Cisco − Change Management: Best Practices White Paper

Table of Contents

Change Management: Best Practices White Paper

Introduction

This document provides a template for change management that promotes high−availability networks. Specifically, the template provides the critical steps for creating a change management process, a high−level process flow for planned change management, an emergency change process flow, and a general method to evaluate the success of your process.

Critical Steps for Creating a Change Management Process

Change management can be divided into two basic areas: planning for change and managing change. These areas are defined as follows.

Planning for Change

Change planning is a process that identifies the risk level of a change and builds change planning requirements to ensure that the change is successful. The key steps for change planning are as follows:

- Assign all potential changes a risk level prior to scheduling the change.
- Document at least three risk levels with corresponding change planning requirements. Identify risk levels for software and hardware upgrades, topology changes, routing changes, configuration changes, and new deployments. Assign higher risk levels to non−standard add, move, or change types of activity.
- The high−risk change process you document needs to include lab validation, vendor review, peer review, and detailed configuration and design documentation.
- Create solution templates for deployments affecting multiple sites. Include information about physical layout, logical design, configuration, software versions, acceptable hardware chassis and modules, and deployment guidelines.
- Document your network standards for configuration, software version, supported hardware, Domain Name System (DNS), and device naming, design, and services supported.

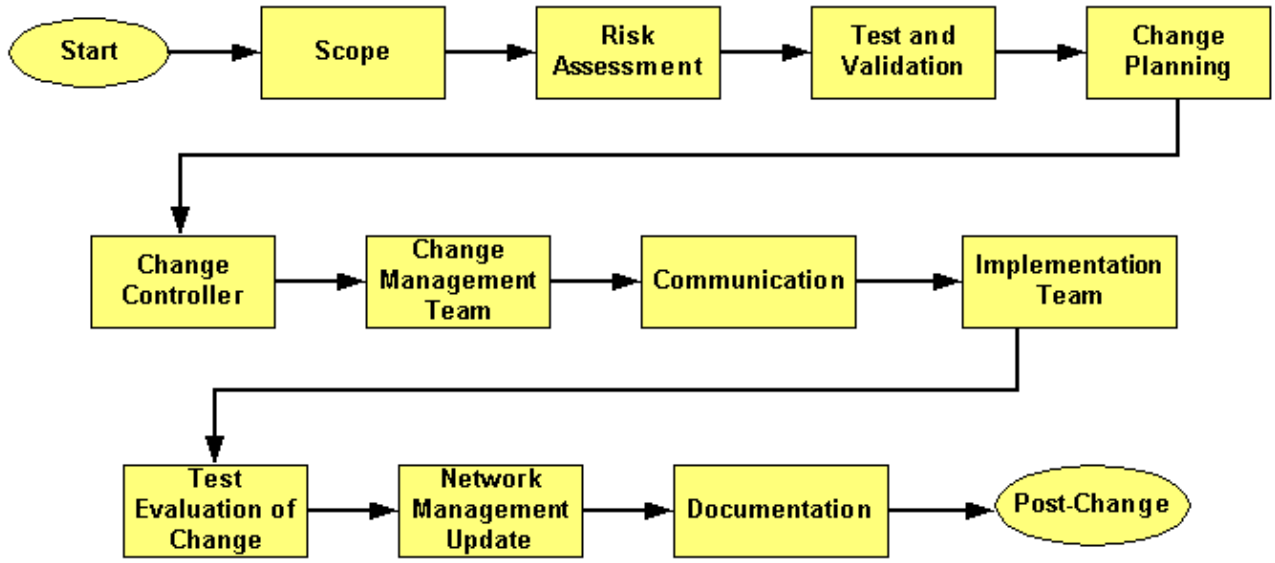
Managing Change

Change management is the process that approves and schedules the change to ensure the correct level of notification and minimal user impact. The key steps for change management are as follows:

- Assign a change controller who can run change management review meetings, receive and review change requests, manage change process improvements, and act as liaison for user groups.
- Hold periodic change review meetings to be attended by system administration, application development, network operations, and facilities groups, as well as general users.
- Document change input requirements, including change owner, business impact, risk level, reason for change, success factors, backout plan, and testing requirements.
- Document change output requirements, including updates to DNS, network map, template, IP addressing, circuit management, and network management.
- Define a change approval process that verifies validation steps for higher−risk change.
- Hold postmortem meetings for unsuccessful changes to determine the root−cause of change failure.
- Develop an emergency change procedure that ensures an optimal solution is maintained or quickly restored.

