Just first 10 things that came to my mind. Actually I can't imagine living in a decent network without those things. Yeah, it takes time to implement all those but it'll pay off HUGELY in case of any problems.

NTP and timezones set for every devices:
- must have for some IPSec implementation, DHCP snooping, log management.

Centralized AAA:
- tacacs+ authentication
- tacacs+ command authorization (optional, if not fully trusted persons have access to equipment)
- tacacs+ command accounting.

Centralized log management:
- splunk (mix of google search and excel) is really GREAT for this! It deserves multiple additinonal posts
- well, I use splunk for event monitoring also. It notifies me about some important stuff in my network. Like 'CUCM failed to create backups in a software repository for two days already' and 'Somebody from non-management subnet tried to ssh my devices'
- well, well. I use Splunk for reporting also. Like 'What users have been online with anyconnect since this morning' and 'How many international, long-distance and local calls did my CUCM users yesterday' and reporting about command accouinting 'Who configured that lame ACL on that router? Ooops, that was me a month ago!'. Sorry, can't stop talking about Splunk.

Centralized configuration management:
- regular (daily) config archiving. Git if possible. Cisco Prime is good, but way too heavy
- ability to see diffs between configs
- morning diff ("what we broke yesterday") to admins email box
- configuration distribution to multiple hosts. Cisco Prime is good here, but I've seen bugs like 'silently discarding some devices w/o notifying'
- keeping 'golden configs' aka templates, i.e. verified typical configurations.

Centralized Inventory:
- Cisco Prime (lame) or custom Ansible playbooks + git.

Centralized software repository
- accessible via scp, ftp, tftp, smb. Cisco Prime is kind of ok, but I believe custom repository could be better.

Compliance management:
- one of MUST HAVEs if you really care about your network. Make sure that (all) devices have (all) required policies (i.e. configuration blocks). Does 802.1x present on all users ports? Do you have all necesary ACLs on the outside interfaces? Do usernames configured with 'secret' instead of insecure 'password'?

Centralized AND distributed monitoring
- accessibility monitoring, performance monitoring, system monitoring. Huge topic for another post.

Centralized Summarized IP addressing scheme:
- often overlooked, but this is number one thing in building a scalable and manageable network. At any given time you must be able to reference (in a route, prefix-list or ACL for example) any network module, site, region, country as a one, two or maximum three subnet definition. For example, 10.16.32.0/19 is a subnet of all our users at site X, including users connected by wire, WiFi or VPN.

And one last thing. Not management, but very best practice:
- keep your network as homogeneous/uniform/unvaried/consistent as possible. Same devices, same designs, same configuration for the same type of POP/site. For any exception in configuration you will pay by drops of your blood.

If you want me elaborate on any of the topics mentioned above, just leave a comment. I'll try :)