CHAPTER 1

Unified Access Executive Summary

Cisco's Unified Access (UA) solution provides design guidance on solving key business problems related to network access—on-campus or remotely—with traditional devices such as laptops and desktops as well as non-traditional devices like iPhones, iPads, and other personal devices. Unified Access is an integrated solution that brings together security, mobility, management, and intelligent network infrastructure to target and solve key business problems. Unified Access clearly illustrates the importance of network infrastructure as the foundation for intelligently and dynamically solving network access challenges.

In Unified Access 1.0 we describe how businesses can deliver a consistent access experience for their employees regardless of network access location or device and deliver a consistent authentication method using wired or wireless devices. Context-awareness is introduced to the wired network to help businesses understand from where a user or device is physically accessing the network. Finally, UA helps businesses understand, in real-time, who and what are currently on the network.

Business Problems

The Unified Access solution addresses the following business problems:

- Network Access Experience
- Authentication for Wired Devices
- Securing Remote Access
- Securing Smart Phones
- Physical Location of Network Access
- Real Time Network Usage

Network Access Experience

One of the biggest frustrations employees face is the different methods required to access their employer's network based on their location. An employee sitting at a desk in their cubicle plugs their laptop into the network, logs in, and gets connected to the network. That same employee in a conference room logs in to the operating system, associates their computer to the wireless system, and enters their username and password to access to the network. At home with their laptop, they log into the operating system, associate their computer to their home wireless system, enter their wireless username and password to access their home network, launch a VPN client connect to their employer's network, enter a username and a one-time password, and then finally access the network. If access policies change,

software is modified, or their laptop is replaced, the employee must re-learn all these steps. If an employee received an iPad as a gift and wants to access the corporate network, then the employee must learn all of these different combinations for that device.

Authentication for Wired Devices

When an employee accesses an employer's network on-campus using wireless technology, there is almost always a need to authenticate that device to make sure it should have access. Companies do not want unauthorized users on campus using their devices to access the internal company network. However this logic is rarely applied to wired ports in the company, which means anyone that gains access to a campus building can plug a device into a port and access the internal company network, without the need to actually authenticate in any way. Disgruntled employees, hackers, and people with bad intentions can bring personal wired devices, plug them in, and gain network access with the intent of gathering confidential information, launching attacks against the company, or generally disrupting network resources.

Securing Remote Access

Companies generally have tight network controls about who can access what information when on campus. Network administrators use access control lists and operating system security settings to ensure compliance with security policies. However when the employee leaves the campus, enforcing a security policy becomes much more difficult so most companies resort to turning their remote access employees into second-class access entities by placing strict access rules in place, making them enter through a separate area called a DMZ. In general companies want to mitigate risk, however it makes some network resources unavailable to remote workers or, if the network as a whole is made available, then the remote worker becomes a higher risk due to the lack of policy controls.

Securing Smart Phones

As more and more "smart" devices become available, it is natural for employees to want to use them to accomplish business goals. The invention of smart phones, such as the iPhone and Blackberry, as well as the introduction of new computing platforms, such as the iPad and Droid operating systems, can lead to severe security risks. The device being used is normally employee-owned and the "apps" running on it probably are not limited to productivity tools. In fact, many of the apps could have serious security implications. Should a company let an employee on their network with a personally-owned device? If the device is allowed on the network, from where should access be allowed? Only on-campus, remotely, or both? How will companies ensure that personal devices do not violate security policies? These devices can lead to greater employee response and benefit the company, but they also pose very serious security risks as well as the added IT support these devices require.

Physical Location of Network Access

As companies become larger, their facilities also grow. It is easy to determine from where someone is physically accessing the company network when you only have 20 employees, but how about when you have 200, 2,000, 20,000 or 200,000? How do you know where an asset, such as a printer, laptop, or video conferencing device, actually plugs into the network? The lack of visibility can lead to business problems, such as how do you locate someone that is performing malicious activity on your network? How can you inventory the devices on your network and actually know where they reside? What happens

when a device gets misplaced and you have to find it? How can you enforce location-based security policies if you do not know the location of the person/device accessing the network? Understanding the context around where a device enters the network is the foundation of understanding and enforcing network access policies.

Real Time Network Usage

Network administrators face a fundamental problem today in that they do not know who is actually connected to the network. Their servers can indicate who is accessing them by using programs that operate on the server operating system. However to determine what devices are physically connected to the network, you can enable authentication, which lets you know who entered the network, but rarely lets you know if they disconnected. You can enable troubleshooting tools to see what traffic is traversing the network, but it is very time consuming to piece all that traffic into a list of devices. You can enable SNMP management tools to send traps to a management server to keep a list of every time a port turns on, but this is very limited information. You can initiate a port sweep to try to discover every device, however most personal firewalls simply drop this traffic, treating it as unsecured traffic. Hence the ability to actually take a snapshot of what devices are on the network at any given time is a great tool to understand inventory, find outdated equipment that should be removed from the network, and generally understand the makeup of the network end points. Finally, what would be even more beneficial would be to actually know the user name associated with the device on the network.

Pillars of Unified Access

The Unified Access solution brings together security, mobility, and management running over an intelligent routing and switching infrastructure to show how these items working together as a system can be used to solve specific business problems.

Note This document is version 1.0, which will be updated to include additional business problems that are specifically addressed by the Unified Access solution.

To fully understand the approach this solution takes, a brief description of the pillars of Unified Access is provided.

