IP COMMUNICATIONS

Practical Cisco Unified Communications Security

Brett Hall, CCIE® No. 20774
Nik Smith

ciscopress.com

Practical Cisco Unified Communications Security

Brett Hall, CCIE® R&S, Collaboration #20774

Nik Smith

Cisco Press

Hoboken, New Jersey

Practical Cisco Unified Communications Security

Brett Hall, Nik Smith

Published by:
Cisco Press

ScoutAutomatedPrintCode

Library of Congress Cataloging-in-Publication Number: 2020916934

ISBN-13: 978-0-13-665445-2
ISBN-10: 0-13-665445-2

Warning and Disclaimer

This book is designed to provide information about the practice and methodologies used to secure a modern Cisco Unified Communications environment. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Editor-in-Chief: Mark Taub

Director, ITP Product Management: Brett Bartow

Executive Editor: Nancy Davis

Sponsoring Editor: Mudita Sonar

Managing Editor: Sandra Schroeder

Development Editor: Ellie Bru

Project Editor: Mandie Frank

Copy Editor: Chuck Hutchinson

Technical Editors: Paul Giralt, Christopher Hsu

Editorial Assistant: Cindy Teeters

Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Ken Johnson

Proofreader: Donna E. Mulder

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Credits

Figure 1-1 oOhyperblaster/Shutterstock

Figure 2-2 Kyryl Gorlov/123RF

Figure 2-4 The Wireshark team

Figure 2-22 © CYBERDATA CORPORATION 2020

Figure 2-23 Hywit Dimyadi/Shutterstock

Figure 10-6 Screenshot © 2020 Apple Inc

Figure 10-7 Screenshot © FileZilla

About the Authors

Brett Hall, CCIE R&S, Collaboration #20774, is a Customer Solutions Architect supporting Cisco's product and service offerings for enterprise customers across the U.S. Army and defense agencies. He has more than 20 years' IT experience and has worked with Cisco to support federal government initiatives for more than 13 years. He also works with Cisco business units to define product and service strategies and helps lead a global team of Cisco architects. To support customer requirements, Brett works with presales teams to engineer solutions that lead to customer adoption. Brett also drives solution development to help support future needs of his customers.

Nik Smith, Technical Leader for Collaboration at Cisco, supports Cisco Unified Collaboration (UC) products and service offerings for the public sector, enterprise, and defense agencies. His 24 years of networking experience cover technologies ranging from RF communications and telecommunications to UC. For 14 years, he has supported some of the world's largest Cisco UC deployments. During this time, he has led several large implementation teams involved in migrating from TDM to VoIP, along with network support and modernization. He now leads a team of UC engineers supporting the public sector, Department of Defense and providing guidance and mentoring to ensure that Cisco delivers best-in-class, highly secure UC capabilities.

About the Technical Reviewers

Paul Giralt, CCIE R&S, CCIE Voice, CCIE Collaboration #4793, is a Distinguished Engineer in the Customer Experience organization where he focuses on Cisco collaboration technologies and has been with Cisco since 1998. He spends much of his time helping customers accelerate the adoption of Cisco technologies and solutions and building services capabilities to provide more proactive and predictive services as well as improve product serviceability. Paul has spent his career at Cisco in the TAC, the Collaboration Technology Group, Solution Validation Services, Cisco Advanced Services, and most recently as part of the Customer Experience organization. He has spent years troubleshooting and diagnosing issues on some of the largest and most complex Cisco Collaboration deployments. Paul is passionate about the intersection of programmability and Cisco Collaboration products as well as making it easier for customers to diagnose issues on their own. He is also the author of the Cisco Press book *Troubleshooting Cisco IP Telephony* and a member of the Cisco Live Distinguished Speaker Hall of Fame Elite. He holds a degree in computer engineering from the University of Miami.

Christopher Hsu is a Solutions Architect in the Cisco Unified Collaboration domain. He has over 20 years of extensive hands-on experience in designing and implementing Cisco Unified Collaboration technologies. He has been with Cisco for 14 years and specializes in large-scale Unified Collaboration solutions. He has certifications in CCIE and CISSP.

Dedications

Writing a book for Cisco Press has always been a bucket list item for me. Despite all of the craziness in my day job, my wife understood this and allowed me to pursue my dreams of writing this book. I cannot thank my wife, Wendy, enough for the patience, understanding, and support that she has provided me during the writing process, but more importantly the past 20 years that we have been married. I also would like to thank my kids, Gabriel and Hannah. You understood the stress that was accumulating during those late nights and didn't hold it against me as I raced toward the finish line. I pray that this example will leave a lasting impression on you to always chase your dreams and to work hard in the process of doing so.

—Brett

I would like to thank my wife, Elizabeth, and kids, for putting up with me while I worked on this book. The immense patience they showed makes me even more grateful for having them in my life. I especially want to thank my wife for checking on the progress of each chapter I wrote. You're an amazing PM, and yes, now I can get started on the honey-do list you've been compiling over the last couple of months.

—Nik

Acknowledgments

Sometimes it is not what you know, but who you know and the support system that you have around you. I want to thank God for blessing me by putting me in a place in my career where I had such a tremendous team surrounding me with mentorship and engineering talent. I also would like to acknowledge the people who have been willing to help when I needed it most. Depending on whether I lacked perspective or knowledge in certain areas, the team around me has never hesitated to give me a hand.

Cliff Potts and Paul Giralt, you have both been great mentors to me and have helped me understand many things. This book would not be possible without either of you. Nick Russo, I remember having a conversation with you about this crazy idea that I had about UC Security. You helped connect me with Nik, who had a similar idea so that we could make this book a reality. Also, for those I managed to cajole into either helping me with my lab environment or providing a second set of eyes for my work—Dave Fusik, Baron Rawlins, Dan Keller, Hussain Ali, Kevin Roarty, Laurent Pham, Tony Mulchrone, Joe Tansey, Vernon Depee, Robbie Horgan, Jason Newman—I owe you guys one!

—Brett

Over the years I've been blessed to have the chance to work with numerous exceptional engineers who have helped me become the engineer that I am today.

Dan Gallagher, you are a mentor to me and one of the most productive, knowledgeable, and prepared people I have ever had the pleasure of knowing.

Dave Duncan, you are and always have been that calm, reassuring voice at 2 a.m. in the middle of a change going south. You've kept us on track and even-keeled many a time with your demeanor and in-depth knowledge of UC and data networking expertise.

Bill Donaldson, among the engineers I've worked with, I'm pretty sure I've worked with you the longest. Thank you for being able to provide an alternative point of view to a design or solution to a problem.

For this book specifically I was very lucky to be able to work with Paul Giralt and Chris Hsu as my technical editors. You guys were brutal, and I hope I did your comments justice. I also want to thank Laurent Pham and James Arias for giving me a second set of eyes on a couple of the chapters. It would have been a lot more difficult without your inputs.

Lastly, I want to give a special thanks to Franklin Hall, who got me interested in VoIP so many years ago.

—Nik

Contents at a Glance

Contents

Icons Used in This Book

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in Cisco's Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets [ ] indicate optional elements.
- Braces { } indicate a required choice.
- Braces within brackets [{ }] indicate a required choice within an optional element.

Note This book covers multiple operating systems, and a differentiation of icons and router names indicates the appropriate OS that is being referenced. IOS and IOS XE use router names like **R1** and **R2** and are referenced by the IOS router icon. IOS XR routers use router names like **XR1** and **XR2** and are referenced by the IOS XR router icon.

Introduction

Security in a Unified Communications network has become an essential aspect that organizations must account for in any modern UC environment. The purpose of this book is to provide a solid foundation to those individuals interested in learning the methodologies and technologies involved in securing a UC environment. In simple terms the purpose of this book is to start the conversation about how to secure a UC environment and where to look for more information.

Our goal in building the foundational knowledge for UC security is not to simply restate the various Solution Reference Network Design (SRND) guides or other configuration guides. The goal is to provide practical examples of when and how to secure aspects of the UC environment while providing direction on where to look for more detailed explanations of the technologies.

The methodology used in this book to convey the information is *explain, demonstrate, and verify.* Using this method, we first explain the concept (why is this being done). We follow up with a demonstration (how this is implemented). Lastly, we provide the process to verify the security aspect implemented (how you know it worked).

Goals and Methods

The primary focus of the book is that of helping Collaboration engineers and IT managers understand the need for security in their Collaboration environment and how to implement it. The content is intended to provide a foundation for the concepts and technologies used to secure modern Collaboration environments. The structure of the book is to first explain the concept and then walk through the configuration process. Lastly, this methodology will aid engineers and IT leaders in understanding how to verify their Collaboration environment is operating in a secure manner.

The core sections of the text show how to secure a modern Cisco UC environment that supports voice, video, IM, and presence to include the integrations with other real-time Collaboration technologies that facilitate Mobile and Remote Access (MRA) and bring your own device (BYOD). We also help you understand the reference network design to support UC services; portions of text are dedicated to helping you understand the attack surface and how to secure sections of the network in a logical progression through the different Cisco UC application domains.

We provide the relevant reference links for a more in-depth explanation as required. Chapter summaries provide a quick checklist of the learning objectives covered.

Because we provide the consolidated leading practices to protect a Cisco UC environment using the methodology of *explain, demonstrate, and verify*, you are afforded an understanding of the threat that is being protected against, followed by the steps to implement the security features, and lastly how to verify that the implemented security features are working.

Who Should Read This Book?

The book's primary audience is administrators and leaders who are planning to implement or are interested in improving their Collaboration security. One of the challenges for those who are interested or required to secure UC environments is the need to utilize numerous different resources to find the proper steps to secure systems, and unfortunately, the reasons are often not fully explained. This book provides the "why" that is often missing from the documentation and provides the foundational knowledge of current threats to a UC environment.

This book is intended for those with an intermediate level of understanding of the applications being discussed. You then will be able to take the information from this book and ensure that your Enterprise Unified Communications environment is deployed to the highest security standards and aligned with industry leading practices, giving you the best chance at achieving all levels of compliance to various types of security audits and inspections.

How This Book Is Organized

For those who are linear thinkers, our writing style is for you. This book takes you on a natural progression of securing a Unified Communications environment. Starting with the basic principles of security (physical security), we also include how to provide life and safety solutions for the most important asset of an organization: its workforce. From there, we progress to helping you understand the importance of securing the network before the UC applications, because the network is often the second point of insertion for an attacker (after physical). In a practical way, we spend time explaining how to enable security features on core components of a UC environment, which are the UC applications hosted within the network. Lastly, we communicate the importance of securing the edge of the network and UC services that are located outside of a traditional on-premise environment to help you understand what implications there are when consuming services from a cloud environment. Using a fictional case study to provide a basis for thought, we employ a storytelling style to help simplify the message.

Although there is a natural progression for securing UC environments, we have written chapters so that you can focus on specific areas of interest, ensuring that you do not miss out on introductory material if you decide not to read through the book from start to finish. Given this information, however, we recommend reading through each of the chapters. Because security is often about exploiting the weakest link, we recommend thinking about security from an architectural perspective. This is also how you will be able to get the full benefit of the book.

Chapter 3

Security Through Network Fundamentals

In this chapter, we discuss the dependencies that Unified Communications (UC) systems have on the network while also highlighting the security features that can be implemented to provide additional security to the UC environment. In its most simple form, a network's purpose is to help connect things. In the case of most organizations, these things include personal computers, printers, phones, and mobile devices. To enhance a network's capabilities, various features can be enabled to help simplify the user experience. In this case, there must be a balance to make sure that the process of how the different types of devices connect to the network is not oversimplified. Otherwise, it is security that is often left out.

