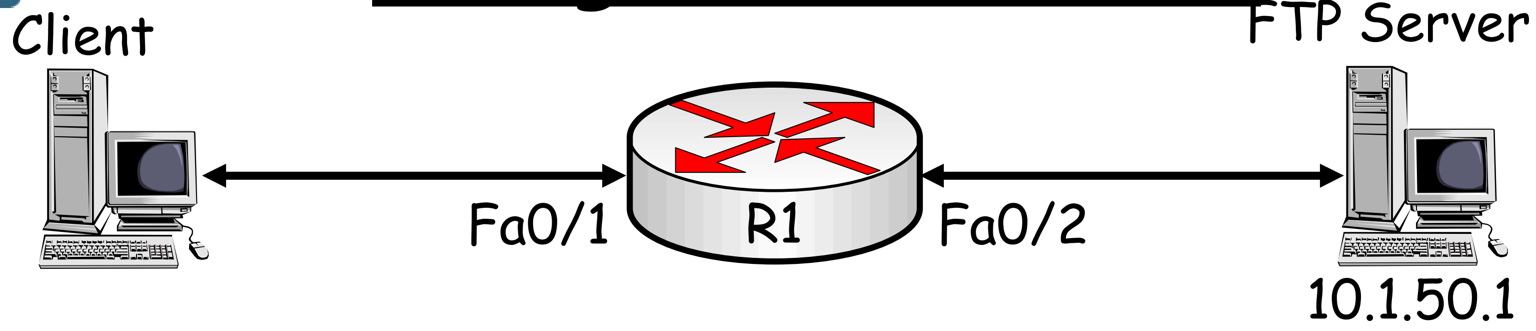


- The username and password can be specified in the configuration, instead of on the command line, for the FTP, HTTP, and HTTPS protocols:

```
R1(config)# ip ftp username backup
R1(config)# ip ftp password san-fran
R1(config)# ip http client username backup
R1(config)# ip http client password 0 san-fran
R1(config)# exit

R1# copy startup-config ftp://10.1.50.1/R1-test.cfg
Address or name of remote host [10.1.50.1]?
Destination filename [R1-test.cfg]?
Writing R1-test.cfg !
2323 bytes copied in 0.304 secs (7641 bytes/sec)
```

Configuration Archive



- The *configuration archiving* feature, part of the Configuration Replace and Configuration Rollback feature can be used to create local or remote configuration archives.

```
R1(config)# archive
R1(config-archive)# path flash:/config-archive/$h-config
R1(config-archive)# write-memory
R1(config-archive)# time-period 10080
```

- Verify the presence of the archived configuration files by using the *show archive* command:

```
R1# show archive
There are currently 2 archive configurations saved.
The next archive file will be named flash:/config-archive/RO1-config-3
Archive # Name
1 flash:/config-archive/RO1-config-1
2 flash:/config-archive/RO1-config-2
```

Configure Replace

- The configure replace command enables you to replace the currently running configuration on the router with a saved configuration without the need to reload:

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# hostname TEST
TEST(config)#
TEST# configure replace flash:config-archive/RO1-config-5 list
This will apply all necessary additions and deletions to replace the current running
configuration with the contents of the specified configuration file, which is
assumed to be a complete configuration, not a partialconfiguration. Enter Y if you
are sure you want to proceed. ? [no]: yes
!Pass 1
!List of Commands:
no hostname TEST
hostname R1
end
Total number of passes: 1
Rollback Done
R1#
```

Chapter 1 – Introduction to Network Maintenance
Objectives

- Describe network maintenance tasks
- Explain the difference between proactive and reactive network maintenance.
- Describe well-known network maintenance models.
- Identify common maintenance procedures.
- Describe tools required for network maintenance.

Any Questions?