# CSC 11

*John Ryan Zelling Analyst*

*Jan 2017*

## Contents



## CSC 11.0

[1] "Critical Security Control #11: Secure Configurations for Network Devices"

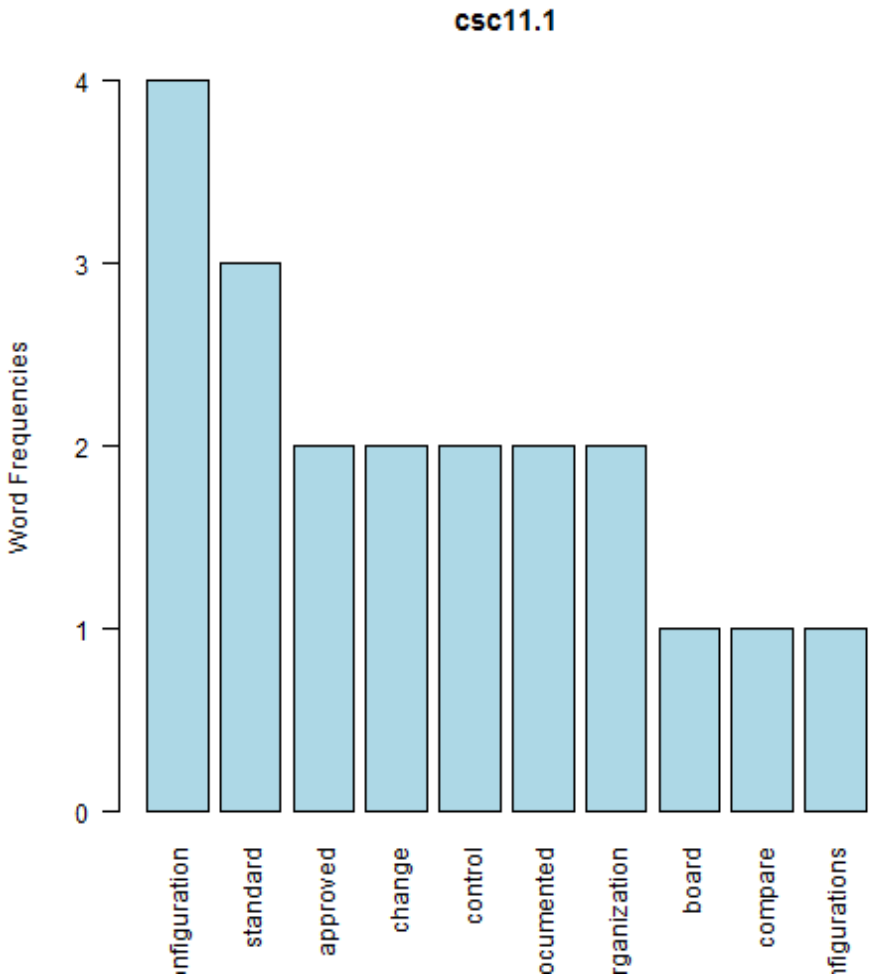
[1]

[1] [1] "To further clarify the Creative Commons license related to the CIS Critical Security Controls content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Â  Additionally, if you remix, transform or build upon the CIS Critical Security Controls, you may not distribute the modified materials. Users of the CIS Critical Security Controls framework are also required to refer to (http://www.cisecurity.org/critical-controls.cfm) when referring to the CIS Critical Security ControlsÂ in order to ensure that users are employing the most up to date guidance. Â Commercial use of the CIS Critical Security Controls is subject to the prior approval of The Center for Internet Security."

**CSC 11.1**

[1] “configuration + standard”