A sophisticated attacker understands how an organization's critical services are built and also understands how to leverage weaknesses in the architecture to launch attacks. While implementing various protocols and features, Cisco provides many enhancements that can be beneficial to network security as well as Unified Communications security. By the end of this chapter, you should have an increased understanding of how the network can be used to safeguard against the most common threats used against the various protocols that exist within a Unified Communications environment. This chapter also provides a fundamental approach for increasing the amount of security on the network to protect against common threats and different types of attacks.

Working with ACME's Network Team

A recent network audit has determined that ACME has failed to maintain compliance with the Mechanized Equipment Specifications and Standards. ACME leadership considers this a serious issue. If the company is unable to resolve network issues in 90 days, it could be penalized financially, and it could possibly lose some of its existing customers to competitors.

ACME's Chief Operating Officer (COO), Dr. Nicholas Fury, has invited all of the IT leaders to a series of meetings to determine the options that they can take to gain compliance to industry standards in a short and operationally effective way. Dr. Fury has also invited leaders from business units to a series of meetings to develop a list of requirements and priorities so that the IT leaders can develop a strategy for modernization efforts that will help business units increase sales and productivity to meet ACME's growth targets. Business unit leadership wants to take advantage of this opportunity by deploying additional security solutions that would allow the company to collaborate with business partners and integrators in a secure fashion.

Network leadership seems to be interested in implementing both network virtualization and network access control solutions to improve the ability to segment the network and strengthen the security at the edge of the network. Fortunately, several members from the UC team have a network background and have established good working relationships with the network and data center teams, so they are willing to work together if doing so means getting back into compliance in a more streamlined fashion.

ACME's newly hired UC administrator, Anthony Starke, is responsible for articulating the network requirements for the UC environment and making recommendations to get back into compliance. Anthony is a bit overwhelmed with this challenge because he does not have a lot of real-world experience with network security, so he has scheduled a series of planning meetings with the network team to collect details about the proposed security enhancements. Anthony believes that this will help him understand which security enhancements are being proposed, allow him to recommend specific features for ACME's UC environment, and develop a better relationship with the network team members.

After an interview with the manager of the network team, Anthony has discovered that not only has ACME failed a recent network audit but that ACME's network was hacked. As part of the network audit, ACME decided to hire a team of penetration testers to discover how much security the network had in place. One of the penetration testers was able to gain access to the network through MAC address spoofing. According to the reports, a MAC address was obtained from the IP phone located in the lobby of the building. After changing the MAC address of his laptop, unplugging the IP phone, and plugging his laptop into the same network port, the penetration tester had access to the entire voice VLAN.

According to network team members, they had only recently implemented Cisco Identity Service Engine (ISE), so they were in the initial stages of deploying 802.1x to a portion of ACME's network. To make sure that the UC environment was functional, they temporarily decided to use MAC Authentication Bypass (MAB) until they were ready to roll out 802.1x for the UC environment. Anthony has been asked to prepare a briefing that helps the network team understand how to further prevent MAC spoofing attacks and to provide a status update for which IP phones support 802.1x, what methods can be used to support 802.1x, and where IP phones are located across ACME's network.

Informally, Anthony is wondering whether MAC spoofing attacks will continue to be a risk that he needs to worry about until he can get funding to replace the older IP phones. In the

meantime, he decides to go back to his UC team to figure out what challenges he should expect to encounter when ACME's IP phones will use 802.1x authentication to join the network.

Questions that you should ask:

1. What network security is currently in place to protect the UC environment?
2. What network features help increase the availability of the UC environment?
3. What mechanisms exist to provide continuous monitoring of the network?
4. What authentication and authorization policies are in place for UC endpoints?

Introduction to Network Security

After physical security, the second layer of defense for the UC infrastructure is the network. Following the Open Systems Interconnection (OSI) model, the various layers include Data Link, Network, and Transport. To best secure connectivity across these layers, experts have traditionally recommended use of defense-in-depth principles. The recommendation is no different when securing UC applications inside an organization. Cisco recommends that security be implemented at the edge of the network, starting at the access layer. From the access layer, organizations can continue to extend security into the distribution layer or layer on additional security features across the rest of the network and at the network perimeter. When the system is secured properly, organizations can seamlessly and securely connect to services in a cloud environment or allow remote teleworkers to connect to local resources. We address these topics in more detail in Chapters 11, "Securing the Edge," and 12, "Securing Cloud and Hybrid Cloud Services."

Using the access layer as a starting point for implementing security allows organizations to minimize the attack surface without encroaching on the availability of the UC applications, which reside in the data center. A methodology and practical approach for implementing security in the network for UC involves a three-step approach that involves

1. Segmentation (logical)
2. Secure network access
3. Security features

This security approach enables an organization to secure the environment while maintaining optimal performance. The idea is to develop a modular approach, which allows for the addition of security anywhere in the network while minimizing complexity and not interfering with operations. Extending security into the rest of the network is based on the existing network architecture and which types of network devices are used to support the different layers in the network, such as in the distribution layer, and also the devices used to support server infrastructure, which typically resides in the data center.

Segmentation

A best practice in today's networks is to provide logical segmentation through the use of virtual LANs (VLANs). Within a UC environment, this approach is implemented on access switches at layer 2 in the form of voice VLANs and also at layer 3 to prevent attacks on an IP subnet by applying access control lists (ACLs) on VLAN interfaces. By segmenting UC and data traffic, organizations can reduce the attack surface to which attackers have access. Ideally, attackers would have access only to the segment they are connected to. Segmentation also helps with simplifying the network by allowing an administrator to view and distinguish the different types of traffic that traverse specific interfaces in and out of the logical network. By segmenting the network (virtually) into smaller networks (in this case, VLANs), administrators can easily control the types of traffic that are permitted across different layer 2 and layer 3 interfaces to prevent unwanted traffic.

Dedicated UC and data segments also help minimize the size of a broadcast domain, which reduces the amount of traffic flooding across a network. Within a single VLAN or broadcast domain, there is potential for devices to generate (and flood) the network with traffic, which can be problematic from a security perspective. We discuss this issue later in the section on security features. Large broadcast domains also have the potential to impact the performance of the network. When segmenting a network, an organization is better insulated from a broadcast storm or denial-of-service (DoS) attack. This way, only a portion of the network can be disrupted if an attack were to occur on a particular VLAN. Cisco best practices currently recommend limiting the size of a logical segment to 256 devices, if possible, and not to exceed 512 devices.

When an organization uses the latest IOS-XE platforms (e.g., 16.9), the data and UC networks can be logically segmented by applying configurations for data and voice VLANs on a single interface. The following example shows the syntax:

```
switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# int gig1/0/10
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 10
switch(config-if)# switchport voice vlan 100
switch(config-if)#
```

At this point, we have discussed segmentation at layer 2 of the OSI model. The next section provides additional detail about layer 3 segmentation using Virtual Route Forwarding (VRF).

VRF is a way to segment the network segmentation at layer 3 of the OSI model. VRF was originally designed for service providers to essentially provide existing and new customers with their own virtual private network (VPN) across the service provider's physical infrastructure. This solution allowed service providers to take on new customers with minimal costs, without having to worry about a customer's existing IP scheme or

infrastructure. Within a VPN built with VRFs, each VRF instance has a separate layer 3 routing table. IP packets from one VRF are intentionally isolated from other VRFs.

If the flow of UC traffic isn't taken into consideration, use of VRFs may unintentionally create user experience issues. These issues could be related ACLs inside a fusion router/firewall that break functions of a UC environment, such as screen sharing. Additionally, their use could cause issues with performance by introducing latency, jitter, and/or packet loss as traffic is routed between interfaces on a fusion router or firewall during a time in which the network has high utilization. As an example, an organization decided to segment the network with VRF. To minimize the attack surface, it decided to create VRFs for each line of business (sales and marketing, research and development, support) and also for each device type (e.g., printer, IP phone, Internet of Things [IoT] sensor). The belief was that creating specific groups would simplify how ACLs are applied on the network, with a fusion firewall that supports group-based security policy. During testing, engineers were able to print, make phone calls between IP phones, and access shared resources. Unfortunately, network administrators didn't consider all of the network requirements for a UC client such as Jabber. Therefore, they unintentionally created firewall policies that prevent Jabber calls between IP phones.

Certainly, changes can be made to network policy, especially to help resolve problems as they arise. Some questions that a UC administrator can ask to proactively prevent issues with VRF include but are not limited to

- Will a VRF disrupt the user workflow or calling patterns?
- Where will the inter-VRF routing take place to ensure a quality user experience between UC endpoints (e.g., Jabber, IP phone, video device)?

It is important to realize that care should be taken when designing segmentation in the network to ensure that the network supports the desired features within a UC environment. It is also important to make sure that the network does not force UC traffic to flow across the network in ways that are less than optimal to help avoid the addition of latency, delay, and jitter.

At this point, we have discussed basic segmentation as one approach for providing security at different logical layers of the network so that organizations can apply security controls at whichever level of granularity is necessary to comply with security policies. Basic segmentation by itself, which logically separates different types of devices or business entities, can be referred to as segmentation at a "macro" level. As part of a defense-in-depth approach, another layer of segmentation is possible to further reduce the attack surface. This approach is known as micro segmentation, is discussed next.

Micro Segmentation

Micro segmentation has many security benefits. As previously discussed, it can be very effective in preventing specific unwanted traffic flows within a VLAN segment. One specific use case of micro segmentation may be to restrict the spreading of malware laterally

within a VLAN (that is, spreading of malware to neighboring devices) by only permitting specific protocols that are expected across a network. As an example, a micro segmentation policy would allow a network administrator to instruct the network to allow only PCs with a UC client, such as Cisco Jabber, to establish VoIP calls with other PCs running the Jabber client over specific TCP/UDP ports that have been designated for UC. This type of granularity allows UC clients such as Jabber to function exactly as a user expects by supporting all of the UC features, such as instant messaging, VoIP/video calling, and content sharing. It also helps meet security requirements to minimize the attack surface on a network by denying specific protocols that may traditionally be used by worms, malware, or an attacker.

Customers who previously had requirements to restrict access within a network segment such as a VLAN have traditionally been limited to either VLANs, with VLAN ACLs (VACLs), or private VLANs. Two different modern architectures that provide micro segmentation capabilities are Cisco Software-Defined Access (SDA) and Cisco TrustSec, which offer security policy based on scalable groups. The next section provides an introduction to the SDA solution while also highlighting how TrustSec can be incorporated into SDA to obtain a deeper level of granularity for restricting traffic flows within a network.

Cisco SDA is a solution within the Cisco digital network architecture (DNA) that provides software-defined networking for the campus environment. SDA provides network security by facilitating end-to-end segmentation of network traffic between users, devices, and applications. A software-defined network, providing centralized management, allows organizations to enable security features on a more aggressive basis because there is less of a burden for enabling security across network devices on a device-by-device basis, which is often a reason that networks are not as secure as they could be. SDA also provides organizations with a means and methodology for increasing visibility of network traffic and applying network policy to wired and wireless network devices (such as switches and access points) in an automated manner as a user or devices move around a network. Using the earlier example with Jabber, SDA would ensure that the security policy that has been assigned to a user with a Jabber client will stay with that user while roaming between different places in the network (e.g., desk, conference room, cafeteria).