Security

Security comprises many broad technologies that work together to ensure that the right user or device is allowed to access the company network and they are only allowed to access resources based on the security policy of the company. Sometimes security is mistakenly believed to be a specific device, such as a firewall or intrusion prevention system, but in reality those are just different tools in the security arsenal. A true security system is made up of network devices that have the ability to authenticate, authorize, and perform accounting on the network. It also includes having the right authorization servers to perform those tasks. The ability to create access controls on the network device is also critical for security policy enforcement. Devices such as firewalls also play a role in a true security system to ensure traffic traversing in or out of the company network complies with the security policy and that unwanted traffic is dealt with properly. All these items working together constitute what a network security system actually represents. So, as a part of the Unified Access solution, security means much more than a single device; it is everything described above working together to ensure that security policies are enforced.

Mobility

Unified Access sees mobility as much more than a company's wireless system. Mobility truly represents the ability to work anywhere, whether on-campus, off-campus in a coffee shop, at the home office, or connected by wires or wirelessly. Mobility is the ability to offer the appropriate services to the end user based on where they are, what device they are using, and how they are connecting to the network. The services made available and the connection used should be dynamic and not require the end user to have to perform tedious tasks. In Unified Access mobility is made up of wireless access points, wireless controllers, mobility service engines, VPN devices, and mobility software working directly with the intelligent routing and switching infrastructure to deliver secured anytime, anywhere access to the network.

Management

Unified Access defines management as:

- Having the ability to understand the network, how it is reacting, and what is being used on it
- Easing deployments
- Having a central location from which the network administrator can operate the company network

Management is a non-technology specific item. Management can mean:

- Deploying security features, such as identity-based networking using configuration templates, to routers and switches
- Having a list of every device on the network and where they are located
- Having a location where intelligent network devices actually send alerts to notify a network administrator of a situation on the network

The key to managing a network is to have the management station act as the coordinator of the network, allowing it to interface with routers, switches, security systems, mobility systems, and any other part of the network to build a holistic view of the network and to make operating the network easier.

Unified Access 1.0 Solution

In Unified Access 1.0 we tie solving the above business problems into specific chapters. Some of the chapters address multiple business problems and include:

- Chapter 3, "Secure Unified Access Experience"
- Chapter 4, "Context-Awareness for Wired Devices"
- Chapter 5, "User and Device Network Access Reporting"

The following subsections provide an overview of each chapter.

Bring Your Own Device—Unified Device Authentication and Consistent Access Experience

The chapter focuses on identifying and authenticating users connecting to the network from different places with different devices over different connection media. The devices can be categorized as laptops, desktops, and smart phones, the places can be on the campus or remote, and the connection media can be wired, wireless, or over an un-trusted network.

The specific business problems that are covered in this chapter include:

- Unified Access experience whether on-campus or remote, using either a traditional or non-traditional networking device
- Wired Device Authentication for networking devices that connect to the network, including describing how to tie the authentication into existing directory systems such as Microsoft's Active Directory
- Securing Remote Access for employees that work off the network. Detailed authentication and authorization information is provided to allow network administrators to implement highly-secure, policy-based remote access.
- Securing Smart Phones for company network access. Details describe how you can enforce security policies on smart phones as they connect to the company network.

Context-Awareness for Wired Devices

This chapter focuses on applying best practices towards the enablement and use of Cisco Context-Aware Services for wired endpoint location tracking in Unified Access solutions. It is intended as a guide to producing functional designs that incorporate the Cisco Mobility Services Engine (MSE) and Cisco Wireless Control System (WCS) to help fulfill common business needs in enterprise environments. Very specific use cases of how a company can use context awareness are detailed, such as building asset inventories, recovering lost assets, and discovering user, server, and network device locations.

User and Device Network Access Reporting

This chapter describes how to use Cisco's LAN Management Solution (LMS) to collect user and device information about who is accessing the company network, what device(s) they are using, and what specific networking device are they connecting into to provide information such as:

- Current port utilization of the network
- Movement of employees and devices on the network
- Suspicious or unauthorized access to the network

Additionally, this chapter shows how companies can use historical information to provide the network administrator with:

- Historical port utilization data
- Persistent records of when users and devices accessed specific locations in the network
- Searchable data of historical access for troubleshooting and asset tracking

Overview of Topics Anticipated in UA 2.0

At the time of writing of the Unified Access 1.0 document, efforts were underway to expand the number of business problems that Unified Access will address. The Unified Access solution will be adding additional technologies and systems to address issues that companies and network administrators are experiencing. A preview of some of the high-level business problems that Unified Access 2.0 will address is provided below (subject to change).

Dynamic Policy Enforcement

Building upon the work done in Unified Access 1.0, the next step is the evolution of security policy enforcement. Unified Authorization and Accounting, along with context awareness, an intelligent network infrastructure, and the Access Control solutions, will be brought together to allow a company to have the network dynamically enforce the company's security policies.

The network administrator will be given the tools to allow them to create security policies much as is done now for server operating systems. They will be able to create groups and users and define what each user or device can access on the network based on who they are, what they are, what they can do (from a device posture standpoint), when they are accessing the network, and from what location. This gives companies the ultimate amount of flexibility to implement detailed security policies into a centralized system, which in turn works with the intelligent network infrastructure to dynamically enforce network access security policies.

Mobility Service Optimization

Unified Access 2.0 will explore business problems related to mobility services, such as providing high-quality uninterrupted video services and wideband audio to mobile devices over multiple network types:

- Build a system that will automatically mitigate RF interference in a campus wireless system and alert the network administrator to the source and physical location of that interference.
- Deliver context-aware information from the wireless environment so that network policies and management stations can understand where someone is accessing the network when they are connected via a wireless technology.

Network Device Configuration Optimization

This high-level topic will explore business problems that network administrators face when deploying new features on existing or new network infrastructure equipment. Unified Access 2.0 will also highlight how network information is gathered and shared among mobility, security, and management systems to give the network administrator central control and information about their network. Finally, the business problem of easing the level of complexity when deploying intricate solutions, such as identity-based networks, will be explored.