null device 1

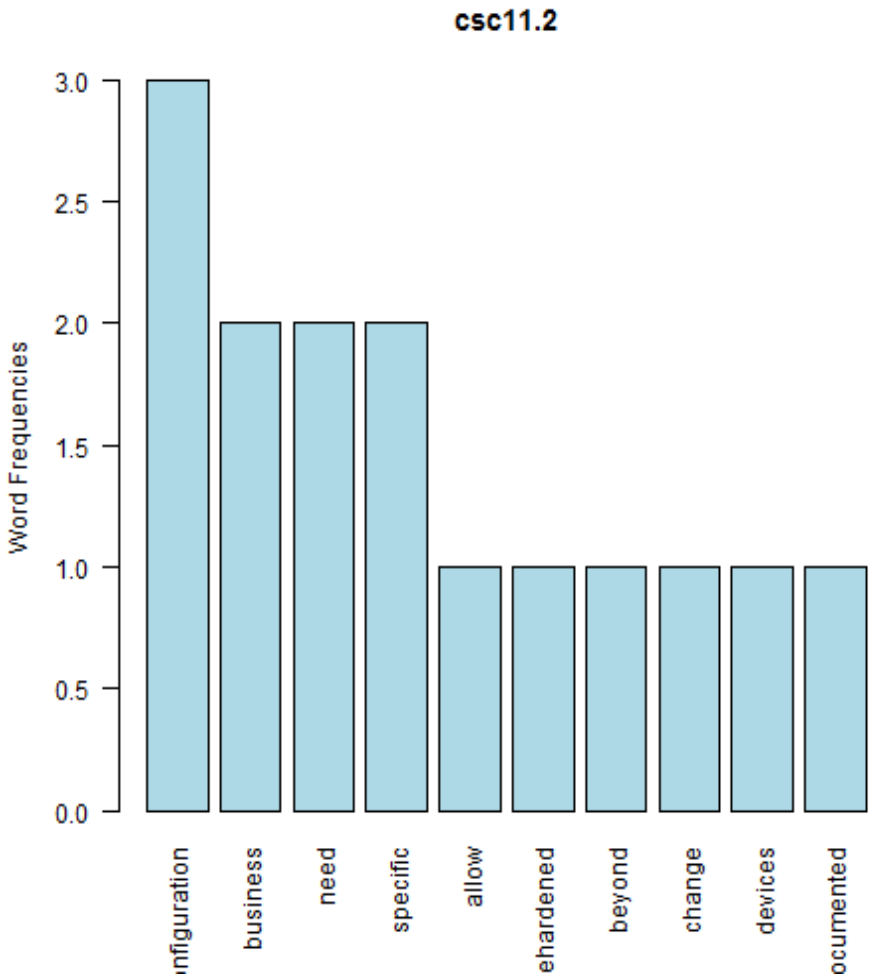



null device 1 [1] “Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.”

**CSC 11.2**

[1] “configuration + business”