This type of security approach requires a paradigm shift when compared to a traditional approach of managing ACLs that are applied to network devices to protect specific IP subnets. Using an architecture, such as SDA, security controls are no longer based on IP subnets. Security controls are associated with the identity of a user or device. This is why a policy can still be assigned to users as they roam around a network. The following components are required to support SDA:

- **Cisco DNA Center (DNA-C):** This component provides centralized management of network infrastructure; it is used to create policies (e.g., security, QoS) and automate provisioning of software features and images across network devices. It also provides visibility into network incidents, network telemetry, and analytics.
- **Cisco Identity Services Engine (ISE):** This component integrates with DNA-C to provide access controls (e.g., ACLs, dynamic VLAN assignments), group-based

policy, and policy enforcement. It integrates with external repositories such as Active Directory for authentication and authorization.

- **Network infrastructure (wired and wireless):** This infrastructure includes network devices, such as Catalyst switches and access points.

The last element that is included inside an SDA solution is the network fabric. The network fabric is essentially a virtual network that is overlaid on top of the existing physical network with a separate control and forwarding plane. The separation of the control plane from the forwarding plane helps improve the overall performance and scalability of the solution while also simplifying policy, provisioning, and management. As an example, it allows network administrators to provide a consistent policy to a user/device as it moves around the network. To do this, DNA-C and ISE work in unison with network devices to enforce policy that either permits or denies the different types of traffic allowed across a segment of the network. Figure 3-1 depicts a sample SDA solution.

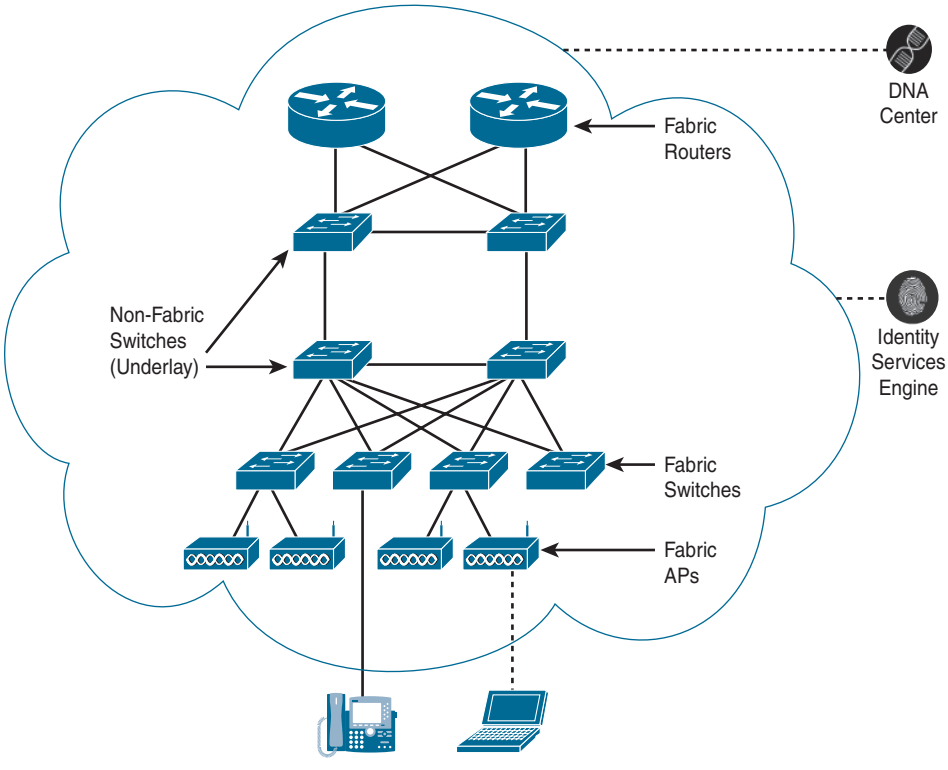

Figure 3-1 *SDA Solution Featuring DNA Center, ISE, and Network Fabric*

Now that we have introduced SDA, we must also introduce a few more key terms regarding how the SDA solution provides security:

- **Virtual network:** This network provides logical separation (macro segmentation) between devices and other virtual networks. This is analogous to a Virtual Route Forwarding technology.
- **Scalable group:** This mechanism for grouping functions or devices is based on business roles (e.g., employee, contractor, finance, printers, IP phones). Once a group is created, a unique scalable group tag (SGT) is assigned to the scalable group to provide micro segmentation. This security concept is based on Cisco TrustSec.
- **Contracts:** These are used for enforcing policies that have been created within DNA-C to specifically permit or deny certain types of traffic. They are also known as security group ACLs (SGACLs).

At the time of configuration, an administrator needs to align to the virtual networks that have been previously defined by an organization. Because we have been discussing how to create a micro segmentation policy to support UC security within DNA-C, we can use DNA-C as the central place of management and policy configuration. To follow this example, you should take the following steps:

1. Define virtual networks (e.g., ACME_HQ).
2. Define scalable groups (e.g., ACME_UC, ACME_WIDGETS, Employees, Contractors, Printers).
3. Assign scalable groups to virtual networks. This process allows access to resources within a virtual network (e.g., it allows employees and contractors to communicate with IP phones and printers).
4. Create contracts (e.g., Permit_VoiceUDP) that specify the traffic flows that are allowed within scalable groups using SGACLs.
5. Deploy the micro segmentation policy to network devices.

An example of step 3 is provided in Figure 3-2, and an access contract is provided in Figure 3-3, showing how an administrator can permit VoIP traffic on an SDA environment.

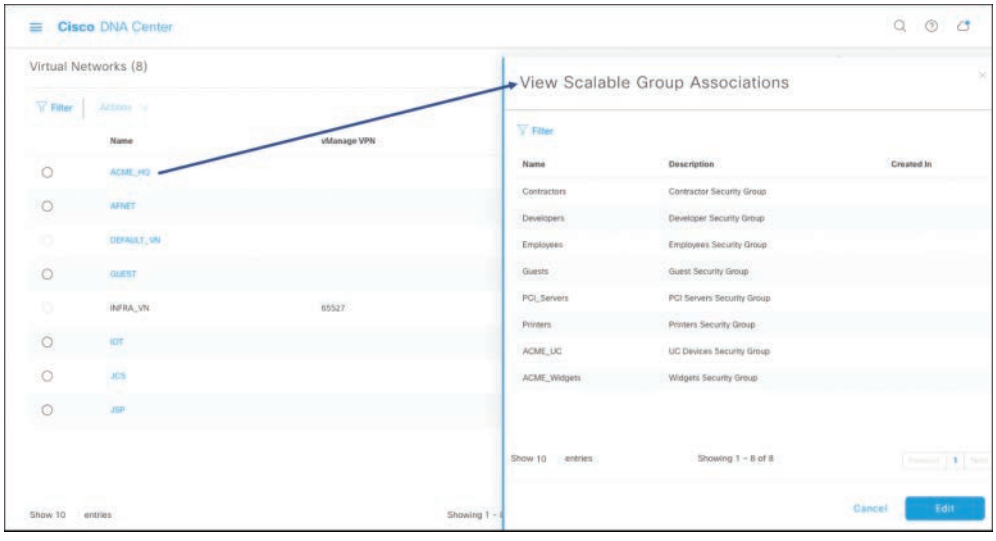

Figure 3-2 *Assigning Scalable Groups of Resources to a Virtual Network Within DNA Center*

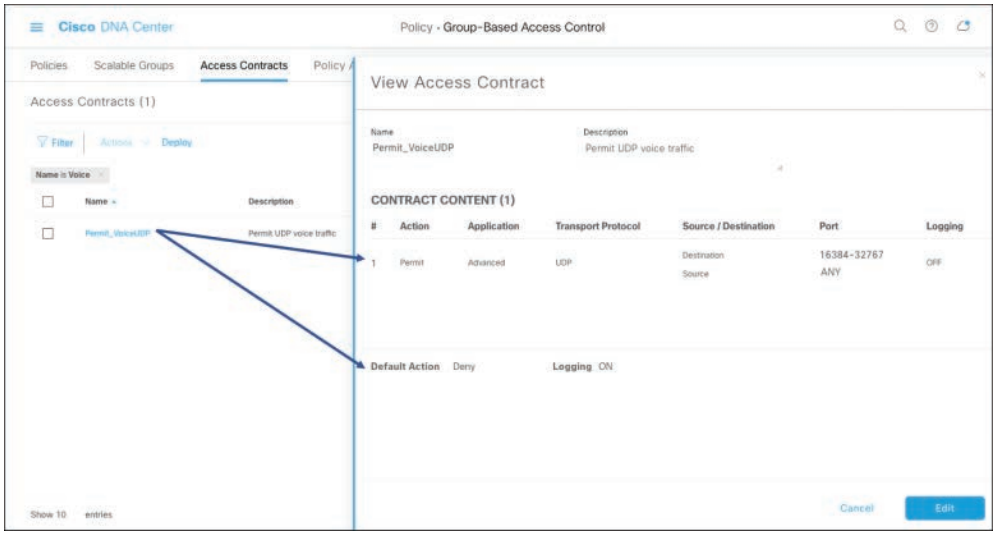

Figure 3-3 *An Access Contract Created Within DNA-C to Permit UDP-Based VoIP Traffic, While Denying All Other Types of Traffic*

Once the scalable groups and the associated contracts are defined in DNA-C, they are then also shared with ISE over a RESTful API. This setup allows ISE to be the authoritative point of security enforcement across the network. An example illustrating how ISE imports the policy from DNA-C and creates security group ACLs to enforce policy is included in Figure 3-4.

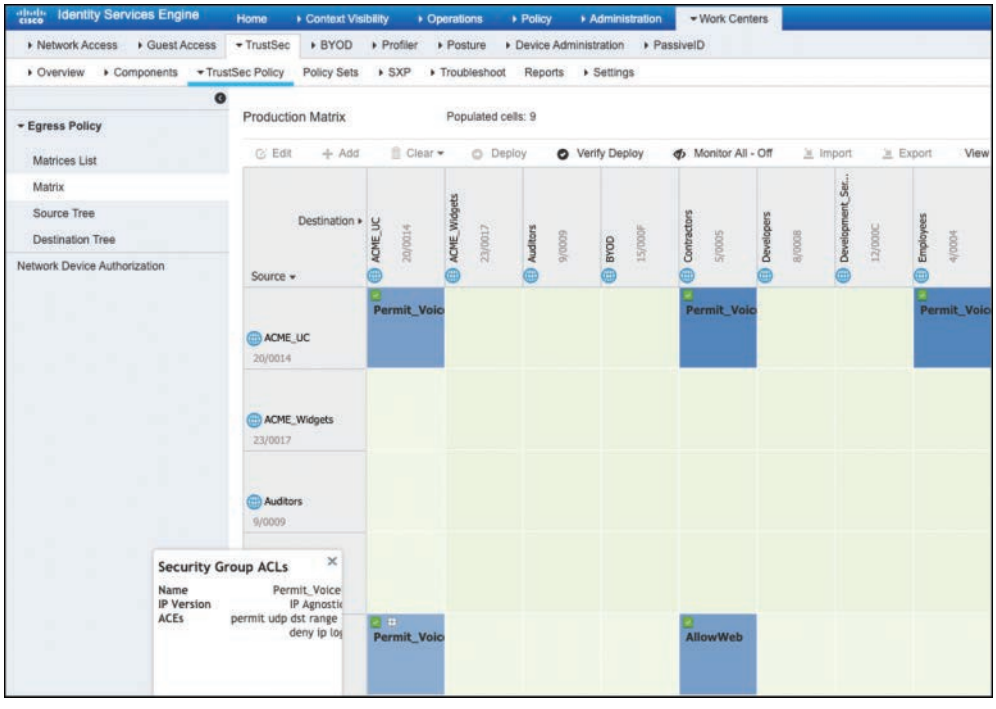

Figure 3-4 *A Micro Segmentation Policy Within Cisco ISE to Permit VoIP Traffic Between Scalable Groups*

Due to the simplicity involved in this type of workflow, organizations are able to respond to new security threats while reducing operational costs by using a centralized policy engine such as DNA-C. As the threat landscape continues to grow, organizations may need to adopt micro segmentation capabilities to gain more granular security controls instead of the traditional macro-based segmentation approach. It is beyond the scope of this chapter to cover all of the necessary steps needed to design, configure, and provision VRF, DNA-C, ISE, and the network to support SDA. For additional information about SDA, visit www.cisco.com/go/sda.