High−Level Process Flow for Planned Change Management

The different steps you'll need to follow during a network change are represented in this basic flow. Click each box for more information about that step:



Scope

The scope of a proposed change should include a complete technical definition and the intent or purpose of the change. In addition, the person or department requesting the change should include information describing who will be affected, both during the change period and after deployment. This may include business units, user groups, servers, and applications. In general, most changes can be categorized as one of the following:

- Network expansion

- Addition of LAN segments at existing site(s)
- Addition of new sites
- Connection to existing networks
- Connection to the Internet
- Corporate mergers and acquisitions
- Design and feature enhancements
- Software release upgrade
- Host software
- Distributed client software
- Configuration changes
- Support for additional protocol(s)
- Implementation of enhanced features

Risk Assessment

Every network change has an associated risk. The person requesting the change should assess the risk level of the change. Modeling the change in a lab environment or with a network modeling tool can also help assess the risk of a change. We recommend assigning one of the following risk categories to each change request:

- **High−risk** These network changes have the highest impact on user groups or particular environments, and may even affect an entire site. Backing out of the change is time consuming or difficult. You should research high−risk changes using the tools available on the Cisco Technical Assistance Center web site, including the , and implement the change in conjunction with Cisco support personnel. Make sure management is aware of the change and its implications, and notify all users.

- **Moderate−risk** These network changes can critically impact user environments or affect an entire site, but backing out of the change is a reasonably attainable scenario. You should research moderate−risk changes using tools such as the , and possibly review the change with Cisco support personnel. We recommend notifying all users of a moderate−risk change.

- **Low−risk** These network changes have minor impact on user environments and backing out of the change is easy. Low−risk changes rarely require more than minimal documentation. User notification is often unnecessary.

You may choose to have additional risk levels to help identify the correct level of testing and validation undertaken prior to a change. The following table shows five different risk levels that help identify testing and validation requirements.

Risk Level	Definition
1	High potential impact to large number of users (500+) or business−critical service because of introduction of new product, software, topology, or feature; change involves expected network downtime.
2	High potential impact to large number of users (500+) or business−critical service because of a large increase of traffic or users, backbone changes, or routing changes; change may require some network downtime.
3	Medium potential impact to smaller number of users or business service because of any non−standard change, such as new product,

	software, topology, features, or the addition of new users, increased traffic, or non standard topology; change may require some network downtime.
4	Low potential impact, including adding new standard template network modules (building or server switches, hubs, or routers); bringing up new WAN sites or additional proven access services; and all risk level 3 changes that have been tested in the production environment. Change may require some network downtime.
5	No user or service impact, including adding individual users to the network, and standard configuration changes such as password, banner, Simple Network Management Protocol (SNMP), or other standard configuration parameters; no expected network downtime.

Test and Validation

Once you've assessed the risk level of the potential change, you can apply the appropriate amount of testing and validation. The table below demonstrates how testing and validation may be applied to the five−level risk model.

Risk Level	Testing and Validation Recommendations
1	Requires lab validation of new solution, including documented testing, validation, and what−if analysis showing impact to existing infrastructure; completion of an operations support document, backout plan, and implementation plan; and adherence to the change process. Recommend solution pilots and a preliminary design review prior to testing.
2	Requires what−if analysis performed in lab to determine the impact to the existing environment in regards to capacity and performance; test and review of all routing changes; backout plan, implementation plan, and adherence to change process; and design review for major routing changes or backbone changes.
3	Requires engineering analysis of new solution, which may require lab validation; implementation plan and adherence to change process.
4	Requires implementation plan and adherence to change process.
5	Optional adherence to change process.

For changes with risk levels of 1 to 3, two types of lab validation are important: feature and functionality testing, and what−if analysis.

