Towards a Task Oriented Method for Accessing Network Based Services

Nils Pedersen
Cisco Systems, Inc.
5575 Tech Center Drive
Colorado Springs, Colorado, USA
+1 408 424 0492
nipeders@cisco.com

Paul Clark
Cisco Systems, Inc.
2200 E. George Bush Hwy
Richardson, Texas, USA
+1 972 813 5107
aggie@cisco.com

Martine Freiberger
Nandana Studios
359 San Carlos Avenue
Redwood City, California, USA
+1 650 364-6889
martine.freiberger@gmail.com

ABSTRACT

Today's networked users are required to configure a number of different network settings on their computer in order to access specific network based services. For example, these users need to know whether to enable a Virtual Private Network (VPN) tunnel and, in some cases, also select the appropriate wireless network. As more sophisticated security models are incorporated into networks, the user's task in managing these settings will become more complex.

This paper describes a design which simplifies the task of accessing network based services using a more user oriented, less technology centric task flow.

Categories and Subject Descriptors

H.5.2 [**User Interfaces**]: User-centered design

General Terms

Design, Human Factors.

Keywords

Virtual Private Network, Networking, User Interface, Flyout, Borderless Networks, Identity Based Networking, Network Access, User Credentials, Network Security.

1. INTRODUCTION

Traditional network security systems that presented a single perimeter are being supplanted by models which offer finer levels of granularity. For example, corporate network access is provided by selecting one wireless network, while guest network access is provided by selecting a different wireless network.

This [network security] system needs to enable businesses to express policies in terms of who the user is, what application they use, and what content they access. It must work both inside and outside of the traditional corporate network to meet the security challenges of today's decentralized and highly collaborative work environment (Gillis 2010).

CHIMIT'10 , November 12-13, 2010, San Jose, CA, USA

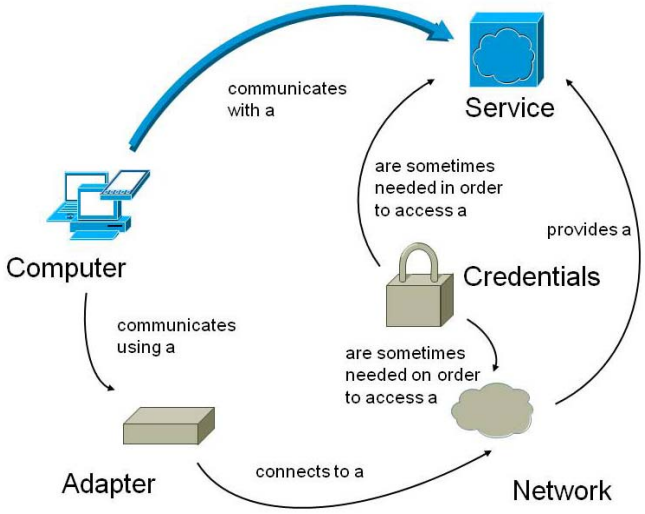

Figure 1 A Network Client Access Model

Different technologies, with different user interfaces have been developed for accessing the network from inside or from outside the network perimeter. Typically, the onus is on the end-user to manage this complexity. Most network access clients assume an IT-knowledgeable user is utilizing the software, and that little effort seems to be placed on user-friendly features (Schacter 2009).

In order to access a particular service, like email or a web application, the user has to know how to correctly configure the network settings of their computer. In some cases (as shown in Figure 1) they have to select the correct hardware network adapter, the correct network connection, and provide authentication credentials.

Figure 2 shows the available wireless networks in Mac OS X. This particular Macintosh is displaying the available wireless networks in a corporate office environment. If a user wants to access their work email, which network would they connect to? In fact, in this particular instance, the network that would provide access to their work email is called *blizzard*. The user has to learn to associate the unintuitive word *blizzard* with their work.