Secure Network Access

Providing security at the edge of the network is perhaps the most overlooked approach for UC security despite the power that it can bring to an organization and the simplicity involved. Put simply, if an organization can strengthen how users and UC devices join the

network, it can help reduce the attack surface that attackers have access to while making it easier to protect against UC attacks. Security at the edge of network access comes in many forms. The oldest, and perhaps most common, is through use of switchport security. The strongest approach is through implementation of 802.1x authentication. The next few sections explain in more detail how port security can help an organization and show how it is configured. After that, we transition over to 802.1x authentication and then wrap up by covering what can be considered the middle ground—MAC Authentication Bypass (MAB) and how MAB can be further secured when using Network Access Control (NAC).

Port Security

The port security feature enables organizations to specify what identities can join the network by specifying which MAC addresses are allowed. Port security has traditionally been popular because it provides an easy way for an organization to limit the number of devices that are allowed to connect to an access port and prevent shadow IT.

As an example, port security can help prevent a user from plugging in an access point that has not been previously sanctioned by the IT department to add wireless capability. Port security is also useful for protecting against attacks against the network, such as flooding the Content Addressable Memory (CAM) table on a switch with false MAC addresses to create a man-in-the-middle attack.

If an organization chooses to use port security at the edge of the network, administrators should know that Cisco switches do not support explicit configuration of MAC addresses for the voice VLAN. Therefore, administrators should consider allowing a maximum of two MAC addresses to connect to each switch port to account for the IP phone and the PC plugged into the back of the IP phone. If any type of port security is enabled on the access VLAN, dynamic port security is automatically enabled on the voice VLAN.

To enable switchport security, you need to take the following steps:

1. Specify the maximum number of MAC addresses allowed on the network:

```
switch(config)# int gig1/0/1
switch(config-if)# switchport port-security maximum 2
```

2. Specify the MAC address that is permitted for the network port(s):

```
switch(config-if)# switchport port-security mac-address
00cc.fc98.1b10
```

3. Specify what action to take if the switch doesn't recognize a MAC address that is trying to join the network:

```
switch(config-if)# switchport port-security violation restrict
```

4. Enable the switch port for port security:

```
switch(config-if)# switchport port-security
```

When the **restrict** key word is used, and a violation occurs, an SNMP trap is sent, a syslog message is logged, and the violation counter increments. The other options are to protect and shut down. When configured to protect, the switch just drops packets with an unknown source address. When configured for shutdown, the interface becomes error-disabled, an SNMP trap is sent, a syslog message is logged, and the violation counter increments.

Now that we are discussing port security, it is important to understand that a configuration that limits the specific MAC addresses that are allowed to connect to an access port is a potential issue. This type of environment assumes that the environment is static and that a limited number of phones require Moves/Adds/Changes (MAC) around the network. If the desire is to have a dynamic but yet secure environment, the organization can convert from static MAC addresses to dynamic "sticky" MAC addresses, in which the switch converts all of the dynamic MAC addresses to the running configuration on the switch. To enable port security that is dynamic, leverage the **mac-address sticky** command, as in the following example:

```
Switch(config)# int gig1/0/11
Switch(config-if)# switchport port-security maximum 2
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security
```

This option is more flexible because sticky MAC addresses do not automatically become part of the start-up configuration file, which is the configuration used each time the switch restarts. Learned sticky MAC addresses are just added to the running configuration as shown:

```
switch# sh run int gig1/0/11
Building configuration...

Current configuration : 364 bytes
!
interface GigabitEthernet1/0/11
 switchport access vlan 20
 switchport mode access
 switchport voice vlan 100
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky f8b7.e294.6d00 vlan voice
 switchport port-security
 spanning-tree portfast
end
```

Although effective in securing network access for the common user, switchport security has some downfalls. MAC addresses can easily be spoofed or falsified to allow

unauthorized devices onto a network. If attackers do this, they can attack the network segment(s) that they are connected to laterally, unless layer 2 VLAN ACLs (VACLs) are in place. This is one of the reasons why we have previously discussed use of segmentation in the network (macro and micro). In any regard, because organizations understand the limitations of port security, many of them are moving away from this approach and toward 802.1x authentication. The next section discusses this technology in further detail.

802.1x Authentication

The IEEE 802.1x standard method of authentication is widely considered the strongest method of authenticating users and devices to the network. In typical implementations with 802.1x authentication enabled, the access port allows only Extensible Authentication Protocol over LAN (EAPoL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic to the port until an endpoint is authenticated. In addition to providing port-based authentication, an architecture that provides 802.1x offers increased visibility that may be useful for security audits, forensics, and troubleshooting. The downside of this method of authentication is that there are several dependencies on the infrastructure components. These components are not typically managed by UC administrators, so there is an element of cooperation and teamwork needed for a fully functional 802.1x solution. The basic components of an 802.1x solution include

- Authenticator (Access Switch)
- Authentication server, such as Cisco Identity Services Engine (ISE)
- Authentication database
- Client supplicant
- Public key infrastructure (PKI)

The 802.1x authenticator (access switch) helps relay authentication information over Extensible Authentication Protocol (EAP). Common EAP methods in 802.1x environments are EAP-MD5, EAP-FAST, EAP-TLS, and Protected EAP – Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2). EAP-TLS uses certificates for client/server authentication, whereas EAP-MD5, EAP-FAST, and PEAP-MSCHAPv2 use passwords for authentication. Cisco Catalyst switches fully support authentication of UC devices and PCs through the use of multidomain authentication (MDA) configuration parameters.

The authentication server, such as Cisco Identity Services Engine, provides authentication, authorization, and accounting (AAA) for devices trying to access the network by leveraging standards-based protocols, such as EAP over LAN (EAPoL) and Remote Authentication Dial-In User Service (RADIUS). The authentication server enables organizations to create flexible and granular security controls as they request access to the network and once they have authenticated to the network by incorporating authorization policy. In practical terms, this means that administrators can dynamically place

authenticated users and devices into separate logical network segments and apply certain security policies to those groups and devices. Within ISE, this is done with downloadable ACLs (dACLs).

An authentication database, such as Microsoft Active Directory or ISE, is a critical component of an 802.1x authentication implementation. The authentication database holds the credentials of the users to be authenticated in a centralized location. This type of solution provides the ability to align with organizational security policies. If users do not update their credentials, they are cut off (or restricted) from acquiring network access based on the authentication policy that is configured.

A client supplicant is software running on a device that attempts to gain access to the network. Operating systems such as Windows and OS X provide native supplicants to aid with 802.1x authentication. Software such as Cisco AnyConnect can run on top of an OS to also provide a supplicant. Last but not least, the firmware on Cisco IP phones also has a native supplicant for performing 802.1x authentication to a network. The next section discusses this topic in further detail.

The current release of the native supplicant inside a Cisco IP phone leverages either EAP-FAST or EAP-TLS for 802.1x authentication. EAP-TLS is the only option that supports X.509 certificates to simplify the 802.1x authentication process. The two different certificate types that are currently supported are the manufacturing installed certificate (MIC) and a locally significant certificate (LSC). A MIC is preinstalled at the factory during manufacturing of the IP phone and signed by one of the Cisco Manufacturing CA certificates:

- Cisco Manufacturing CA
- Cisco Manufacturing CA SHA2
- CAP-RTP-001
- CAP-RTP-002

These certificates are important because for ISE to successfully authenticate a phone onto the network via 802.1x, it needs to be imported into the ISE's trusted certificate store. From a certificate perspective, one thing that we must discuss is a certificate's chain of trust. This chain is important because it validates the authenticity of an X.509 server (or phone) certificate. Three components are needed to establish a chain of trust between certificates:

- **Root certificate:** An X.509 certificate that belongs to a certificate authority. It is used to issue other certificates.
- **Intermediate certificate:** An X.509 certificate that is subordinate to the root and issues server certificates.
- **Server certificate:** An X.509 certificate for a specific server or device.

A phone certificate and its certificate trust chain are shown in Figure 3-5.

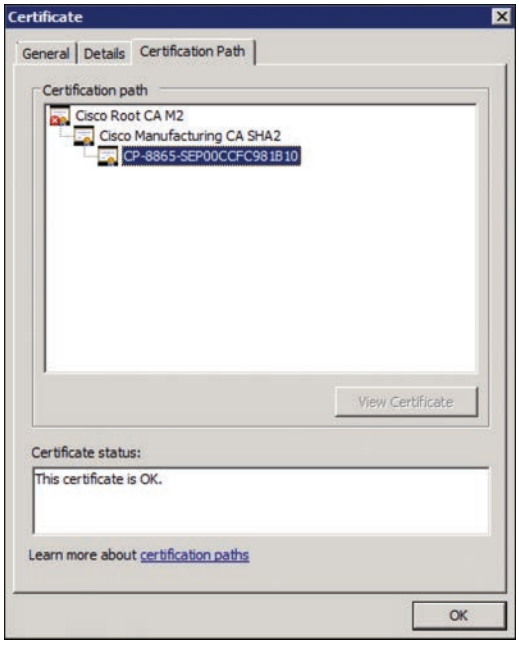

Figure 3-5 *A MIC and Certificates in Its Certificate Trust Chain*

For ISE to authenticate a phone by its MIC, the manufacturing certificates need to be imported into ISE. You can find the MIC and then export it out of Cisco Unified CM by navigating to **Cisco Unified OS Administration > Security > Certificate Management.** The certificate should be exported in a .pem format. When importing into ISE, you should navigate to **Administration > System > Certificates > Trusted Certificates** and then choose **Import**. Figure 3-6 shows an example of ISE displaying the manufacturing certificates that have been imported.

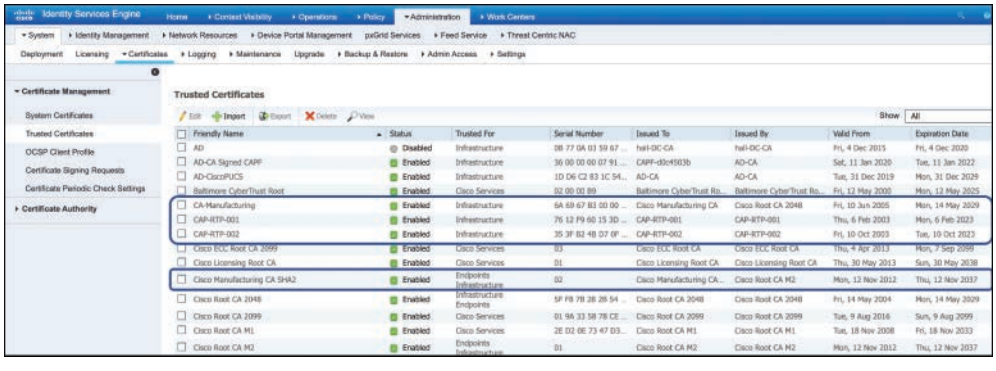

Figure 3-6 *Cisco CA Signed Certificates Inside the Trusted Certificate Store Within ISE*

Now that certificates have been imported into ISE, we can further explain the authentication process. Once ISE receives an authentication request from a client supplicant, it must examine the authentication policy and, ultimately, the sequence of identity stores that can be used in sequential order to authenticate a device. Within ISE, this is known as the identity source sequence. Because IP phones authenticate locally to ISE, a simple identity source sequence can be defined, such as to use only the internal ISE database. After this, you simply need to reference a certificate authentication profile that specifies what attribute to use inside the x.509 certificate to authenticate an IP phone. As shown in Figure 3-7, ISE uses the Subject – Common Name attribute. An example of the identity source sequence is shown in Figure 3-8.

