IP Telephony – Best Practices Part 1

Hello, and welcome to the "Cisco on Cisco" Seminar on IP Telephony Operations Best Practices. I'm Rich Gore, Manager of the Cisco At Work team which is a part of Cisco IT's Cisco on Cisco initiative. Now the theme of our show today is IP Telephony best practices at Cisco. It's an overview of how Cisco IT manages its global deployment of IP Telephony. And today, it's my pleasure to introduce the star of our show, Kevin O'Healey, who is one of the IT Engineers responsible for IP Telephony operations at Cisco. Now Kevin has been with us for three and a half years and has been part of the IP Telephony operations support team all of that time. Kevin, thanks for coming today. Thank you, Rich. It's a pleasure to be here and to be able to present the best practices IT has learned over the years. So sit back and enjoy as we explore Cisco IT's best practices for IP Telephony.

AGENDA

Today's agenda will include a discussion of IP Telephony best practices as it relates to Cisco CallManager, voice quality, security, monitoring, support, considerations for best practices related to DialPlan, as well as IP Telephony in small offices, home offices and lab environments. And then we'll wrap up with a list of additional considerations, things that you should focus on as part of your deployment of IP Telephony. First on the agenda today is Cisco CallManager best practices.

CISCO CALLMANAGER BEST PRACTICES

One of the key components of Cisco CallManager is the ability to place redundancy into the CallManager cluster and the environment, strategically placed Cisco CallManager servers to maximize redundancy and load balancing within the cluster. CallManager servers should be located in multiple locations to provide spatial redundancy.

AUDIENCE QUESTION: **Q.** So in Cisco IT, how do we do that? We put multiple sets of CallManagers in different locations, for instance, in EMEA?

A. We do. We utilize two different methods. We utilize a combination of clustering over the LAN and clustering over the WAN. So in the states, for instance in San Jose, what we'll do is place our CallManager servers in multiple data centers within the campus. And we'll have primary servers in one location and alternate servers in a secondary location.

AUDIENCE COMMENT: Both on the same campus. Both on the same campus, so clustering within the LAN. In other regions, what we've chosen to do is cluster over the WAN. And this enables us to spread out the geographical reach of a particular CallManager cluster. We're able to provide, based on latency of the circuits, CallManager services to more of our end devices.

AUDIENCE QUESTION: **Q.** And within the United States, do we do any clustering over the WAN? For instance, there's CallManagers in San Jose, CallManagers in RTP on the east coast. If San Jose stopped working, would RTP pick up or what would happen to the other sites that are homed into San Jose?

A. It really depends on the individual cluster in question. So in San Jose, for our primary deployment, what we've done is placed redundancy based on different data centers, as well as placing our gateways throughout the environment. We also utilize centralized call processing for many of our sites, our remote sales offices. In which case, if we were to experience a WAN failure for instance, for those sites, we have survivable remote site telephony or SRST in place. So the phones would register to their local gateway, still be able to receive and place calls to the PSTN.

AUDIENCE COMMENT: Fantastic, okay, thank you very much. You're welcome. Something else to consider is where to place your CallManager servers. Ideally, all of the CallManager servers would be placed in a Class A data center. These are data centers that provide multi-circuit UPS and generated power systems. The benefit is that, if there is an extended power outage affecting the building or the site, there are UPS as well as backup power systems in place to provide a longer running power supply. Physical access security is also a feature or a component of a high availability data center. Only those individuals with a legitimate access to need to gain access to the CallManager servers should gain physical access to the data center. And then lastly, HBAC, fire suppression and diverse circuit entrances are also important considerations really to maintain a high availability environment for the servers.

CISCO CALLMANAGER BEST PRACTICES

The next step is to replicate key services to provide the highest level of resiliency. Key services include TFTP, DNS, DHCP, IP phone services, provided by the individual Web servers and also media resources. CallManager clusters have the ability to have multiple TFTP servers. The TFTP server is responsible for providing configuration loads as well as firmware loads to the IP Telephony endpoints, including phones and gateways. The individual IP Telephony endpoints can learn about the different TFTP servers, either through manual programming or through DHCP option number 150. DNS and DHCP are critical components within most networks and should be duplicated generally on separate servers. And then the Web servers that provide IP phone services should also be duplicated.