Feature and functionality testing requires that you validate all configurations, modules, and software with lab−generated traffic to ensure that the solution can handle the expected traffic requirements. Create a test plan that validates configuration parameters, software functionality, and hardware performance. Be sure to test behavior under real−world conditions, including spanning−tree changes, default gateway changes, routing changes, interface flaps, and link changes. Also validate the security and network management functions of the new solution.

What−if analyses seek to understand the affect of the change on the existing environment. For instance, if you add a new feature to a router, the what−if analysis should determine the resource requirements of that feature on the router. This type of testing is normally required when adding additional features, users, or services to a network.

Change Planning

Change planning is the process of planning a change, including identifying requirements, ordering the required hardware and software parts, checking power budgets, identifying human resources, creating change documentation, and reviewing technical aspects of the change and change process. You should create change planning documentation such as maps, detailed implementation procedures, testing procedures, and backout procedures. The level of planning is usually directly proportional to the risk level of the change. A successful project should have the following goals for change planning:

- Ensure all resources are identified and in place for the change.
- Ensure a clear goal has been set and met for the change.
- Ensure the change conforms to all organizational standards for design, configuration, version, naming conventions, and management.
- Create backout procedure.
- Define escalation paths.
- Define affected users and downtimes for notification purposes.

Change planning includes the generation of a change request, which should be sent to the change controller. We recommend including the following information on the change request form:

- Name of person requesting change
- Date submitted
- Target date for implementing change
- Change control number (supplied by the change controller)
- Help desk tracking number (if applicable)
- Risk level of change
- Description of change
- Target system name and location
- User group contact (if available)
- Lab tested (yes or no)
- Description of how the change was tested

- Test plan
- Backout plan
- If successful, will change migrate to other locations (yes or no)
- Prerequisites of other changes to make this change successful

The technical description of the change is an important aspect of the change request, and may include the following: current topology and configuration, physical rack layouts, hardware and hardware modules, software versions, software configuration, cabling requirements, logical maps with device connectivity or VLAN connectivity, port assignments and addressing, device naming and labeling, DNS update requirements, circuit identifiers and assignments, network management update requirements, out−of−band management requirements, solution security, and change procedures.

In addition, a change request should reference any standards within your organization that apply to the change. This helps to ensure that the change conforms to current architecture or engineering design guidelines or constraints. Standards can include the following: device and interface naming conventions, DNS update requirements, IP addressing requirements, global standard configuration files, labeling conventions, interface description conventions, design guidelines, standard software versions, supported hardware and modules, network management update requirements, out−of−band management requirements, and security requirements.

Change Controller

A key element to the change process is the change controller, usually an individual within your IT organization who acts as a coordinator for all change process details. Normal job functions of the change controller include:

- Accepting and reviewing all change requests for completeness and accuracy.
- Running periodic (weekly or biweekly) change review meetings with change review board personnel.
- Presenting complete change requests to the change review board for business impact, priority, and change readiness review.
- Preventing potential conflict by maintaining a change schedule or calendar.
- Publishing change control meeting notes and helping communicate changes to appropriate technology and user groups.
- Helping ensure that only authorized changes are implemented, that changes are implemented in an acceptable time frame in accordance with business requirements, that changes are successful, and that no new incidents are created as a result of a change.

In addition, the change controller should provide metrics for the purpose of improving the change management process. Metrics can cover any of the following:

- Volume of change processed per period, category, and risk level.
- Average turnaround time of a change per period, category, and risk level.

- Number of relative changes amended or rejected per period and category.
- Number of relative change backouts by category.
- Number of relative changes that generate new problem incidents.
- Number of relative changes that do not produce desired business results.
- Number of emergency changes implemented.
- Degree of client satisfaction.

Change Management Team

You should create a change management team that includes representation from networking operations, server operations, application support and user groups within your organization. The team should review all change requests and approve or deny each request based on completeness, readiness, business impact, business need, and any other conflicts.

The team should first review each change to ensure all associated documentation is complete, based on the risk level; then the team can investigate the business impact issues and business requirements. The final step is to schedule the change. Once a change has been approved, the change management team is also responsible for communicating the change to all affected parties. In some cases, user training may also be needed.

Note: The change management team does not investigate technical accuracy of the change; technical experts who better understand the scope and technical details should complete this phase of the change process.