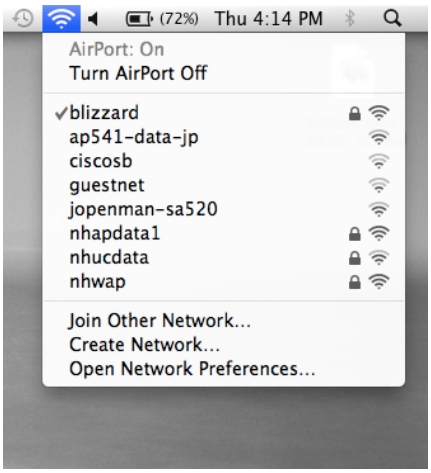

Figure 2 Mac OS X Network Selection Menu

2. BACKGROUND

A user interface was required for a new software product, combining the functionality of a VPN client and a network connection client. The VPN client software allows a computer to connect to a VPN headend gateway using a secure encrypted connection. Typically, the headend gateway is located on the perimeter of an organization's network and facilitates access to the organization's internal network. The network connection client software allows an administrator to define how a computer client connects to wired and wireless networks and which networks are available for that computer client to use. In other words, the network connection client helps the user choose a local network to connect to and the VPN software establishes a secure connection, through the local network, to an organization's internal network.

These products are typically targeted at large enterprises. A combination of both pieces of software would allow an administrator to define an organization's network access policy for both remote and local clients. By combining both pieces of software into one, users would be provided with a single tool which can manage all their work, as well as non-work, network connections.

2.1 Design Goals

In conjunction with the engineering team it was agreed that the user interface should intrude on the user only when absolutely necessary and the design abstraction presented should be targeted at a corporate, non-technical user. The experience should be seamless, more like a cell phone than a computer.

The primary target platform was Windows 7, although the design was expected to function equally well on other operating systems including, OS X, Linux and handheld platforms (such as iPhone and Android). In contrast, there was also a requirement that there be a consistent experience across all platforms, both from an end-user support perspective as well as an administrator one.

3. DESIGN

3.1 Design Hypothesis

The designs presented by the current versions of the products are delivered in a technology centric manner. By simply merging those two disparate experiences into a single task flow the overall experience would be improved. However, users would still have to know how their current network environment was implemented in order to correctly configure the optimal network connection for their current task. This state of affairs was deemed to be particularly problematic, especially for non-technical users.

It was hypothesized that providing an abstraction that mapped more closely to the task would be a better fit than directly exposing the existing network centric model.

3.2 Tasks

The main task supported by the current VPN product is to make a secure connection to a protected network using a network device known as a headend gateway. From the end-user's perspective they are either enabling or disabling a connection *to work*. The network connection client software attempts to maintain the best network connection available, given the current environment and security policies configured by the administrator.

3.3 Model

The basic premise was that it would be more natural for users to associate a particular label or friendly name with a set of desired services or applications rather than learn the intricacies of client network configuration. There would be fewer things for a user to remember and fewer decisions for them to make. The primary concept in the user model is a *network destination*, or just *destination* – as shown in Figure 3.

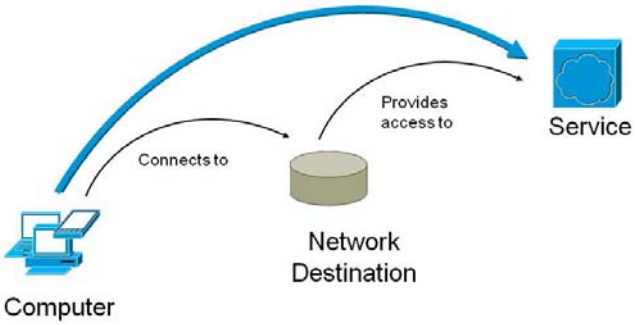

Figure 3 Simplified Network Client Access Model

Destination may be associated with a combination of a network adaptor, a network, and a VPN headend. When a user selects a *destination* the system would determine if the network associated with the *destination* was available; if so, it would connect to that *destination*.

If that network was not available, the system would connect to the best available network that would enable access (sometimes using a VPN connection) to that *destination*. It was envisioned that administrators would typically create two *destinations* by default, a *destination* mapped to the organization's internal network called *Work*, and one mapped to the current local network called *Internet*. The client software would automatically connect to known (those that it had previously connected) networks; it would prompt the user for acknowledgement before connecting to unknown networks.