AUDIENCE QUESTION: **Q.** So you were talking earlier about having two separate sets of CallManager clusters within the campus or within the WAN?

A. So there's a CallManager in one set, the primary set that is a TFTP server, another that's a DNS and DHCP server. And then in the backup, there's also a dedicated TFTP and DNS and DHCP server? Let me clarify. Within a CallManager cluster, you generally have four different types of servers, either a CallManager Publisher, a TFTP server, primary subscriber and a secondary subscriber. So within a given data center, we will place all of our primary servers. That would be, for instance, the Publisher, primary TFTP and the primary subscribers. And the primary subscribers are where the endpoints register on an ongoing basis. I think the phones and gateways, etcetera. DNS and DHCP are generally going to be separate servers within the environment, in the case of DNS and IP address, DHCP to provide IP addresses.

AUDIENCE COMMENT: Oh, okay, it makes sense, thanks. In the case of TFTP, we do replicate it within our cluster. So we will have a primary TFTP server and a secondary TFTP server. In the event that the primary server is unavailable, there's a network failure or if there were a power failure and that server were offline, then the IP Telephony endpoints would request their configuration files from the alternate TFTP.

AUDIENCE COMMENT: Got you, thanks. A discussion of media resources. Media resources include conference bridges, Music-on-Hold servers, as well as transcoders. These also need to be deployed in a redundant fashion across the environment so that you're users can initiate conference bridges, for instance. In order to set up your redundant media resources, you can utilize the media resource group list and media resource group components within CallManager and build multiple conference bridges, Music-on-Hold servers as well as transcoders and place them into the media resource group list. Next, let's turn our attention to Voice Gateways and some of the best practices. First is to implement diverse routing, including utilize redundant carriers and devices. So ideally, utilizing multiple vendors to provide both local and long distance access for your circuits. The benefit is that, if one vendor has a problem within their network, the alternate vendor is still available to process your calls. Ideally, your circuits would also be duplicated throughout the environment. Not all of the circuits would be placed in one chassis or in one location. Within San Jose, for instance, we spread our gateways across multiple different buildings, between a half dozen and a dozen different buildings, so that in the event we were to experience a power failure to the building, we still have alternate gateways we can utilize. For call routing, utilize your local and long distance trunks interchangeably. To

place a long distance call, first place that call over your long distance trunk. If that trunk is fully consumed or if the circuit is down, then reroute the call through your local trunks and vice versa. Utilize the route pattern, route list and route group components within CallManager to perform the dial plan and digit manipulation necessary to make this work. And then lastly, provide multiple paths out of each cluster. So if you're routing calls from one office to another office, for instance, you will have the option of routing the call on net, on your own corporate network. In the event that there is an out of bandwidth condition, reroute the call out of a long distance circuit. And in the event that circuit is unavailable, you can also reroute the call out of a local circuit.

CISCO CALLMANAGER BEST PRACTICES

When you install CallManager, you should utilize a checklist. And what is included in the checklist will be specific to your individual environment. Within Cisco IT, these are just some of the examples of what we look for when we install the new CallManager cluster or add a server to an existing CallManager cluster. First, as part of the operating system and Cisco CallManager installation, we utilize a global naming standard. The naming standard enables us to look at simply the name of a server and determine what cluster that server is a member of. Also indicates what region that server is located in. Your naming standard may also give additional information, such as, the function of that server within the cluster, whether it is a Publisher, TFTP, primary subscriber or a secondary subscriber. You should also utilize standardized passwords throughout your environment. So within a particular cluster, all of the servers need to utilize the same password. Keep in mind that passwords should only be provided to those individuals directly responsible for the management of that server.

AUDIENCE COMMENT: So that way, if there's an alert, if there's a performance hit on one of the servers or if it's moved from the primary to standby, then the alert, just the naming of the server itself will tell people where it is, what services it's been performing. And of course they'll be able to password into it and fix it. Yes, indeed.

AUDIENCE COMMENT: Okay, makes sense. We've essentially removed the guess work as far as which servers we need to look at if there is an alert or an event. If we see phones unregistered from one server, registered to an alternate server, we know, based on the server name convention, where that server is and what function it provides.

AUDIENCE COMMENT: That's a lot of information, good to know, thanks. Antivirus software should be installed on all of the IP Telephony servers, including the CallManager server. And one important consideration for antivirus software is to make sure that the virus definition files are updated on a regular automatic basis. In this way, the antivirus software is always up to date and where are the most recent strains of viruses.

