CISCO

IP COMMUNICATIONS

VoIP Performance Management and Optimization

A KPI-based approach to managing and optimizing VoIP networks

Adeel Ahmed, CCIE® No. 4574
Habib Madani
Talal Siddiqui, CCIE No. 4280

ciscopress.com

VoIP Performance Management and Optimization

Adeel Ahmed, CCIE No. 4574

Habib Madani

Talal Siddiqui, CCIE No. 4280

Cisco Press

800 East 96th Street
Indianapolis, IN 46240

Network Readiness Assessment

To ensure a consistent level of service, the underlying IP network must

- Have the bandwidth and performance to handle converged services including media and data
- Meet the demand of high-availability voice services by providing resiliency to mitigate the effect of network outages
- Be modular, hierarchical, and consistent to promote consistency and manageability

This predeployment IP network infrastructure assessment should address each of these areas. The infrastructure assessment is accomplished by gathering the needed information from network engineering staff and direct scanning and performance data gathering from the network devices to evaluate the current or planned network implementation, including hardware, software, network design, security baseline, network links, and power/environment.

The following sections examine areas of the infrastructure assessment that must be evaluated.

Network Design

This section discusses the following aspects of the network design that must be evaluated during network readiness assessment for VoIP deployment:

- **Hierarchy and modularity:** Network hierarchy is perhaps the single most important aspect of network design resiliency. A hierarchical network is easier to understand and easier to support because consistent, expected data flows for all applications occur on the network over similar access, distribution, and backbone layers. This significantly reduces the complexity of network management, increases the understanding and supportability of the network, and often results in decreased traffic flow problems and troubleshooting requirements, and improved IP routing convergence times. Network hierarchy also improves the scalability of the network by enabling it to grow without major network changes. Hierarchy also promotes address summarization, which is important in larger IP routing environments.

  Network modularity can be defined as a consistent building block for each hierarchical layer of the network and should include like devices, such as configurations and identical software versions. By using a consistent "model" for each layer of the network, supportability can be improved as it becomes much easier to properly test modules, create troubleshooting procedures, document network components, train support staff, and quickly replace broken components. Each defined hierarchical layer should have a basic solution that is used repeatedly throughout the network. If enhancements or special requirements are added to specific modules, special attention should be paid to testing, documentation, and supportability.
- **IP routing:** IP routing is a design issue for all larger IP network environments. The primary issue is that the routing protocol converges quickly following various failure

scenarios. In addition, the routing scales differently in the particular network environment. The readiness assessment process should include IP routing protocol selection, configuration, IP summarization, and IP routing protocol safeguards to prevent IP overhead and undesirable routing loops. In general, Cisco recommends Open Shortest Path First (OSPF) or Enhanced IGRP (EIGRP) for improved convergence with added variable-length subnet mask (VLSM) support. In environments that anticipate an excess of 100 routes in a routing table on core and distribution layer devices, IP summarization is recommended into the core, generally configured at the distribution layer. For WAN environments, additional summarization might be needed at the edge to reduce overhead on slower WAN links. Routing protocol safeguards are also recommended to reduce overhead and prevent unexpected routing behavior, such as routing across user or server virtual local-area networks (VLAN). In larger WAN environments, it is also recommended that only routes from a particular area be routed into the core and that a particular site should not be a potential reroute point for core or other major traffic.

- **IP addressing:** The IP addressing scheme's evaluation should investigate specifically how the allocation of current IP address space affects the allocation of IP addressing for IP phones and other communications devices. In most cases, an organization does not have available within its current allocation an IP address space within the existing user VLANs or subnets for an IP phone rollout. The following strategies exist for the allocation of space:
    - Increasing subnet size.
    - Providing additional VLANs and subnets for phones using either additional access ports or 802.1Q trunking on user ports.
    - Using secondary interfaces to allocate additional address space where 802.1Q trunking is not supported.
    - Network Address Translation (NAT) should be used with caution. The VoIP network architect should explore the impact on voice signaling protocols when packets from endpoints with translated IP addresses traverse firewalls and proxy servers.
- **Hot Standby Router Protocol (HSRP):** HSRP is a Cisco-specific software feature implementation as described in RFC 2281 that permits redundant IP default gateways on server and client subnets. HSRP can be configured for router prioritization to identify the primary and backup device, preempt the capability to return the gateway to a higher-priority router, and provide "backbone track" support to track the availability of a backbone or WAN interface on the router. On user or server subnets that require default gateway support, HSRP provides increased resiliency by providing a redundant IP default gateway.
- **Quality of service (QoS):** Voice quality on a network is ensured by the use of QoS features. These features must be enabled and available end to end in a network to provide high-quality voice services on the converged network.