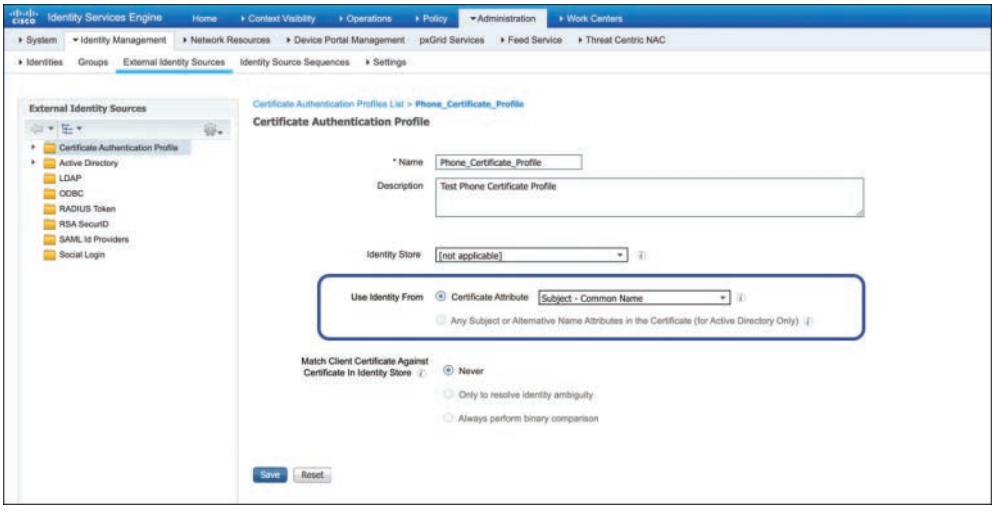

Figure 3-7 *The Certificate Authentication Profile Within ISE Using the Common Name Attribute*

Now that you understand how certificates are used and have a basic understanding of how Cisco ISE uses certificates to authenticate devices, we can discuss the differences in the certificates (MIC versus LSC) and why an organization may choose to use one or the other.

A downfall to using MICs is that it is difficult to prove that the phone belongs to a customer's Unified CM cluster(s) or that it even belongs on the network. This means that an attacker could place a rogue phone with a MIC on the network and potentially register it if auto-registration is enabled on Unified CM. Locally significant certificates (LSCs) provide an additional layer of security and verification that a phone belongs to the network because LSCs are signed by the Unified CM Publisher's Certificate Authority Proxy Function (CAPF) certificate based on RFC 5280, which allows Unified CM to take on the role of a root certificate authority. When CAPF facilitates the signing of LSCs, and an administrator intentionally deploys LSCs to IP phones used by UC administrators, an LSC provides a higher level of security and therefore is preferred (and prioritized) by the IP phone over the MIC.

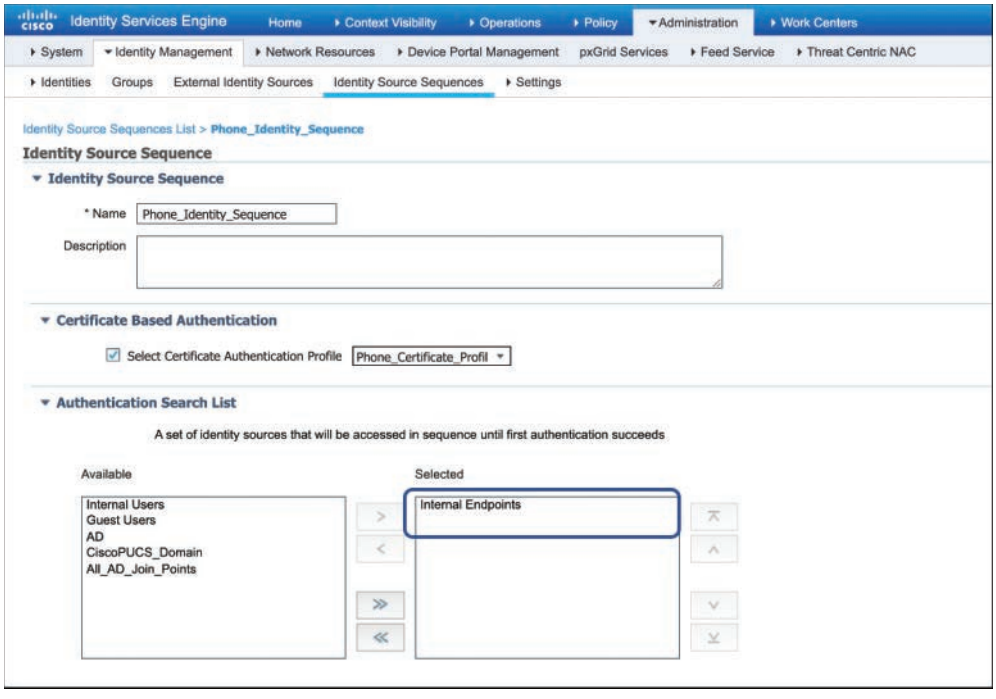

Figure 3-8 *The Identity Source Sequence Within ISE, Which Is Used to Reference the Location (and Ordered List) of Authentication Databases for Endpoints*

When you're deciding which certificate to use for implementing 802.1x security on the network, one approach is to begin by using the MIC because it is the quickest and simplest option. When phones are able to join the network and are able to register to Cisco Unified CM, LSCs can be deployed at any time with minimal changes to the network (e.g., modification of authentication policy). It is a good idea to eventually use LSCs for 802.1x authentication because for many organizations, they are useful for encrypting voice and video traffic. We discuss this topic in more detail in Chapter 7, "Encrypting Media and Signaling."

While 802.1x authentication for Cisco phones has been supported since Unified CM 7.1.2, it is possible that an organization is currently using an IP phone that does not support 802.1x—for example, Cisco IP phones such as 7935, 7936, 7940, and 7960. In some cases, older phone models may have previously supported 802.1x, but with legacy protocols, such EAP-MD5, which have been deprecated. In some cases, the MICs may be expired and therefore no longer valid, so 802.1x authentication with certificates is possible only through use of LSCs. Further, some of the newer TLS 1.2 algorithms used with LSCs may not be supported on legacy phones. Cisco currently recommends checking the release notes for your current version of Unified CM and IP phone firmware to determine support for 802.1x.

Within Cisco's authentication framework, different modes of deployment are available so that organizations can implement a phased approach for strengthening authentication onto the network. Currently, organizations can use three different deployment modes to ensure that PCs and UC endpoints are not prevented from joining the network:

- **Monitor mode:** Provides a nondisruptive environment to monitor the impact that 802.1x can have to the organization without preventing access to the network
- **Low-impact mode:** Uses a pre-authentication ACL (PACL) to allow a subset of traffic prior to authentication, such as DHCP requests
- **Closed mode:** Prevents access to the network prior to authentication/authorization

By using one of these modes, an organization can deploy security in phases. As an example, an organization can deploy 802.1x in monitor mode in conjunction with MAC Authentication Bypass so that it can monitor network authentication failures and adjust policies on an as-needed basis. This way, leadership can evaluate risks while ensuring operations are not impacted by the addition of more stringent security policy being applied to the network infrastructure, which includes Cisco Catalyst switches, wireless LAN controllers, wireless access points, DNA Center, and ISE. For additional detail about configuring the network infrastructure to support 802.1x and MAB, see the relevant security configuration guide for the version of IOS/IOS-XE software that your organization is using. The next section provides additional detail around benefits and use cases for MAB.

MAC Authentication Bypass (MAB) and Network Access Control (NAC)

MAC Authentication Bypass is helpful for scenarios in which you need to authenticate devices that do not have a client supplicant that will support 802.1x authentication. Devices that do not typically support a client supplicant include fax machines, printers, and IoT devices. When MAB is enabled, the Cisco switch uses an endpoint's MAC address as the client identity. For a device to join the network with MAB enabled, MAC addresses of endpoints such as IP phones must be whitelisted in a database that is present in Cisco ISE.

One benefit of Cisco's authentication framework is that it supports flexible authentication methods. As an example, MAB can be enabled as a backup authentication method to 802.1x authentication. An authentication policy that can be created to prioritize 802.1x authentication and to use MAB only as a backup method is shown in Figure 3-9.

When MAB is configured as a backup authentication method, and an administrator designates the voice VLAN as critical, if ISE does not respond to an authentication request, a switch port goes into critical authentication mode. When traffic coming from an endpoint is tagged with the voice VLAN, the endpoint (e.g., IP phone) is put into the voice VLAN that was previously configured on the switch port and allowed onto the network. As previously discussed, the voice VLAN can be learned dynamically through Cisco Discovery Protocol (CDP) or through LLDP. Critical voice VLAN support prevents a scenario in which IP phones become usable because they cannot access the network or the UC infrastructure.

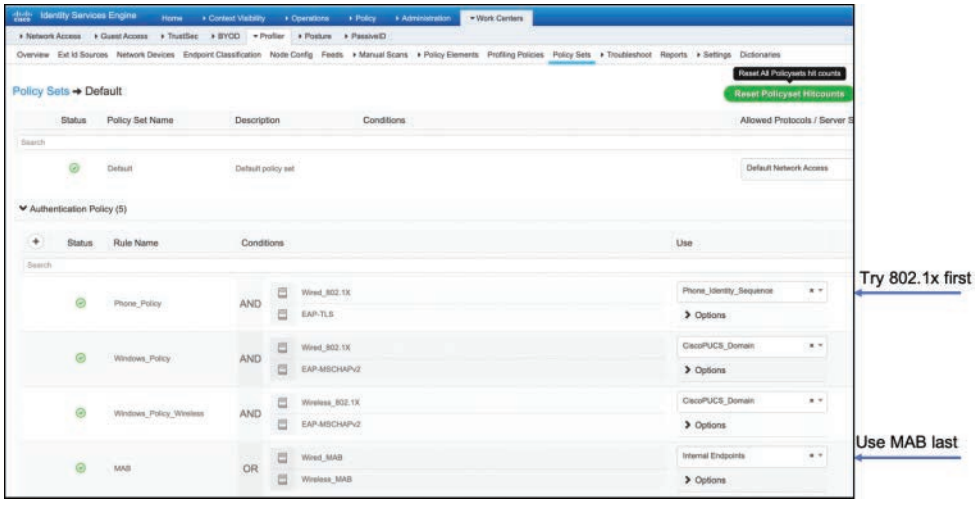

Figure 3-9 *An Authentication Policy Within ISE That Prioritizes 802.1x and Uses MAB as a Failover Mechanism*

It is worth mentioning that MAB is not truly an authentication method. Because MAC addresses can be easily spoofed, MAB is considered more of a backup authentication method for situations when an endpoint is unable to perform 802.1X authentication. In scenarios that 802.1x cannot be deployed, here are some questions that you should ask:

- What are the risks to unauthorized users gaining access to the network infrastructure through a spoofed MAC address?
- What is the likelihood of someone gaining access to the network environment?