AUDIENCE QUESTION: **Q.** So Cisco IT has the servers pull the definitions? Or do we push definitions to the servers on a regular basis? **A.** It's going to be pushed to the servers on a regular basis. And another important consideration is, if we have a server that is out of compliance, we receive an automatic notification for that server is out of date. We can go in and manually rectify that situation or also restart the processes to receive that updated virus definition file.

AUDIENCE COMMENT: Good to know, thanks. Network configuration, this is a lesson that we've learned the hard way. Hard set both the speed and the duplex on your CallManager servers and also the switch to which the server uplinks. This is going to remove the possibility of a speed and duplex mismatch which could lead to collisions on the network. Where we've seen this is on upgrades or, for instance, when we're consolidating or collapsing clusters and we need to download a large number of firmware upgrades, for instance, or phone configuration files. Collisions on a network, just as it would with a data server or Web server, for instance, impact the amount of traffic that can be passed over that particular link. So we highly recommend hard set both the speed and the duplex on the CallManager server and the switch to which it uplinks.

AUDIENCE QUESTION: **Q.** So what would happen if, for instance, it wasn't hard set? I'm still a little puzzled. And you mentioned that there was a story behind that, so I'm curious now.

A. We did, there is a story. Several years ago we were doing a consolidation of five clusters to a single CallManager cluster and it was a large number of phones. It was roughly 20,000+ devices.

AUDIENCE COMMENT: That's a lot. So it was a large number. And we had identified how long it should take to download all of the new phone configuration files. And it's based entirely on the TFTP server. The phones that request the file, TFTP server would provide those files. What we're finding is that we expected to migrate the campus in a matter of hours. However after significantly longer than that, we'd only managed to migrate 10 to 20% of the phones. We started to look at the network and what we discovered was a high number of collisions on the server and the uplink port for the TFTP server. We just weren't getting the network throughput required to download all of that information.

AUDIENCE QUESTION: **Q.** And that was because the servers themselves had not had the line speed or the duplex settings hard coded, it had been just left up to the server?

A. Sure, ultimately it was a negotiation between the server and the switch. And in this case, it missed the negotiation and we ended up with a duplex speed mismatch. What we learned from it and took away from it is that now whenever we deploy a new server, hard set both the speed and the duplex.

AUDIENCE COMMENT: That makes sense, thanks. Next is time configuration. Implementing NTP or Windows Time Service on all of your CallManager servers. The reason we highly recommend this, is so that when you are troubleshooting a problem and looking through the CallManager traces, you have a consistent timestamp on all of the traces. This is important when you're looking at traces from two servers within the same cluster. But also it's larger than that when you're looking at traces between servers and multiple clusters. Each of the clusters needs to represent or reference the same master clock. Ideally the IOS routers and Catalyst switches would also reference the same NTP source, consistency across all of the devices.

CISCO CALLMANAGER BEST PRACTICES

Continuing on with the checklist for installing Cisco CallManager. You may wish to modify the default CallManager trace file configuration settings. By default, all of the CallManager servers are going to utilize the same naming convention when they generate CallManager trace files. It can be difficult to correlate or to determine which server generated a specific trace file when you're comparing trace files for multiple CallManager servers. Potentially, for multiple CallManager servers in different clusters. Internally what we found is that there's a benefit to gathering more CallManager traces than less. Based on the call volume of your cluster, you may find that only one or two days worth of CallManager traces can be stored with the default settings. Our goal internally is to store at least five days worth of traces. In this way we don't run into a situation where a user opens a case and a day or two later we go to gather those traces and they're not available because they've been overwritten.

AUDIENCE QUESTION: **Q.** So what level of trace information do we collect internally?

A. There are two different schools of thought in regards to what CallManager traces to gather. One school of thought is to preserve system resources. Use less drive space. Gather fewer CallManager traces. And also, at the same time, reduce the amount of CPU utilization, disk utilization for traces.

AUDIENCE COMMENT: Makes sense. The downside, of course, is that if you have an outage or an event that you need to troubleshoot, you may not have all of the information and the traces. In which case you'll need to increase the trace level, replicate the problem and then

gather those traces.