Communication

Once a change has been approved, the next step is to communicate details of the change by setting expectations, aligning support resources, communicating operational requirements, and informing users. The risk level and potential impact to affected groups, as well as scheduled downtime as a result of the change, should dictate the communication requirements.

We recommend creating a matrix to help define who will be affected by a change and what the potential downtime may be for each application, user group, or server. Keep in mind that different groups may require varying levels of detail about the change. For instance, support groups might receive communication with more detailed aspects of the change, new support requirements, and individual contacts, while user groups may simply receive a notice of the potential downtime and a short message describing the business benefit.

Implementation Team

You should create an implementation team consisting of individuals with the technical expertise to expedite a change. The implementation team should also be involved in the planning phase to contribute to the development of the project checkpoints, testing, backout criteria, and backout time constraints. This team should guarantee adherence to organizational standards, update DNS and network management tools, and maintain and enhance the tool set used to test and validate the change.

Specifically, the implementation team should fully understand the following testing questions (and should include them in the change documentation prior to approval by the change control board):

- How thoroughly should we test the change?

- How will we roll−out the test?
- How long will testing last, and at what point can we make the decision that the change has been implemented successfully?

The implementation team should also be fully aware of all backout criteria, time constraints and procedures. The team should answer the following questions as part of the change documentation for high−risk change prior to approval by the change control board:

- How is the change to be removed?
- At what point is the decision made to backout the change?
- What information should be gathered before backout occurs to determine why the change needed to be backed out or why it affected the network adversely?

During the implementation of any change, it is key to follow the change management team recommendations on how to make the change. If anything is performed on the network that deviates from the recommendations, the implementation team should document and present these steps to the change controller upon completion of the change.

Test Evaluation of Change

Testing and verification can be critical to a successful change. You should identify testing steps after defined change checkpoints and final change completion. In addition, allocate sufficient time for testing, both during and following the implementation and backout, if necessary. In some cases, you can do testing prior to the change when new service is involved, such as new circuits or links that are not currently in production. The following additional testing and verification procedures may be pertinent to a network change:

- Extended pings for connectivity and performance (may require many to many)
- Traceroutes
- End−user station network and application testing
- File transfers or traffic generation for performance−related changes
- Bit error rate testor (BERT) testing for new circuits
- Interface statistic verification
- Log file verification
- Debug verification
- Display or **show** command verification
- Network management station availability and verification

After achieving some level of comfort with the change, evaluate what has been accomplished. Does the change make sense? Did the change address the network problem? What should be done differently the next time a change is warranted?

Network Management Update

Operational readiness requires that you update all network management tools, device configuration, and DNS to reflect the change. In addition, your organization may have tools for fault management, configuration management, availability measurement, inventory management, billing, and security that require updates. The following are some typical network management update requirements following change:

- Router loopback address with DNS primary name following naming standard.
- Router interface addresses with DNS primary/interface names following naming standard.
- Removal of DNS entries and network management system (NMS) management for devices removed from the network.
- Standard SNMP configuration entered on devices, including community string, location, support contact, syslog server, trap server, and SNMP server host.
- Trap source, syslog source, and SNMP source configured for loopback0.
- Fault management tool update.
- Inventory management tool update.

Documentation

Possibly the most important requirement in any network environment is to have current and accurate information about the network available at all times. During the process of changing the network, it is critical to ensure that documentation is kept up−to−date. Network documentation should include the following:

- Detailed physical layer drawing displaying all network devices that have a medium risk (or higher) on the network; includes rack layouts, cable connections, and devices.
- Detailed network layer drawing of all network devices that have a medium risk (or higher) on the network; includes addresses, and IP subnet and VLAN information.
- Out−of−band management access maps and documentation.
- Solution templates.
- Detailed IP and Internet Packet Exchange (IPX) numbering plans and assignments.
- VLAN numbering plans and assignments.
- Source router bridge ring numbering plan and assignments.
- Naming standards for all network devices.
- Software code and hardware types currently implemented and supported.
- Protocol filtering criteria and methodologies.
- Routing protocols standards and supported modifications from default settings.

- Global configuration standards.
- Inventory database for all physical connectivity and contact information.