As an additional security measure, to minimize MAC spoofing, Cisco ISE can be used to provide network access control (NAC) for the network. This is possible because the Cisco ISE profiler can be used to dynamically detect and classify the types of endpoints that are connected to the network. While still using a device's MAC addresses as the unique identifier, ISE is able to collect various attributes from each endpoint and then use a profiler policy to determine the Total Certainty Factor (TCF) of the credibility of the device. In other words, ISE is able to determine whether a device is really who it says it is. As shown in Figure 3-10, the process is cumulative based on how a device matches the collected attributes to prebuilt or user-defined conditions, which are then correlated with an extensive library of profiles. These profiles include but are not limited to a wide range of device types, such as IP phones, mobile devices, cameras, printers, gaming consoles, and IoT sensors. A TCF that has been assigned to an endpoint, such as a Cisco IP phone, is shown in Figure 3-11.

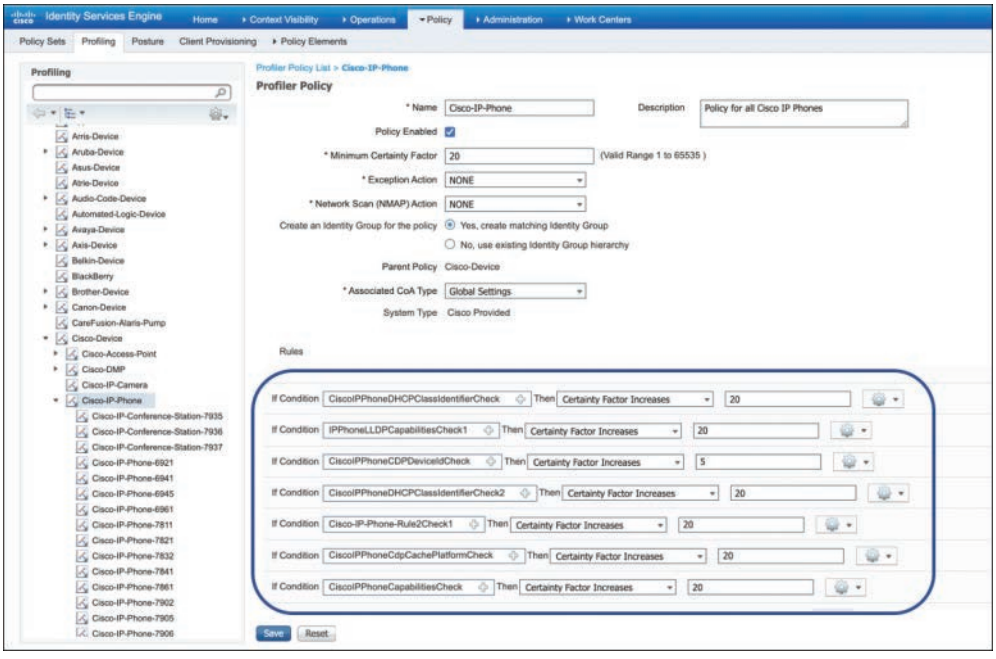

Figure 3-10 *The Way the Total Certainty Factor Is Dynamically Created Within ISE*

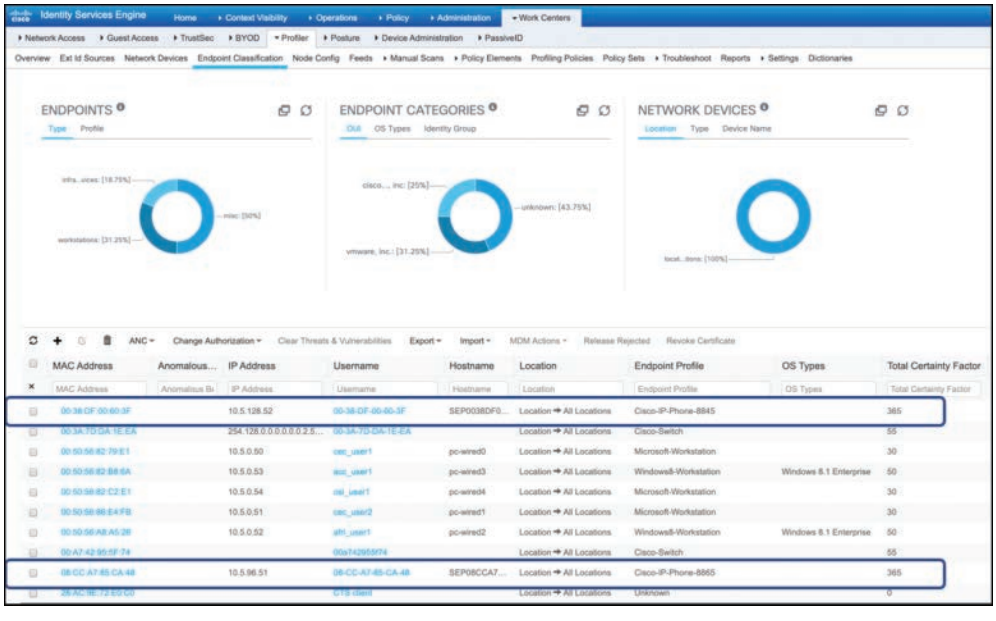

Figure 3-11 *The Total Certainty Factor That Is Assigned by ISE*

Once endpoints are classified and granted access to the network, an authorization profile can be created to specify the type of network access that should be granted to a device based on the profile. The theory behind this approach is that because certain devices are more trusted than others, the level of network privileges should reflect it. An example of the controls that administrators have is that different devices can be put into different VLANs and, if necessary, downloadable ACLs (dACLs) can be assigned to limit access to specific resources. This solution helps prevent or limit the exposure of access to a network if an attacker were to spoof MAC addresses to connect to the network. Practically, the authorization policy may have more trust for UC endpoints that are authenticated via 802.1x with an LSC than devices that use MAC Authentication Bypass as an authentication method. An authorization policy is shown in Figure 3-12.

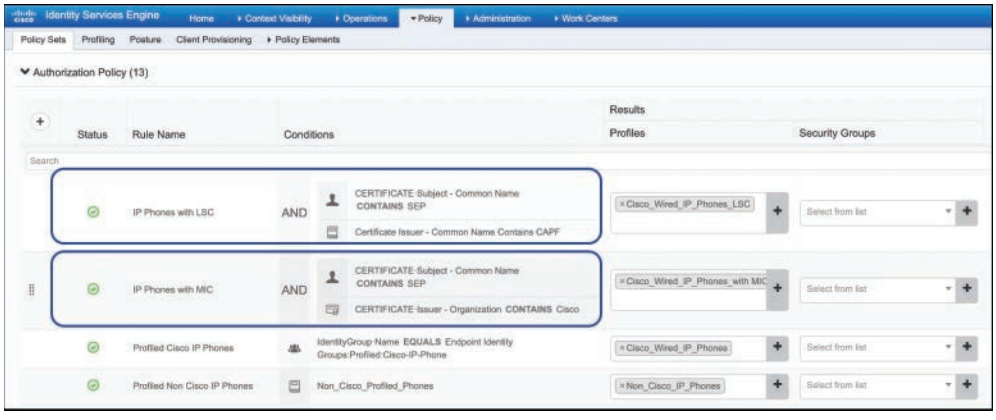

Figure 3-12 *An Authorization Created Within ISE to Apply Different Levels of Trust to Endpoints*

Security Features

A secure UC environment requires the coordinated design of network services such as Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), Trivial File Transfer Protocol (TFTP), Network Time Protocol (NTP), and Domain Name System (DNS). To provide a resilient UC environment, security features should work in unison with these network services.

Figure 3-13 shows which network services are needed to support a UC environment across the network and for which purpose.

Protocol	Purpose
CDP/LLDP	To obtain VLAN/Voice VLAN, negotiate PoE
EAPOL	To authenticate endpoints to the access port
DHCP	To obtain IP address and initial configuration information
ARP	To discover the network's default gateway
TFTP/HTTPS	To obtain device configuration files, firmware, Certificate Trust List, etc.
NTP	Synchronization to the network clock, ensure accurate CDRs
DNS	To resolve hostnames to IP addresses

Figure 3-13 *Protocols and Their Purposes for a UC Environment*

To help stress the importance of leveraging security features in the network, let's discuss the ease of access to information that an attacker can get from the settings button on an IP phone. The network settings page lists many of the network elements and detailed information that is needed for the phone to operate, such as

- IP address of the router (default gateway of IP phone)
- IP address of the DNS server
- IP address of the TFTP server(s) within the Unified CM cluster

By obtaining these pieces of information, an attacker could initiate a network reconnaissance attack, which is the first step in learning more information about a network. The goal of a reconnaissance attack is typically how to gain access to or attack the network or attack the UC infrastructure. Common examples of network reconnaissance attacks include port scanning, ping sweeping, packet sniffing/captures, and more. A network setting screen from an IP phone is shown in Figure 3-14. Unified CM provides the ability to disable access to network settings. To do this, you should navigate to **Unified CM Administration > Device > Phone (Phone Configuration) > Product Specific Configuration Layout > Settings Access** and then choose the disabled parameter.

Figure 3-14 *Information That Can Be Gathered from the Settings Button on an IP Phone*

VLAN Hopping

Before the phone has its IP address, an endpoint discovers which voice VLAN it should be located in by means of the Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP). The auto-assignment of a voice VLAN is useful for providing dynamic segmentation at layer 2 from other types of endpoints on the network. This segmentation typically allows administrators to prevent unwanted traffic across a network with a security control such as an access control list. An example to depict the typical traffic flow is shown in Figure 3-15.

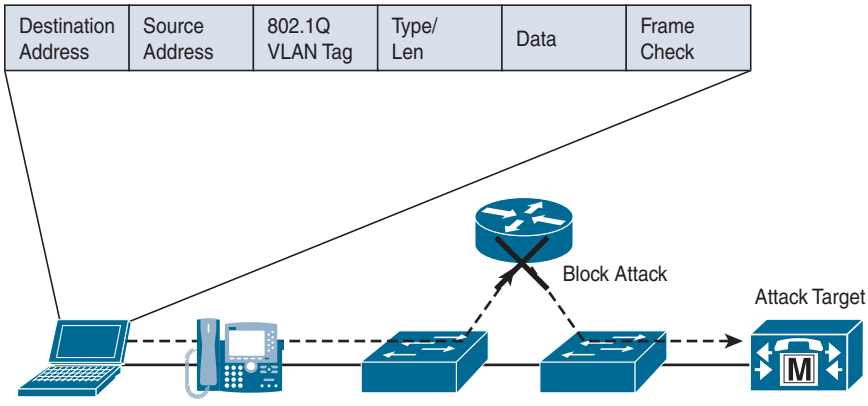

Figure 3-15 *The Way an ACL on the Network Can Be Used to Provide Security*

A threat, known as *VLAN hopping*, is able to bypass security controls in a layer 3 device such as a router or firewall using two different approaches:

- **Double tagging:** When a hacker crafts an IP packet with dual 802.1q tags to send IP traffic to a target device. An inner tag is the VLAN that an attacker wants to reach, and the outer tag is the native VLAN that a device is supposed to be on.
- **Switch spoofing:** When a hacker PC masquerades as a switch and negotiates a trunk connection using Dynamic Trunk Protocol (DTP). If this happens, an attacker can discover information about the native VLAN and possibly elect itself as the root switch for the network. This is possible when a port is configured for "dynamic auto" or "dynamic desirable."

When a VLAN hopping attack is executed properly, an attacker may can launch an attack against infrastructure without alerting security personnel. As shown in Figure 3-16, an attacker can bypass infrastructure that would ordinarily provide packet filtering.