AUDIENCE COMMENT: And the problem continues as you're doing that, okay. What we have found works best for us internally is to gather traces at the most detailed level, either detailed or arbitrary. So we always have all of the information and can very easily do it through the CallManager traces to identify the relevant information.

AUDIENCE COMMENT: And that's a lot of data collected too. It is a lot of data. And what we've found on our larger clusters in order to have enough drive space for five days is we will install a dedicated drive array specifically for CallManager traces.

AUDIENCE COMMENT: I see, okay. And that's done during the initial installation of operating system and CallManager.

AUDIENCE COMMENT: It makes sense, thanks. Next is configuring performance monitor alerts. Microsoft Windows operating systems come with Microsoft performance monitor. And this includes objects and counters that enable you to monitor and alert on the performance of the system. For example, you can monitor CPU utilization or available drive space. When you install an IP Telephony server from Cisco, such as CallManager, additional objects and counters are added relevant to that service. In the case of CallManager, for instance, you can also monitor registered devices. This includes phones and gateways, conference bridges, transcoders. And you also have the ability to monitor the heartbeat for the CallManager service. Each time the CallManager service is restarted, the heartbeat starts at zero and increments on a regular interval. You can monitor the heartbeat as an indicator of how long the system has been up with the CallManager service running. And also if the CallManager heartbeat returns to zero, you know that either the server has restarted or that the CallManager service has restarted. Also you may wish to set up different monitoring levels for either minor alerts and major alerts. A minor alert is going to be something that is simply a notification for support staff. And generally this is something that would send out an e-mail every 15 minutes, which is beneficial during the day. For instance, if you start to run out of drive space, you can generate a minor alert so support staff can go in and clear out unnecessary information to regain drive space. A major alert is going to be a critical event. For example, the loss of a large number of phone registrations or gateway registrations would trigger a major alert so our support staff can respond immediately. And in these events, we send a page to the support staff every five minutes.

CISCO CALLMANAGER BEST PRACTICES

When installing CallManager, don't install or activate unnecessary services. Not all services are required to be installed and activated on every node within the cluster. The benefit of not installing unnecessary services is that you can preserve system resources and also avoid unnecessary complexity.

AUDIENCE QUESTION: **Q.** Do you have any examples of some services that are unnecessary within a CallManager?

A. For example, the Publisher server does not need the CallManager service, unless it's going to also be providing CallManager functionality or call processing functionality.

AUDIENCE COMMENT: That makes sense. Likewise, the CDR insert service only needs to be installed on the Publisher server. Looking at cisco.com, there are very good reference materials as far as what services should be installed on each of the different CallManager servers.

AUDIENCE COMMENT: Very good, thanks.

CISCO CALLMANAGER BEST PRACTICES

As far as maintaining and administering CallManager, there are a few different things you can do to simplify this task. One of my favorite utilities is the Bulk Administration Tool. I use Bulk Administration Tool, BAT, on a regular basis to import users and devices into an existing CallManager cluster. What we can do is generate a CSV file and import that information directly into the cluster to build out new users in bulk, rather than have to manually build out each user or device individually. BAT can also be used to modify existing phones and lines. For example, if I need to apply a setting to a 1,000 phones, I can go through BAT and make that setting in one change process, rather than have to change each individual line. A recent example would be enabling video on campus within San Jose where we had approximately 20 to 25,000 phones that needed to have video enabled. What we're able to do is generate a file and then import that into BAT and update all of those phones at one time in order to enable video.

AUDIENCE COMMENT: I wondered how that was being done, thank you. Yes, it simplifies the process.

AUDIENCE COMMENT: Quite a bit, yes. One last item is that BAT can be used to migrate data from one cluster to another cluster. So if you're going to be moving users or devices as part of a consolidation, for instance, you can export data from BAT and then re-import that data into the new cluster using BAT as well. A standardized deployment of CallManager makes the administration process easier. Utilizing a consistent naming convention for all of the dial plan components, calling search spaces, partitions, route patterns, etcetera. If everything is configured consistently across all of the clusters, it makes the troubleshooting process that much easier. Ideally, all of the clusters will utilize a common naming convention for all of the dial plan components. It also makes it easier for migrating users from one cluster to another cluster using BAT if all of the partitions and calling search spaces utilize the same naming standard. Something else is utilizing a consistent phone description. This makes it very easy to locate devices with a common function within CallManager. For example, all conference room phones or public area phones should include in the description of that device that it is a conference phone. In this regard, if you need to make a security setting to a public area phone, you can utilize BAT, do a search based on description to identify all of those phones and then make that change. And then as a final point, utilize the Cisco CallManager Solutions Reference Network Design guide; also know as the SRND, which is available on cisco.com as a reference when planning the CallManager deployment. The SRND includes good information about how to plan and deploy CallManager, as well as specific information. For example, in the case of clustering over the WAN where there are specific guidelines for delay and bandwidth, this is included in the SRND. And there is an SRND guide published for each of the major releases of CallManager.