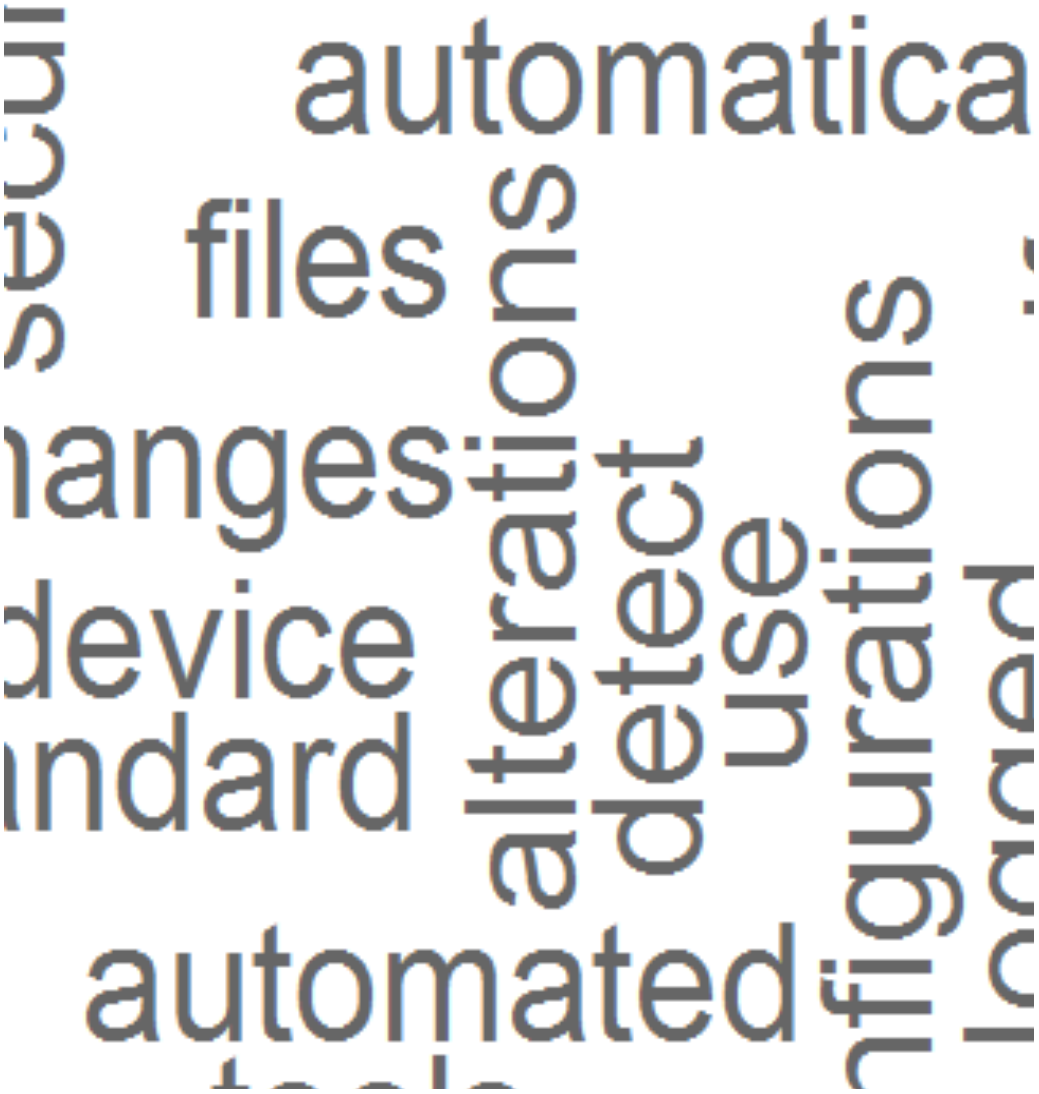

null device 1



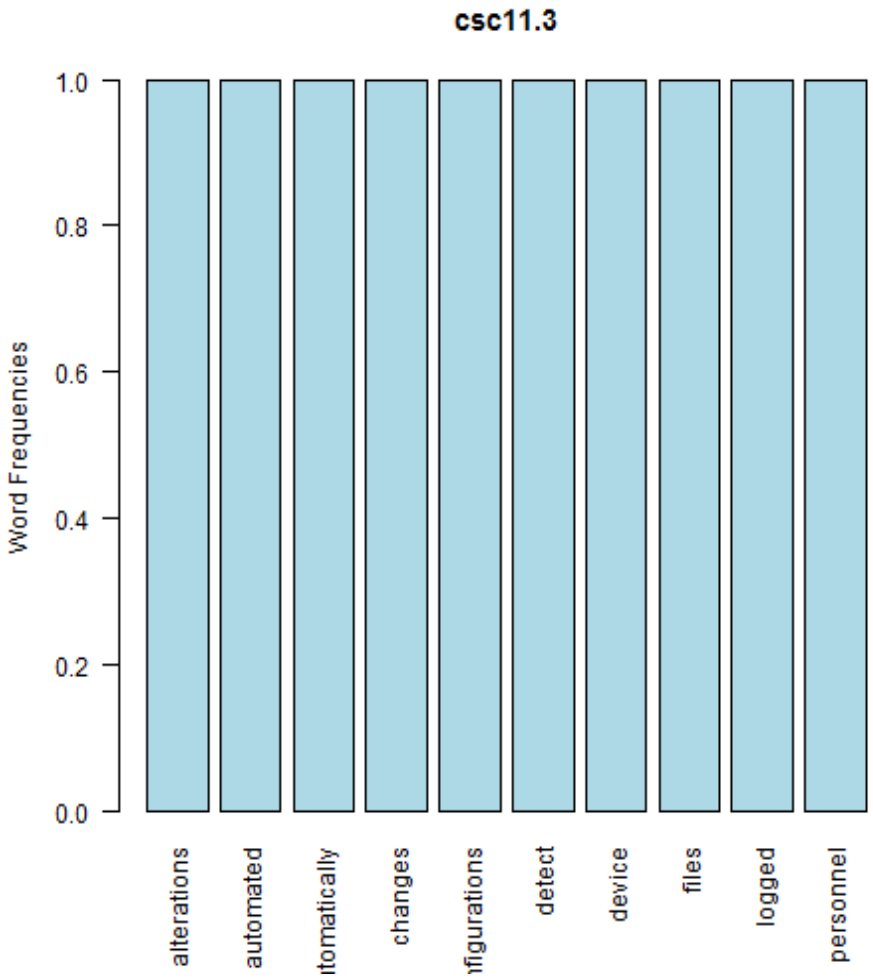

null device 1 [1] “All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, should be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individualâ s name responsible for that business need, and an expected duration of the need.”

**CSC 11.3**

[1] “alterations + automated”