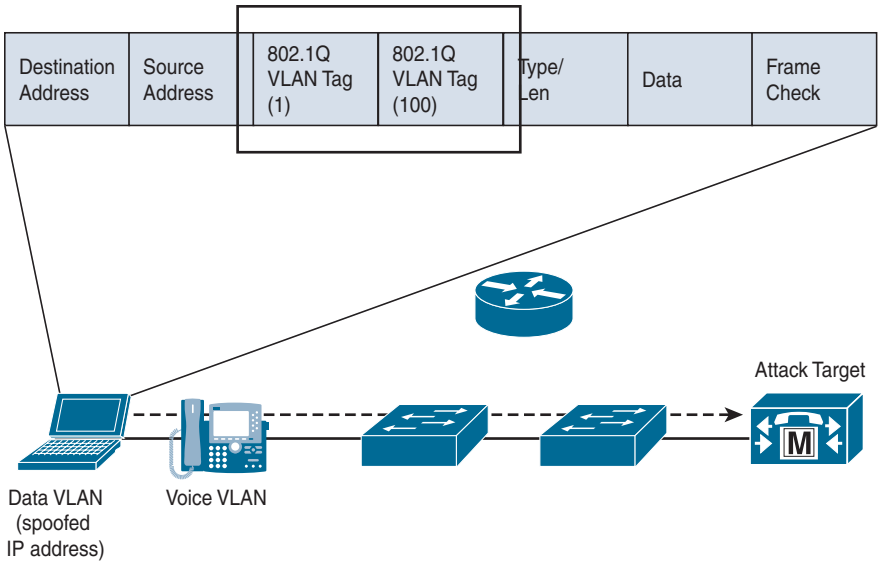

Figure 3-16 *An IP Packet That Has Been Crafted to Bypass Security Controls*

To mitigate a double tagging attack, you can disable PC Voice VLAN Access within Cisco Unified CM. When disabled, this feature does not allow the devices plugged into the PC port on the phone to "jump" VLANs and get onto the voice VLAN by sending 802.1q tagged information destined for the voice VLAN to the PC port on the back of the phone. For most customers, this setting should be disabled. An exception is when a PC is running monitoring and recording applications for training or quality control for someone such as a customer service agent. If this is the case, it may make sense to leave this setting enabled. To disable PC Voice VLAN access, you should navigate to **Unified CM Administration > Device > Phone (Phone Configuration) > Product Specific Configuration Layout > PC Voice VLAN Access** and choose the disabled parameter.

To prevent switch spoofing, dynamic switchport trunking should be disabled on the switch. By default, Cisco switches are enabled to negotiate trunks using the Dynamic Trunking Protocol. Within a switch running 16.9 IOS-XE code, the **switchport nonnegotiate** command can be used to stop a Cisco switch from trying to negotiate a trunk. Network administrators should also consider changing the native VLAN that is used on trunk ports to something different than VLAN 1, which is used by default, and assigning access ports to VLANs that are not be used by other devices. Lastly, administrators should consider mechanisms to prevent a rogue switch from claiming the spanning tree root role. This can be done by configuring **spanning-tree rootguard** and **spanning-tree bpdu guard** on Cisco switches that have been previously designated as the root switch.

DHCP Snooping

In a campus environment, it is common for both PCs and UC endpoints to leverage Dynamic Host Configuration Protocol (DHCP) to minimize the administrative burden

of manually configuring each device with an IP address and other configuration information. By leveraging DHCP, administrators do not have to worry when a user wants to move an endpoint between different locations (and between IP subnets). The configuration information is provided by a DHCP server located in the network, which responds to DHCP requests from DHCP-capable clients.

A well-known attack on the network's DHCP server is called a *DHCP starvation* attack. In practice, a hacker attempting to launch a DHCP starvation attack against an organization leverages tools to create bogus DHCP requests from one or more random source MAC addresses and/or with different DHCP payloads to consume all of the valid IP addresses in the existing DHCP scope(s) of the organization's DHCP server. When the valid DHCP scope becomes exhausted, an attacker can deploy one or more rogue DHCP servers and take control of how devices obtain their network settings, along with other settings that are relevant to UC endpoints, such as TFPT, which is typically included in a DHCP request using Option 150 to obtain configuration information from Cisco Unified CM.

A feature within Cisco IOS/IOS-XE called *DHCP snooping* prevents a nonapproved/rogue DHCP server from handing out IP addresses on a network by blocking all replies to a DHCP request unless that port is allowed to reply. Because most phone deployments use DHCP to provide IP addresses to the phones, you should use the DHCP snooping feature in the switches to secure DHCP messaging. Rogue DHCP servers can attempt to respond to the broadcast messages from a client to give out incorrect IP addresses, or they can attempt to confuse the client that is requesting an address.

When DHCP snooping is enabled, switches across the network provide security by acting like a firewall and filtering out DHCP messages between untrusted hosts and DHCP servers.

To do this, the switch must build and maintain a DHCP snooping binding database. Care should be taken to ensure there is a valid backup of the binding database; otherwise, valid users and endpoints may not have access to DHCP services. The database can be backed up locally on the flash file system or remotely with FTP, TFTP, HTTP, and RCP.

By default, access layer switch ports are considered untrusted for use of DHCP services. Therefore, DHCP snooping is configured only on network ports that connect to a DHCP server.

The following example shows how to enable DHCP snooping:

```
Switch(config)# ip dhcp snooping (enables DHCP snooping)
Switch(config)# ip dhcp snooping database flash:dhcp_snooping_db
(location of DHCP snooping database)
Switch(config)# ip dhcp snooping database write delay 15 (delay before
writing changes to the database)
Switch(config)# ip dhcp snooping vlan 1 100 (VLAN ranges for DHCP
snooping)
Switch(config)# interface gig1/0/20
Switch(config)# ip dhcp snooping trust (interface that DHCP server is
connected to)
Switch(config)# ip dhcp snooping limit rate 1000 (maximum DHCP packets
per second rate)
```

ARP Inspection

The Address Resolution Protocol (ARP) is used to map an IP address to a MAC address. Operationally, if an endpoint tries to communicate with another endpoint, it sends out an ARP request as an IP broadcast message. The endpoint that owns the IP address provides an ARP response (with its IP and MAC address) to the requesting endpoint. The response is stored in its ARP cache for a limited time. For Microsoft Windows, the default lifetime is 2 minutes; for Linux, it is 30 seconds; and for Cisco IP phones, the default lifetime is 40 minutes.

Because ARP allows for gratuitous replies, even if an ARP request was not received, an ARP spoofing attack and/or the poisoning of ARP caches can easily occur. In this type of attack, all traffic from the device under attack can be intercepted by an attacker, as a man-in-the-middle attack, before it is forwarded to a local host, a switch, or an upstream router.

Dynamic ARP Inspection (DAI) is a feature that is configured along with DHCP snooping. Operationally, DAI helps inspect ARP requests and replies whether they are gratuitous or nongratuitous and whether they come from untrusted ports to ensure that the request matches a valid IP-to-MAC address binding in the DHCP snooping database. If DAI is enabled without DHCP snooping, the configuration results in a self-imposed denial of service to any device in that VLAN because none of the devices are to use ARP.

Dynamic ARP inspection is also enabled on a per-VLAN basis by using this global configuration command:

```
Switch(config)# ip arp inspection vlan 1-100 (range of VLANs to inspect)
```

NTP

Network Time Protocol (NTP) allows network devices to synchronize their clocks to a network time server or network-capable clock over UDP port 123. Synchronizing time is critical for troubleshooting network devices or the timestamps that are placed on logs, traces, call detail records (CDRs), and system reports. In fact, many UC applications such as Cisco Unified CM cannot be installed until synchronizing with an NTP server first.

The requirement for NTP also extends to additional servers in the organization, such as a domain controller that contains information about users on the network (such as ACME.com) and ISE servers, which are used for 802.1x authentication. If time is not synchronized on all your devices, certificates cannot be properly validated. In most cases the opposite outcome actually occurs, and certificates are considered untrusted. For this reason, an administrator should make sure that the UC infrastructure, security infrastructure (e.g., ISE), and server infrastructure (e.g., Active Directory) use a common NTP source and are synchronized.

As a point of reference, using Windows Time Services as an NTP source is not recommended or supported for UC infrastructure. The reason is that Windows Time Services often uses Simple Network Time Protocol (SNTP), and Cisco Unified CM cannot

successfully synchronize with SNTP. To avoid potential compatibility, accuracy, and network jitter problems, an NTP server supporting NTPv4 is recommended. An IOS-XE router or Linux server may be utilized to support NTPv4. The Cisco router uses the following version of NTP:

```
cube# show ntp information
Ntp Software Name              :  Cisco-ntpv4
Ntp Software Version           :  Cisco-ntpv4-1.0
Ntp Software Vendor            :  CISCO
Ntp System Type                :  Cisco IOS
cube#
```

It is generally recommended to configure all network infrastructure to connect to NTP time sources that are connected to an accurate and authoritative time source, such as GPS, a radio, or an atomic clock. The internal clock of an IOS/IOS-XE device is not very accurate, so Cisco doesn't recommend its use. A *stratum* is used to describe how many NTP hops away the device is from an authoritative time source. When a network device has access to one or more NTP sources, it uses an algorithm to detect which time source it should synchronize with. In most cases, the algorithm chooses the NTP source with the lowest stratum time, but it is also able to detect when a clock is inaccurate and synchronize with the most accurate time source. Cisco currently recommends having more than one NTP server for high availability/accuracy.

If an organization has an authoritative time source that it would like to use, you can issue the following global configuration commands on an IOS/IOS-XE router:

```
Router(config)# ntp master 2
Router(config)# ntp source [source interface]
```

If an organization doesn't have an authoritative time source to use, network devices can connect to many publicly available NTP sources. An example of a public time source is NIST, which is accessible by directing network infrastructure to *time.nist.gov*, which load-balances NTP requests across its NTP servers. Once a device, such as a router at the edge of a network, is synchronized with a time source such as NIST, it is able to provide NTP to NTP clients across the network. To sync up with one or more authoritative NTP servers, from a network device running IOS/IOS-XE software, you can use the following global configuration commands:

```
Switch(config)# ntp server [ip address of authoritative NTP source]
Switch(config)# ntp source [source interface]
```

Previously, we gave NIST as an example of a public resource for NTP. To ensure authenticity of a public time source, NIST also operates NTP servers that support authentication for registered users. NTP servers that provide authentication sessions are beneficial to an organization because they minimize the risk of the organization encountering an NTP poisoning attack, which happens when a time source is advertised on a public network by an attacker with malicious intent to attack the organization's network

infrastructure. NTP authentication can be configured globally on Cisco IOS/IOS-XE devices. To do this, you can use the following configuration commands.

On an IOS-XE device acting as an NTP server:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 5 md5 [authentication key]
Router(config)# ntp trusted-key 5
Router(config)# ntp server [ip address of authoritative NTP source]key 5
```

On an IOS/IOS-XE acting as an NTP client:

```
Switch(config)# ntp authenticate
Switch(config)# ntp authentication-key 5 md5 [authentication key]
Switch(config)# ntp trusted-key 5
```

As of Cisco Unified CM 11.5(1)SU3, NTP authentication is supported. This feature is based on symmetric key-based authentication with SHA1-based encryption. Unified CM authentication leverages NTP version 4.2.6 and higher. While, in theory, NTP version 4 is backward compatible with version 3, many issues were observed with attempts to use different NTP versions. These issues are documented as of Unified CM version 9.x and later, which specify requirements for NTPv4 servers to be used for NTP. Cisco also currently recommends that UC administrators connect UC applications, such as the Unified CM Publisher, to NTP servers that are not higher than stratum 4 (e.g., stratum-1, stratum-2, or stratum-3). This way, they ensure that the UC cluster time is synchronized with an accurate external time source.

As shown in Figure 3-17, you, as the UC administrator, can check the status of an NTP on a UC cluster by issuing the **utils ntp status** command from the command-line interface. To add one or more NTP servers, you can issue the **utils ntp server add [ntp server]** command.