AUDIENCE COMMENT: Well that's a lot of information about CallManager. And now I think we're going to move right on into, what do we do about the underlying LAN and WAN? Yes, indeed.

VOICE QUALITY

The next area of discussion will be voice quality. IP Telephony requires a well designed, highly available network with proper QoS to provide a desired voice quality level. Before deploying IP Telephony on your network, be sure to perform a Voice over IP audit to identify the network readiness for voice. This is something that is available on cisco.com. It is a questionnaire of several questions that discusses what your existing environment looks like. The number of users that will be deployed, as well as what quality of service or QoS configurations are already in place. It will also look at Call Admission Control, WAN capacity and planning. This would be a first step for the deployment of IP Telephony.

AUDIENCE QUESTION: **Q.** So did Cisco IT go through these kinds of steps when we first rolled out IP Telephony within Cisco?

A. We did. In our case what we did is gathered a group of individual users and support staff from different teams to come together and to work through this process asking questions. What is the QoS on the network? What type of trunking will we need for IP Telephony versus our traditional telephony environment? Utilize a codec that meets your voice quality and bandwidth requirements. Every environment is

different. Some companies have a large amount of bandwidth and can utilize a codec, such as G711, which utilizes a higher amount of bandwidth for each call. Whereas other organizations have less bandwidth available in the WAN. The important consideration is to identify codecs within your organization that meet your voice quality needs as well and the bandwidth requirements. Be sure to test the codec in a lab with a pilot group or steering committee. For instance, don't deploy G729 throughout your organization and then determine after the fact that it does not meet the voice quality requirements required by your users. One example could be contact centers. You may wish to always have G711 for your contact centers. Whereas other voice functions might be able to use a lower bandwidth-intensive codec.

AUDIENCE QUESTION: **Q.** So basically, the higher the bandwidth, the higher the voice quality. And the lower the bandwidth, the more cost savings in terms of WAN, but still the lower the voice quality, so it's a tradeoff?

A. Generally speaking, yes. And it's not uncommon to utilize multiple codecs within your environment. The key is to standardize on codecs within certain areas.

AUDIENCE QUESTION: **Q.** Are there areas where we're using 729 to lower bandwidth utilization?

A. Indeed. Generally what you'll find is that in our Cisco offices as well as our campus environments, we utilize G711. But calls placed over the WAN would utilize G729 where it reduces the amount of bandwidth per call.

AUDIENCE QUESTION: **Q.** So our long distance, as in cross continent calls, is using lower bandwidth? **A.** Yes.

AUDIENCE COMMENT: Okay, good to know. Once again, the key is really going to be standardization and only utilizing one codec over a particular WAN link, for instance.