In addition, we recommend you develop a matrix containing information about user groups, the applications they require, and the servers (addresses and locations) that host these applications. This information is necessary to ensure that users continue to have the level of access and performance they require during and after the change. In addition, previously used test plans assist in simplifying future changes, and they may assist in troubleshooting problems that have occurred because of a change.

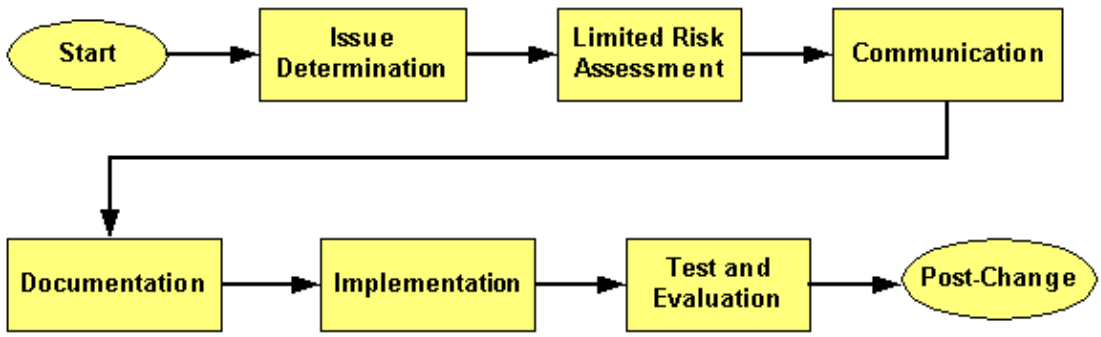
High−Level Process Flow for Emergency Change Management

Unfortunately, not all situations that occur in a network environment are conducive to the extensive research and planning described in the previous section. Sometimes you'll need to make more immediate changes to restore network connectivity following a network outage.

The procedures you put in place to handle emergency changes should be flexible enough to facilitate rapid resolution of the problem, including documentation of who is authorized to make emergency changes to the network, and how to get in touch with these individuals. You should either have a sufficient number of people who can resolve network emergencies, or those people should be easily accessible at all times to prevent a roadblock in the problem resolution process.

It is imperative to maintain both communication and the integrity of documentation through an emergency change. This is the time when documentation is needed most, so documenting the steps taken to resolve the problem is of paramount importance.

Finally, when considering changes, you should think about not only whether the change will resolve the existing problem, but also whether the change will cause other network problems. Steps that are critical for an emergency change process are shown in the process flow below. Click each box for more information about that step:



Issue Determination

It is usually obvious when an emergency change is required in a network environment. However, exactly what change is required may not be obvious. For Cisco equipment, you should include the appropriate Cisco support personnel in the troubleshooting process.

When taking corrective action, it is imperative that you implement only one change at a time. Otherwise, if

the problem is resolved by multiple changes, it is impossible to pinpoint which change actually fixed the problem; or worse, if other problems are introduced, it is impossible to determine which change was the cause of the new fault. Each change should go through the full process outlined above before you begin on the next change. If a change is shown to have no effect, you should back out of it before beginning the next change (the single exception being when the initial change is a prerequisite to the next change under consideration).

Limited Risk Assessment

In most cases, the amount of risk assessment done in an emergency situation is directly proportional to the scope of the change, and inversely proportional to the effect of the network outage. For example, the scope of changing a router software release is much greater than that of changing a protocol address. Similarly, the same change would go through increased scrutiny if a single user was unable to access the network rather than if an entire site had lost connectivity.

Ultimately, risk assessment is the responsibility of the network support person implementing the change. For this, he or she should rely on their own personal experience, as well as that of associated support personnel. Many of the ideas given in the section on Planned Change Management can be adapted to the emergency change environment, but on a more limited scale. For instance, you can use the or even a limited test bed simulation, depending on your situation.

Finally, as part of the limited risk assessment, you should determine which users may be affected by the change.

Communication

Although it isn't always be possible to notify all users of all changes (especially in emergency situations) the user community will certainly appreciate any warning you can provide. You should also communicate the details of any emergency changes with the change manager, allowing them to maintain metrics on emergency changes and root causes. The information may also affect the scheduling or rollout of future changes.