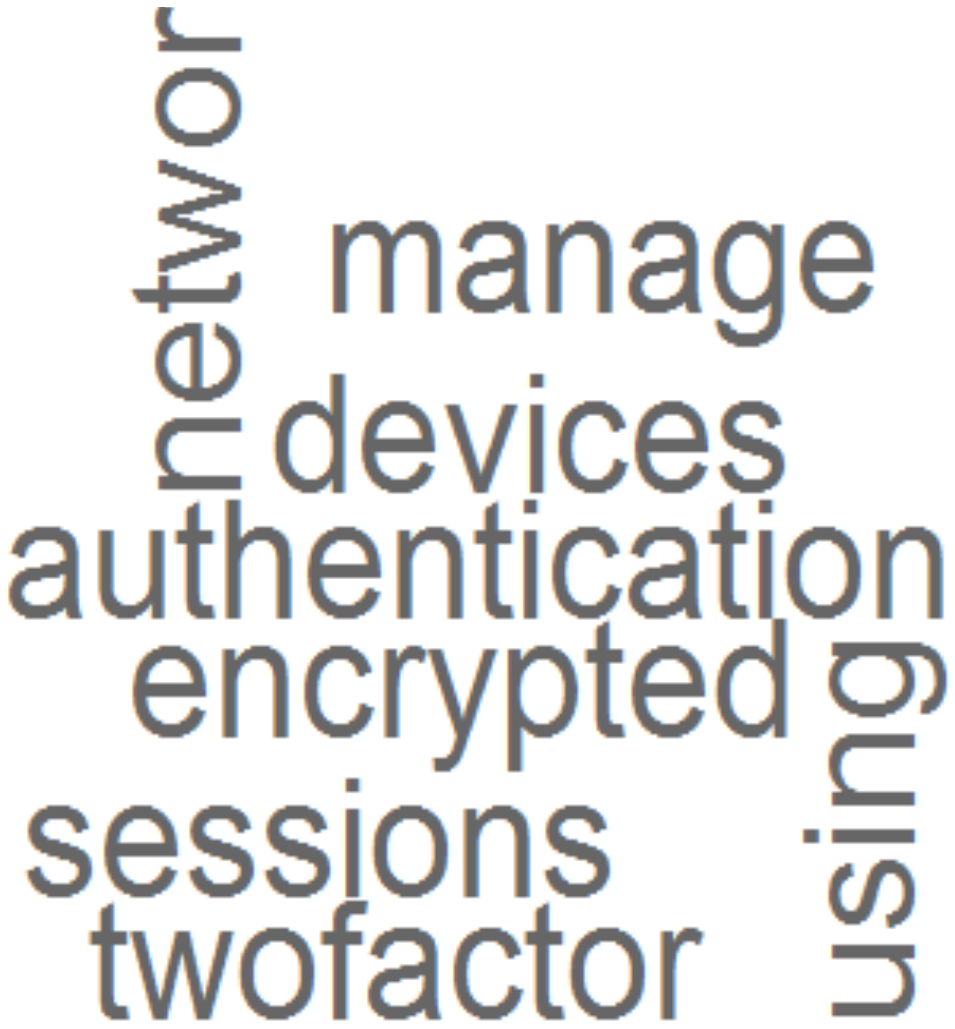

null device 1



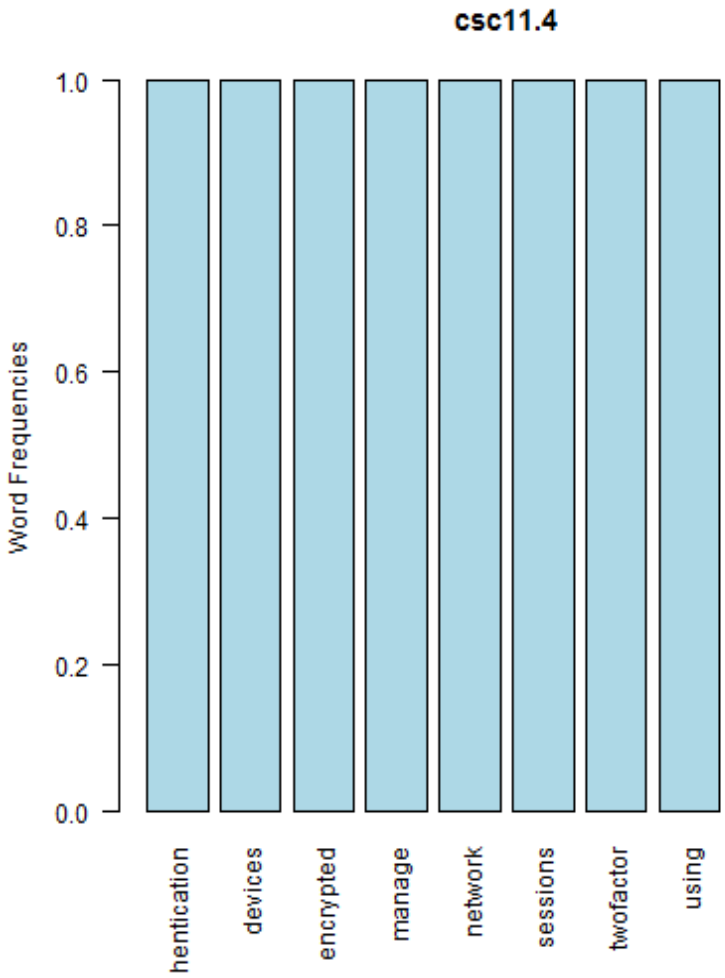

null device 1 [1] “Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be logged and automatically reported to security personnel.”