VOICE QUALITY

Voice quality is highly dependent upon the QoS configuration within the network. Within Cisco, we trust traffic as marked by the IP phone, but we rewrite all other traffic to a default classification of TOS-0. When it comes to QoS, the most important consideration is to consistently apply it end-to-end. Every device needs to have QoS in place to ensure that the voice packets receive priority and are not impacted by jitter or variance in delay and latency. Packets should be classified and marked, including voice, signaling and video traffic. Voice needs to take priority, but signaling and video traffic should also be classified and marked and given a certain amount of dedicated bandwidth. Also, don't forget about voice application servers that you may have deployed. These include IVR servers, Cisco Conference Connection, Personal Assistant or PA servers as well. Any voice traffic sourced from these servers will also need to be classified and marked. Priority queuing at the WAN edge for voice and signaling traffic needs to be implemented, ideally utilizing low latency queuing to dedicate a certain minimum amount of bandwidth to voice traffic. And you should develop consistent QoS policies for links of varying bandwidth. For example, all sites that might have between one and four T1s would utilize a specific QoS policy. Sites that utilize five T1s up to a DS3, would utilize a separate QoS policy. The key is to maintain consistency within the environment, so all sites with links of a specific bandwidth, utilize the same QoS policy. As I just mentioned, consistent Call Admission Control also needs to be in place in the environment. Call Admission Control is going to be utilized to restrict the number of calls that can be placed over your IP WAN, for instance. In a centralized call processing environment where you have a Cisco Call Manager cluster in one location and you have multiple remote sites registered to that CallManager, you can utilize the CallManager locations-based Call Admission Control mechanism to restrict the number of calls that can be active on that WAN link at a time or between two sites. Be sure to match the bandwidth for the location's bandwidth in CallManager to the actual bandwidth configured within the IOS routers. Often times what we have seen, when troubleshooting voice quality, is that CallManager might have the location's bandwidth set to unlimited, when there's a real limit on the IOS WAN links as far as how many calls should be permitted. And also, be sure to account for the variations in codec bandwidth. For example, G711 versus G729. Only run a specific codec or one codec across your WAN links. This will make it easier for determining and calculating

the number of calls that you can run across that link. If you mix different codecs with different bandwidth requirements, it becomes very difficult to restrict and identify the true amount of bandwidth required.

VOICE QUALITY

Another factor in maintaining high voice quality, is implementing a core distribution and access switch layer with high availability components. Redundant power supplies plugged into different power circuits. On more than one occasion, I've walked into a wiring closet, seen a switch with multiple power supplies installed, but both power supplies are plugged into the same UPS or plugged into the same power circuit. That doesn't protect the switch in the event that power circuits were to become overloaded and tripped. Each of the power supplies needs to be plugged into a different power circuit or different UPS. Ideally, redundant line cards and redundant Supervisor modules would also be installed. This simplifies the process of recovering the environment in the event that there were line card failures. Redundant core and distribution routers should be implemented throughout the network. And it's important to test and minimize the route convergence. Voice is very sensitive to lost packets, as well as changes in the latency or jitter. So in the event that the routing table does need to re-converge, utilize a high-speed routing table or routing protocol, such as EIGRP or OSPF. And then utilize HSRP to create a primary and secondary default gateway for all of your endpoints, for both data as well as voice components. This is going to be a feature of redundant WAN routing. A UPS system with a two hour runtime should be deployed in all wiring closets. And you should use a UPS audit and create a UPS policy specific to your organization. The key is to maintain uptime in the event of a power outage for all of your endpoints, including your IP phones. Often times I'm asked, why a two hour runtime? Shouldn't that be longer? Or doesn't that seem excessive? What we've found is that in the event of a power outage, if power is not restored within 15 to 30 minutes, most of the users will leave the building. However, support staff will still need access to the network, as well as the phone system in order to troubleshoot that extended outage. It also gives our support staff time to come into the office, after hours for instance, and properly shut down the equipment before the UPSs run out of power. And something important to mention is that overtime networks grow. Be sure that your UPS is keeping up with the added number of devices that are being added to the environment. And then lastly, implement a disaster recovery plan and be sure to document it. Identify what the disaster recovery policy is for IP Telephony. And also, test the disaster recovery policies now and what the procedure is to restore the environment before it's really necessary. A couple of the key questions to ask would be how often do you take backups of the CallManager servers? And also, where are those backup stored? Are they stored on the network? On a tape drive? And what is the process for obtaining access to those backups? In the event that you do need to rebuild a server, do you have all of the software necessary on site to rebuild that server? For instance, the operating system, CallManager application itself and any patches or hot-fixes that need to be applied to restore that server to its previous state.

AUDIENCE COMMENT: So it sound like Cisco's servers are pretty well protected against, in fact, the network itself? Protected against accidental damage. And I think we're going to be moving into, what about malicious damage? Yes, indeed. Security will be one of the next discussion topics.

AUDIENCE COMMENT: Perfect.