3.4 Prototype

As the primary client platform was Windows 7, it was decided to initially leverage a Windows system gadget flyout (Microsoft 2010) based solution. For design evaluation and iteration, and in order to help socialize the design, a prototype was developed. Adobe Flex was chosen for its rapid prototype capabilities and to create a standalone application that could be run on multiple computer platforms.

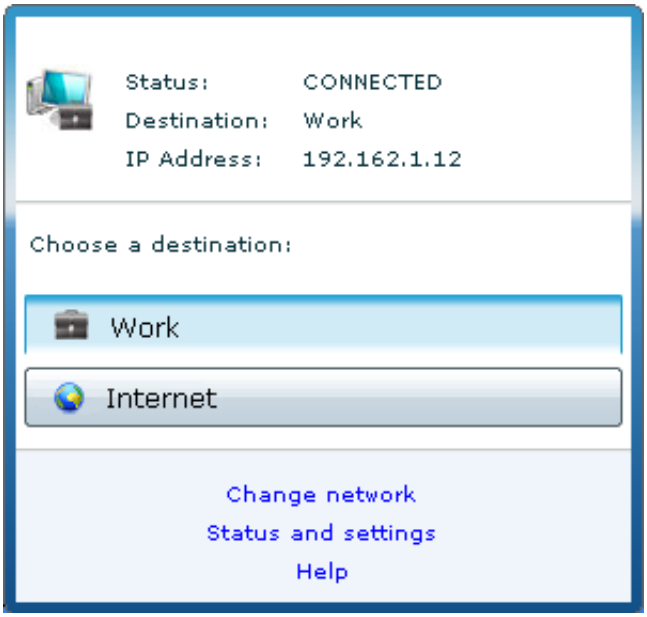

Figure 4: Flyout Design

After a number of iterations, the initial design candidate for formal end-user testing was agreed upon – as shown in Figure 4. Towards the top of the pane, the flyout summary area shows the current status and which destination is connected. The center of the pane, known as the task area in flyout terminology, allows the end-user to select one destination from those that the administrator has made available. The links at the bottom of the flyout allow the user to manually change the current network, access more detailed status and configuration options, and view help information. The flyout is accessed from a Windows notification area icon. An icon overlay was updated based on the current state of the connection.

4. USABILITY STUDY

A formal usability study was conducted to test the main design hypothesis of the concept of a *network destination*. It was important to determine if the original design goals had been achieved, specifically whether non-technical users could successfully perform typical tasks using the design.

4.1 Test Methodology

The design was exercised with network connection tasks in the following scenarios: receiving a new laptop and connecting to a work network, connecting to a home wireless network, connecting to a wireless network at a coffee shop, changing a Wi-Fi shared key, and adding a new *network destination.* Twelve participants, experienced in using computers with wireless networks, were tested. Six of the participants were categorized as non-technical and the other six were technical. For the purposes of the study, the boundary between technical and non-technical groups was defined as whether or not the person had the ability to configure a home wireless network.

As well as participant's subjective comments, metrics were collected including: time-on-task, success rate, error rate and number of assists (interventions required to enable the participant to complete the task) were collected.

In addition, a Software Usability Measurement Inventory (Kirakowski and Corbett 1993) or SUMI questionnaire was completed by each participant.

4.2 Findings

Not surprisingly, non-technical users required more assists and committed more errors than technical participants.

Non-technical users also expected there to be a functioning help system (which was not implemented in the prototype). Technical users seemed more comfortable exploring the prototype and were less likely to look for help. Based on the SUMI results, non-technical users seemed to be more favorable towards the UI than technical ones.

Some technical users expected an interface similar to existing products and were initially confused by the notion of a *destination*. Non-technical users had no such expectations. In fact, if they did not understand technical terminology, like VPN, then they were effectively blocked from successfully completing certain tasks.

Users had difficulty in finding the flyout. This may have been due to their unfamiliarity with the flyout / notification area interaction model. However, they also expected to find certain functionality, like network connection management, in existing Windows tools as they thought it was already provided.