**CSC 11.4**

[1] “authentication + devices”




null device 1

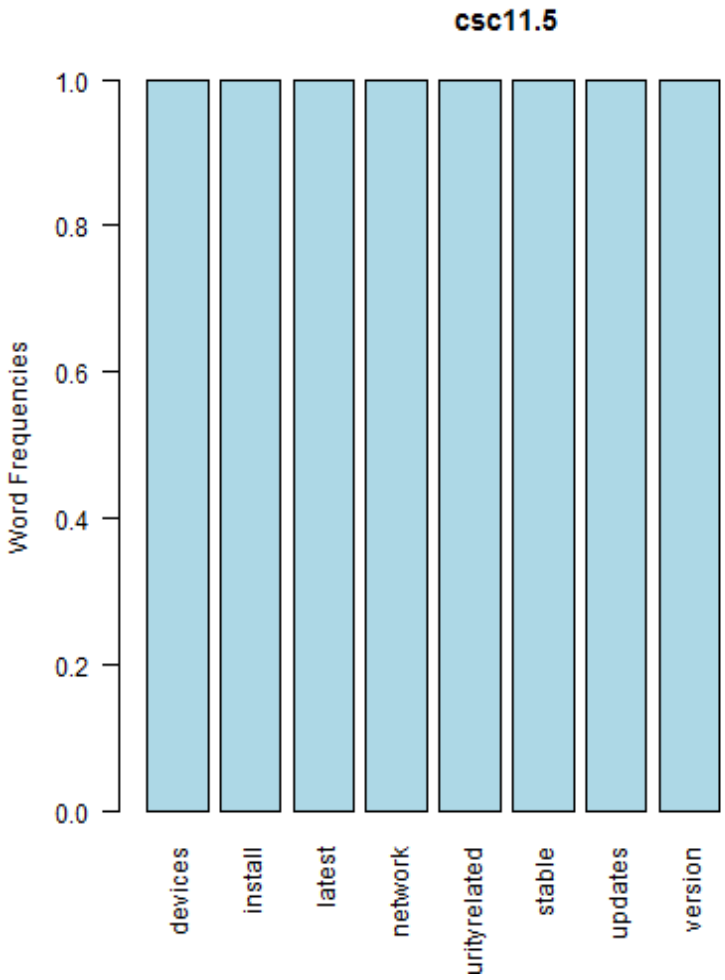



null device 1 [1] “Manage network devices using two-factor authentication and encrypted sessions.”