SECURITY

As a first line of defense, antivirus software needs to be running on all of the CallManager servers. And as I mentioned previously, the antivirus software needs to be automatically updated on a regular basis with the latest virus definition files. Ideally, also implement an automated reporting infrastructure or if the server has an out of date virus definition file. The support staff is notified, so that they can go and update that dat file. CSA or Cisco Security Agent is an IDS client that can be installed on the Cisco CallManager servers. It's a host-based intrusion protection application that is going to be effective against existing, as well as previously unknown attacks on the system. Worms, for instance. You should also implement tight control on network access from the outside. There are a multitude of different ways in which you can protect your CallManager environment. One of them is going to be utilizing standard access control lists, firewalls,

implementing a DMZ or an IDS. For all of your remote access users and VPN users, be sure to have a strong authentication procedure in place. These are users who are not on your network, physically at your corporate site, but instead, accessing the network remotely. So you need to be sure that you can authenticate and verify who these users are.

AUDIENCE COMMENT: And protect the network from people bringing in viruses or worms from home and launching them across the remote access connection. Absolutely. When users are working from home or remotely, you don't have as much control as you would on the corporate network. So it's important to take that first step, be sure that you authenticate who they are.

AUDIENCE COMMENT: Makes sense. And I think Cisco IT is also implementing NAC on all of our remote access connections, so that users will be required to keep their security status completely current, before they can log onto the network. Exactly, before you're able to gain access, you need to meet certain security requirements. Next is implanting auxiliary VLANs or voice VLANs for your voice traffic. The goal is to separate voice from data. This does have security benefits. For example, if voice and data are separate, a user on the data VLAN cannot simply attach a packet capture utility and capture the packets for voice, possibly to crypt them and play back the audio. Also, you could utilize RFC 1918 address space for your auxiliary VLANs. This is going to enable you to preserve your public address space and assign private address space specifically for voice components. But the key is to keep voice and data separate, separate VLANs. This is also simplifies the process of voice classification and marking for QoS.

SECURITY

Physical security should also be implemented. This includes access to your data centers, as well as all of your wiring closets. Routers and switches, if I have physical access, I can perform a password recovery and gain access to those devices. Be sure to limit who has access to all of your devices and to monitor and log who does gain access. The individual network elements also need to be protected. Be sure to follow sound password and authentication practices. Depending on your environment, this could be resetting passwords every 30, 60 or 90 days, so the passwords are always changing. Be sure to configure any network management functions, such as SNMP. Don't use the default read-only and read-write community string of public. Instead create a separate SNMP community string with a more cryptic value, so that it is more difficult to actually use SNMP to gain access to and potentially manipulate your environment. And then lastly, use login services to track access and configuration changes to your environment. So, for example, changes to your router or switches can be tracked. Implement this policy so that you can identify who made those individual changes. Within CallManager, there have been instances within our environment where we've gone back through the IIS logs to determine which one of our administrators made a specific change. So there are different mechanisms and ways of accessing that information. Design a secure IP network. Place all CallManager servers and IP Telephony servers on a logically separate IP network from your data components. Once again, this is going to be the logical separation of voice traffic from data traffic. And then also implement IP filters, such as access control lists, to limit the specific protocols and ports from the data network that can access your voice network or the CallManager servers. And then lastly, place firewalls in front of all call processing clusters. This is going to be a final line of defense to protect the core of the IP Telephony network.

AUDIENCE COMMENT: And since all of our CallManagers are sitting in data centers, which are relatively well protected with firewalls and other levels of security, that's pretty much a given. Yes, indeed.

AUDIENCE QUESTION: Yes, excellent. **Q.** So we talked about keeping the network from accidental destruction, keeping it from malicious destruction. But how do we know any of this stuff is actually working? I think you're going to be talking about that next.

A. Yes, indeed, it's going to be a combination of monitoring and supporting the environment.

AUDIENCE COMMENT: Perfect.

CISCO SYSTEMS

Well, Kevin, thanks very much. That's about all the time we have for today. So thank you for attending the first half of our Cisco IT AVVID Operations Best Practices VoD. If you click down on the next link that you see below this one, you'll be able to see Part 2, which will include some information on, how Cisco IT monitors and supports the IT telephony operations process. How we do dial plans and how we do IP Telephony in a variety of different types of offices. And we'll also have some questions and answers from other viewers. And we'll get a chance to look at some further resources that might help you in your learning about more things related to IP Telephony. So take a look at the next link that's just below this one and click on that and you'll get started on Part 2. Kevin, thanks very much for coming today. I look forward to Part 2. Thank you very much, Rich.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA C78-337371-00 02/06