Documentation

Updating documentation is critical to ensure valid, up−to−date information. During unplanned changes, it's easy to forget to make updates because of the frantic nature of emergencies. However, undocumented change solutions often result in increased downtime if the solution is unsuccessful.

It helps to document changes before they are made in emergency situations from a central location, perhaps at the change manager level. If a central support organization doesn't exist to document changes before they occur, different individuals may make changes at the same time not knowing about each other's activities. Following are types of documentation that often require updates during a change: drawings, IP/IPX/VLAN database, engineering documents, troubleshooting procedures, and server/application/user matrices.

Implementation

If the process of assigning risk and documentation occurs prior to the implementation, the actual implementation should be straightforward. Beware of the potential for change coming from multiple support personnel without their knowing about each other's changes. This scenario can lead to increased potential downtime and misinterpretation of the problem.

Test and Evaluation

In this phase, the person who initiated the change is responsible for ensuring that the emergency change had the desired affect and if not, restarting the emergency change process. Steps to take in the investigation of the change include the following:

- Observe and document the impact of the change on the problem.
- Observe and document any foreseen or unforeseen side effects of the change.
- Determine whether the problem has been resolved, and if so, make sure all necessary documentation and network management updates occur to properly reflect the change.
- If the change is unsuccessful, back out, and continue the emergency change process until the problem is resolved or a workaround is in place.

Once the change has been deemed successful, send all emergency change documentation to the change controller for review and documentation by the change control team. The change controller and change review team should perform a postmortem on the problem to determine potential improvements to prevent future emergency changes of this type. You should also bring the information to engineering or architecture groups for review, and allow them the opportunity to change solution templates, standard software versions, or network designs to better meet the goals or requirements of your organization.

Performance Indicators for Change Management

Performance indicators provide the mechanism for you to measure the success of your change management process. We recommend you review these indicators monthly to ensure that change planning and change management are working well.

- Change Management Metrics by Functional Group
- Targeting Change Success
- Change History Archive
- Change Planning Archive
- Configuration Change Audit
- Periodic Change Management Performance Meeting

Change Management Metrics by Functional Group

Change management metrics by functional group include the percentage and quantity of change success by functional group and risk level. Emergency changes should be identified separately in the metrics by functional group, including the success rate for attempted fixes. Functional groups include any IT teams making changes, possibly including server administration, network administration, database groups, application teams, and facilities. Risk level is important because generally higher risk changes fail or create incidents. You may define change failure as any change that is backed out or causes a problem incident resulting in user downtime.

Determining change−related incidents can be difficult. You should contact the user identified on the change request form following the change to get an understanding of change success. The change controller may also have a help−desk database available that includes problems closed because of change related issues.

Targeting Change Success

To target change success you should start with a baseline of change management metrics. The change controller can then identify potential issues and set overall goals. A reasonable overall goal for change success in high−availability networks should be 99 percent across all functional groups. If your organization is experiencing a higher rate of change failure, it should be targeted for improvement.

Change History Archive

The change controller is also responsible for archiving the change history. Creating a spreadsheet with functional group success and failure columns and month rows is sufficient for archival. Change history archives can help identify current issues based on past change rates and available resources. The information can also be used to investigate change rates in general for overall planning purposes.

Change Planning Archive

The change controller should archive change planning documentation, such as network engineering documents, to create a reference of examples for future successful projects. If the change controller notices change problems, he or she can refer to the change planning document to investigate how well the particular issue was documented before the change. Over time, the change controller may ask to have additional information added to future change planning documents for higher−risk changes to help ensure success.

Configuration Change Audit

We recommend investigating the quantity and risk level of undocumented changes. In networking environments this requires the implementation of user TACACS and network time protocol (NTP), in addition to a configuration file archival process and application. The Cisco Resource Manager Essentials toolbox has a configuration file utility that can help log configuration file changes.

Undocumented change is a common problem in almost all organizations. We recommend that you continually reiterate the requirement for team members to use the required change control process, even though it adds time and effort.

Periodic Change Management Performance Meeting

It is important to review the metrics you collect monthly, including the following: change quantity and risk level, change failure quantity and post mortems, emergency changes and post mortems, change management goals, and undocumented changes. The functional manager should review the metrics and report to the appropriate teams for improvement.

Related Information

- **More Best Practices White Papers**