**CSC 11.5**

[1] “devices + install”


null device 1

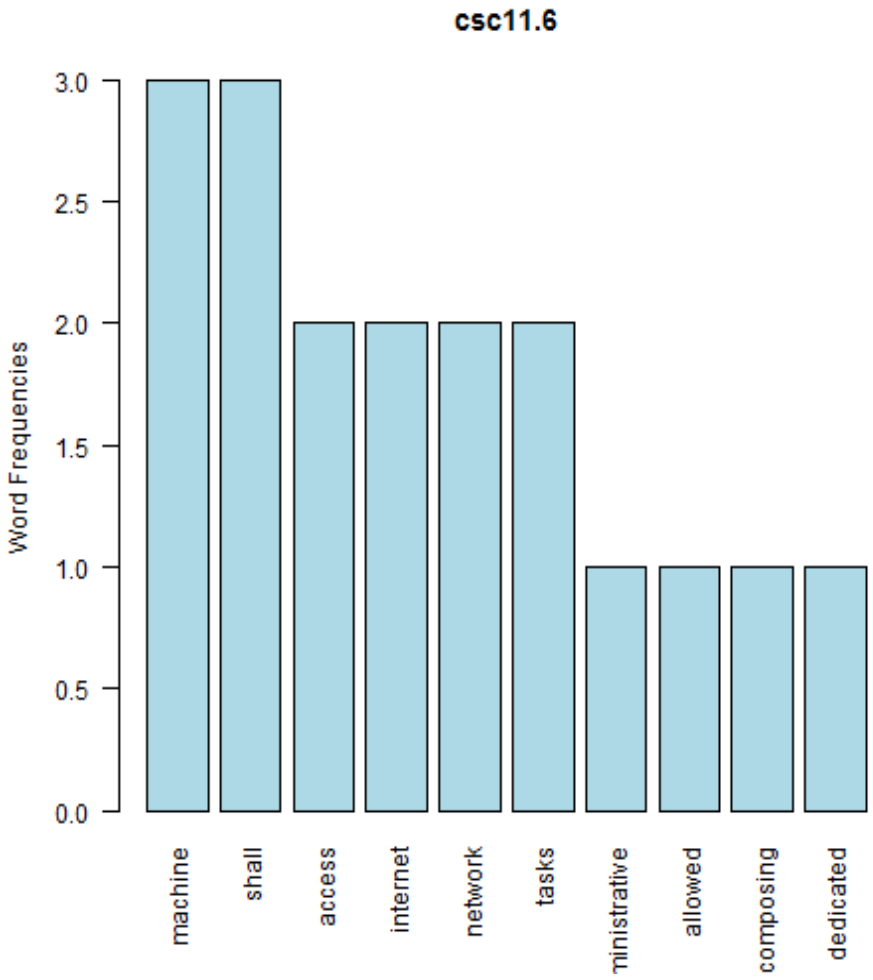



null device 1 [1] “Install the latest stable version of any security-related updates on all network devices.”

**CSC 11.6**

[1] “machine + shall”