```
admin:utils ntp status
ntpd (pid 5936) is running...

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.130.2.1      132.163.97.1     2 u  283 1024  377    0.818  -21.140   9.480

synchronised to NTP server (10.130.2.1) at stratum 3
   time correct to within 77 ms
   polling server every 1024 s

Current time in UTC is : Thu Oct 15 21:33:59 UTC 2020
Current time in America/New_York is : Thu Oct 15 17:33:59 EDT 2020
admin:
```

Figure 3-17 *Checking NTP Status Within Cisco Unified CM*

To check the NTP status from a network device running IOS/IOS-XE software, you can issue the **show ntp associations** command.

DNS

The Domain Name System (DNS) enables the mapping of host names and network services to IP addresses within a network or networks. Based on the configuration of a UC environment, use of DNS is not always required to obtain services from UC applications. However, Cisco highly recommends use of DNS to support full UC functionality. As an example, DNS is currently required to support features and use cases such as

- Use of X.509 certificates with fully qualified domain names (FQDN)
- Discovery of UC services for Jabber clients (internal and external)
- Single sign-on for Jabber clients
- Resolution of FQDN for SIP trunk destinations and patterns
- Simplified system management: using host names instead of IP addresses

With X.509 certificates, the use of fully qualified domain names with certificates is mandatory. As you find out in Chapter 7, X.509 certificates are required to support encrypted signaling and media. We also discuss how Jabber clients use DNS SRV records to find UC services in Chapter 11. In short, a secure and highly functional collaboration solution heavily relies on DNS to function correctly for a number of services. For this reason, DNS servers should be deployed in a redundant fashion and be able to resolve host names inside the organization and also external to the organization.

While many organizations leverage DNS internally, many organizations leave it to their service provider to provide external DNS requests. As more organizations leverage and provide Collaboration services at the edge of the network and use Internet connectivity as a transport, the need for visibility of external DNS requests has increased. The reason is that DNS requests precede the IP connection, which enables DNS resolvers to log requested domains regardless of the connection's protocol or port. Monitoring DNS requests, as well as subsequent IP connections, is an easy way to provide better accuracy and detection of compromised systems, improving security visibility and network protection.

When DNS servers are used to resolve host names externally, cloud-based platforms such as OpenDNS (operated by Cisco) and Cisco Umbrella can be used to provide name resolution along with increased visibility of the DNS requests of various users and devices. This increased visibility allows organizations to identify patterns of users and devices, to investigate anomalous activity, and to prevent DNS-based attacks. To obtain information about current threats, Talos (Talos Security Intelligence and Research Group) integrates with the security community and analyzes millions of malware samples per day. Talos directly integrates into DNS platforms such as OpenDNS and Umbrella to dynamically block traffic that is destined to a wide variety of malicious domains, IP addresses, and URLs. Talos is also able to provide security

intelligence feeds into other network infrastructure such as firewalls, IPSs, email security appliances, and web security platforms. To find out more information about why security is needed for external DNS requests, you can visit OpenDNS by navigating to www.opendns.com/ or https://umbrella.cisco.com/. Organizations that do not currently have DNS security in place for external DNS requests should consider a trial version of OpenDNS. Currently, OpenDNS allows customers to register for free DNS accounts. To find out more information about Talos, visit https://talosintelligence.com/.

Firewalls and Access Controls

Traditional data firewalls can be used in conjunction with access control lists to protect Unified Communications infrastructure along with voice gateways from entities that should not be communicating with UC endpoints. In some cases, firewalls may introduce complexities into a design for Unified Communications solutions that include real-time services such as VoIP and video. As an example, if a VoIP call is encrypted, a firewall does not have much ability to inspect the VoIP traffic, and the firewall serves little purpose because it cannot dynamically inspect SIP-TLS traffic. This is why organizations are deploying Session Border Controllers, which act as a VoIP firewall to provide security controls for VoIP and video traffic. We cover Session Border Controllers in further detail in Chapter 11, "Securing the Edge."

Additionally, some limitations need to be considered with security infrastructure, such as IPv6 addressing. As an example, many organizations are starting to leverage IPv6 addressing for their IP phones because they have exhausted their IPv4 addresses. The ASA firewall currently supports IPv6 for collaboration traffic, but not all other Cisco security devices support IPv6. Until all of Cisco's security products support IPv6 for collaboration traffic, Cisco recommends keeping all IPv6 voice traffic contained within an enterprise network or to use a Session Border Controller, such as CUBE.

It is worth mentioning that UC environments have unique data flows that are both client to server and client to client. Using firewalls and/or ACLs to protect real-time traffic flows will likely frustrate firewall administrators based on the additional complexity of managing all of the required ACLs on a firewall to support the various scenarios for UC. As shown in Figure 3-18, a firewall policy that is based on denying all traffic and allowing only what is explicitly permitted by an organization can become quite extensive, even for a small environment, because an administrator would have to account for all of the client-to-client flows. In the following example, to permit a dynamic range of UDP ports, a firewall administrator must open a range of ports from 16384 to 32767 across six different subnets in each direction. It is at this point that the firewall administrator may be concerned about the security risks that are associated with punching so many holes in the firewall for UC traffic to flow correctly. To further compound the challenges with ACLs, several different ACLs would need to be entered to permit ports required for client/server traffic.

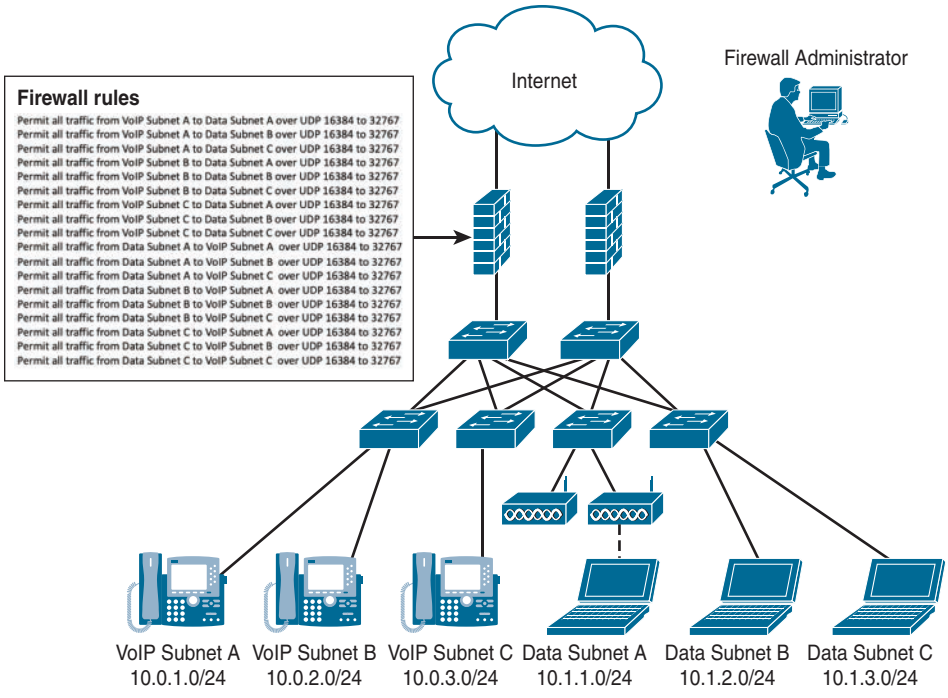

Figure 3-18 *Management Complexity That Is Added on a Firewall for Client-to-Client Traffic*

As when using VRFs, care should be taken when implementing ACLs; otherwise, UC traffic may be less than optimal or lack functionality. For this reason, you must take care in understanding the traffic flows for UC and to position firewalls in a manner so that the quality of the real-time traffic is not impacted by additional latency, delay, or jitter imposed by firewalls. Large amounts of real-time traffic can also cause an undue amount of stress on a firewall. For example, if real-time traffic is encrypted, the firewall cannot perform inspection on the traffic, so the firewall is providing limited functionality.

If organizations are required to place firewalls between UC signaling or real-time traffic for security purposes, the general rule is to monitor the CPU usage of the firewalls and to make sure that it does not exceed more than 60 percent for normal usage. If the CPU consistently runs over 60 percent, it increases the risk of impacting IP phone registration, call setup, and quality of a voice conversation. If firewalls are required to protect VoIP gateways, they can be placed either in front of the gateway or behind the gateway. If you are able to place the firewall in front of the VoIP gateway, the firewall provides filtering of unwanted connections and streams and protects the gateway from denial-of-service attacks. In Chapter 11, we discuss voice-specific firewalls, also known as Session Border Controllers, and the additional protection that they can provide at the edge of the network.

Continuous Monitoring

Continuous monitoring of the network and its security controls for effectiveness is key to the overall health and security of the network. NIST has released publication 800-137 on this topic of continuous monitoring and establishing the practice of monitoring. MITRE provides Common Vulnerabilities and Exposures (CVEs), which are the industry standard for identifying common vulnerability and exposure identifiers. Lastly, there is a Common Vulnerability Scoring System (CVSS) provided by the Forum of Incident Response and Security Teams (FIRST). CVSS is a published standard that is used by organizations worldwide. In principle, the CVSS captures the severity of a vulnerability by associating a numerical score to it.

For new vulnerabilities, the Cisco Product Security Incident Response Team (PSIRT) creates and maintains publications, commonly referred to as PSIRT Advisories, for security-related issues in Cisco products. The method used for communication of less severe issues is the Cisco Security Response.

To get access to Cisco PSIRT information, you have these different options:

- Visit the Cisco PSIRT website.
- Subscribe to RSS feeds.
- Integrate with the Cisco PSIRT's openVuln API, which can be used for programmability and automation of security functionality.

To learn more about accessing and using the openVuln API, visit the Cisco PSIRT page on the Cisco DevNet website: https://developer.cisco.com/site/PSIRT.

Summary

The purpose of the network is to help connect things. These things include IP phones, video teleconferencing devices, laptops, mobile devices, and many other things. A sophisticated attacker understands how an organization's critical services are built (e.g., UC services) and also understands how to leverage weaknesses in the architecture to launch attacks. Therefore, the network can and should be used to secure an organization's UC environment against unexpected attacks and behavior. An approach that organizations can take is based on defense-in-depth principles. Techniques such as segmentation and secure network access (e.g., 802.1x authentication) can reduce the attack surface. Lastly, security features can be enabled to protect against protocol-level attacks.

To gain the most functionality out of the UC environment and implement these various layers of security, an organization needs cross-functional alignment that includes the UC, network, and security teams. When these teams work together for the common good of an organization, this cross-functional alignment positions the organization for the most success.

Last but not least, it is not possible to protect or fix what you cannot detect. This statement has never been truer when considering the use of a network to provide security. When monitoring the network environment and also sharing details about possible issues in the most efficient manner, organizations can stop or minimize the damage of an attack before it can escalate out of control.

Additional Resources

www.cisco.com/go/sda

www.cisco.com/go/ise

www.nist.gov/

http://cve.mitre.org/

www.first.org/cvss/

www.cisco.com/go/psirt

Index

Numbers

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X - Y - Z