In addition, all users expected the tool to provide reasonable defaults and to remember configuration state authentication credentials across sessions. Effective communication of the current connectivity state of the system was critical; participants did not notice the icon overlays changing.

4.3 Customer Validation

In addition to the end-user study, the design was presented to several network architects from customers of the existing products. These customers had installations ranging from thousands to tens of thousands of clients. Anecdotally, it confirmed two of the primary design premises.

The architects agreed that the general direction of providing an abstraction designating a connectivity goal (as opposed to a collection of settings as a means to that end) was headed in the right direction. They also liked that they could potentially restrict a *destination's* use of a particular adapter; for example, restricting use of the mobile broadband adapter for only connections to *Work*.

Customers also liked the concept containing all user interactions within the system tray area while trying to be as unobtrusive as possible.

5. FURTHER WORK

5.1 Design

The design can be improved based on feedback from the usability study. Users wanted better defaults, remembering settings across sessions and clearer communication of connectivity state.

5.2 Model

Although the concept of *network destination* successfully hid some aspects of the complexity of connecting a computer to a network, it was still a foreign term to all users. The most transparent solution would be to make appropriate connection based on which service the user wanted to access (Figure 5).

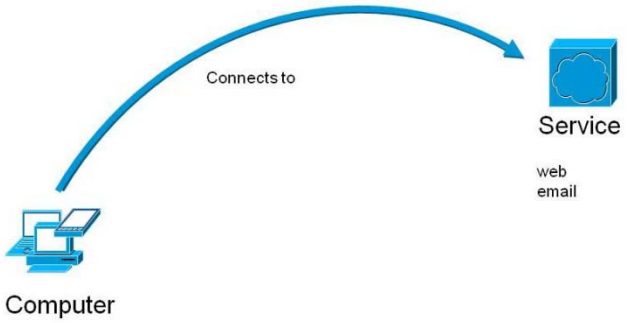

Figure 5 What The User Really Cares About

A registry could be developed which contained information about the service: like protocol, port number and network address, as well as which *network destination* was required. For example, a user might decide to associate the service Facebook with the Internet *destination*. When the system notices an http query to facebook.com it could check the current *destination* and if appropriate change it to *Internet*. Hopefully, at some point, the whole notion of a user explicitly selecting a *destination* would go away, since the system detects what the user is trying to do and automatically provides the best network based on what the user wants to do.

5.3 One Design or Platform Specific

Further investigation is required to understand the requirements for one design for all platforms versus the desire by end users to have a platform specific design. One consistent user experience across all platforms is suggested by some as simplifying the support task for IT departments. However, end-users typically stated that they expected the network client functionality to work consistently with the platform. Given both perspectives, it is unclear how much one single experience benefits supportability. The benefits gained by consistent support procedures across all platforms may be outweighed by the support issues generated by users expecting consistency within each platform.

6. CONCLUSIONS

By simplifying the network access model to one that is more task oriented one, non-technical computer users were more successful using the design than otherwise. By designing for non-technical users, the overall number of assists in the usability study was reduced. Technical terms that might have been roadblocks to success were exposed only when absolutely necessary.

In addition, care must be taken when functionality diverges from what a user expects. If a user expects wireless network management to function in a certain manner, but it does not, then the user has to deal with that inconsistency. IT departments that impose identical tools across all platforms for manageability and supportability reasons may be adversely affecting their end-users' productivity.

7. ACKNOWLEDGMENTS

This paper would not have been possible without the help and support of Anu Subramanian and Neil Schonwald from Cisco's Security Technology Business Unit.

8. REFERENCES

[1] Gillis, T. 2010 *Securing the Borderless Network: Security for the Web 2.0 World*. 1st. Cisco Press, Indianapolis, IN.

[2] Schacter, P. 2009 *Making Authenticated Networks Work*, Research Report, Burton Group, Midvale, UT.

[3] Microsoft, 2010. *Windows User Experience Interaction Guidelines.* http://msdn.microsoft.com/en-us/library/aa511258.aspx

[4] Kirakowski, J., and Corbett, M. 1993. SUMI: The Software Usability Measurement Inventory. *British Journal of Educational Technology*, *24*, 210-212.