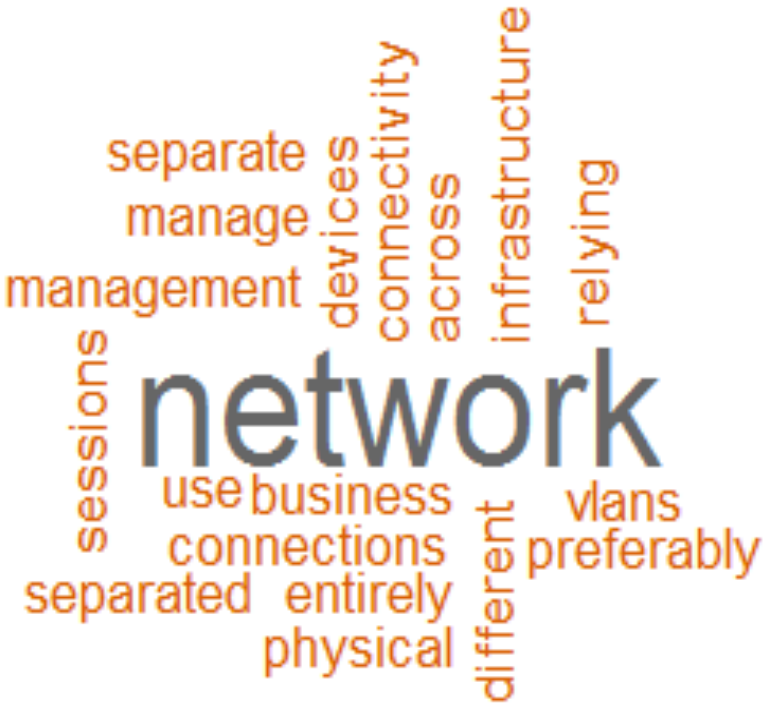

null device 1



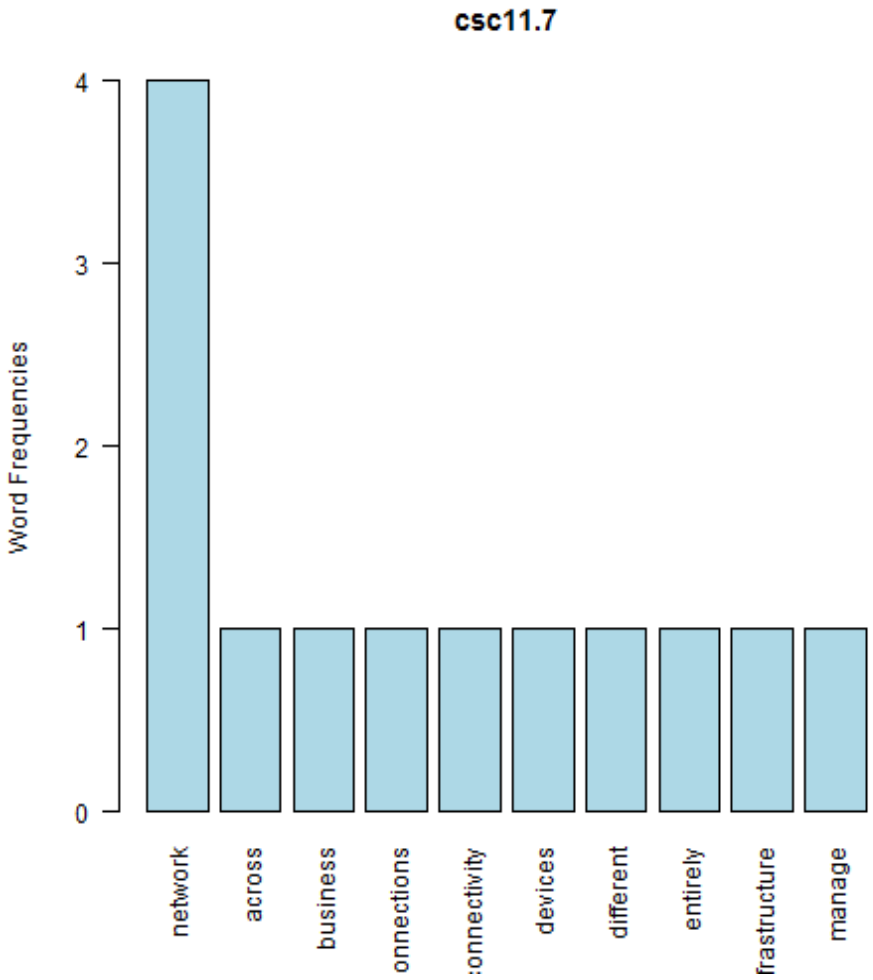

null device 1 [1] “Network engineers shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization’s primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.”

## CSC 11.7

[1] “network + across”




null device 1




null device 1 [1] “Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.”