  Voice quality is affected by two major factors: lost packets and packets with varying delay (jitter). Packet loss causes voice clipping and skips. The industry-standard codec algorithms used in Cisco digital signal processors (DSP) can correct for up to 30 ms of lost voice. Cisco VoIP technology uses 20-ms samples of voice payload per VoIP packet. Therefore, for the codec correction algorithms to be effective, only a single packet can be lost during any given time. Excessive packet delay can cause either voice quality degradation because of the end-to-end voice latency or packet loss if the delay is variable. If the delay is variable, such as queue delay in bursty data environments, there is a risk of jitter buffer overruns at the receiving end. To provide consistent voice latency and minimal packet loss, QoS is required. The following major rules apply to QoS in LAN and WAN environments:

- Use 802.1Q/p connections for the IP phones and use the auxiliary VLAN for voice.
- Classify voice Real-time Transport Protocol (RTP) streams as “Expedited Forwarding” (EF) or IP precedence 5 (priority options in the frame and the IP header) and place them into a dedicated queue (preferably a priority queue) on all network elements.
- Classify voice control traffic with a Differentiated Services Code Point (DSCP) value of 26 or Assured Forwarding AF31 or IP precedence 3, and place it into a dedicated queue on all network elements to receive priority over bulk data traffic.
- Enable QoS in the campus if LAN buffers are reaching 100 percent utilization.
- Always provision the WAN properly, allowing 25 percent of the bandwidth for overhead, including routing protocols, network management, and Layer 2 link information.
- Use Low Latency Queuing (LLQ) on all WAN interfaces.
- Use Link Fragmentation & Interleaving (LFI) techniques for all link speeds below 768 kbps.

  Service providers (SP) can employ advanced QoS features such as Dynamic QoS (DQoS) or Resource Reservation Protocol (RSVP) to manage the dynamic nature of voice-enabled endpoints.

Network Infrastructure Services

Some of the most common network infrastructure services include Domain Name Services (DNS) for host name resolution, Dynamic Host Configuration Protocol (DHCP) for address assignment, server load balancing, and content caching. For the purpose of network readiness assessment for VoIP, we will be discussing the two most relevant services, DNS and DHCP:

- **DNS:** DNS is a critical network naming service within almost all IP networks. Network clients and servers both request connections to other devices by specifying a name. To resolve the name to an IP address, a request is sent to a configured DNS server, and from this point on, the client can use the returned IP address. DNS servers should be located centrally within core areas of the network with backup servers available. DNS should also be set up as a hierarchy with a master and secondary so that the secondary servers are updated in an appropriate time frame. Devices should also be named, and routers should have DNS entries for all ports to avoid IP address conflicts. Network devices should also be set up with backup DNS servers in case the first chosen server is down. DNS servers should also be considered critical services within the organization, requiring the highest level of security, power backup, and potential redundancy. DNS might not be required in enterprise IP communications environments because IP addresses are configured in Call Manager and IP phones for access but is useful for managing the overall network environment. In SP networks, DNS functionality is a must because it plays a crucial role in provisioning of voice endpoints such as Media Termination Adapter (MTAs). It is also required for establishing voice calls because the voice endpoints rely on DNS to resolve the Call Agent's Fully Qualified Domain Name (FQDN) to an IP address.

- **DHCP:** DHCP is typically used for client IP addressing. This allows mobility and improves IP address manageability. The only downside is that critical IP Allocation State for many nodes is kept within one file or database on the DHCP server. An organization should have adequate support for DHCP services and treat the DHCP data as highly critical data. Generally, DHCP databases should be mirrored or backed up on a continual basis. In addition, an organization should have a plan in case DHCP services fail. This can be mitigated by implementing redundant DHCP servers and distributing the load among different servers, or by configuring backup DHCP servers in case the primary server fails. DHCP server uses "options" to configure the hosts remotely when they are connected to a network. The DHCP options are defined in RFC 2132. These hosts can be VoIP endpoints as well. DHCP servers should also support option 150 for IP phone provisioning. This permits the DHCP server to pass control to the Call Manager to download phone configurations following IP address allocation. In addition, the DHCP server should also support option 43 (vendor-specific information), option 60 (vendor class identifier), option 122 (CableLabs Client Configuration), and so on for provisioning voice endpoints in SP environments.

Network Links

Network links evaluation during network readiness assessment for a VoIP domain should encompass the link redundancy and the installation of the physical media. This section discusses the most essential areas to be included as part of this assessment:

- **WAN link redundancy/diversity:** WAN link redundancy and diversity can be a consideration for distributed IP telephony deployments where WAN links are required for call setup and RTP voice traffic. The organization should determine the backup strategy when the primary WAN link is down. Distributed call processing and gateways or WAN redundancy might accomplish this. WAN redundancy and diversity can include local loop providers and long-distance providers.
- **Copper cabling installation:** Copper installation standards and testing help to ensure that the intra-building copper plant meets expected quality and performance expectations. The installation should follow standards and quality guidelines for signal

attenuation, near-end crosstalk, bend radius, cable routing, distance, termination standards and components, labeling standards, patch cord routing, and building conduit requirements. The current documented standard for Category 5 testing requirements is the TIA/EIA TSB-67 standard. All verification and testing should be done following this guideline, which specifies required values for attenuation and NEXT (near-end crosstalk).

- **Fiber cabling installation:** Intrabuilding, campus-area network (CAN), or metropolitan-area network (MAN) fiber cabling installation standards and testing help to ensure that the interbuilding fiber plant meets expected quality and performance expectations. The installation should follow standards and quality guidelines, which include parameters such as loss per connection (measured in decibel or dB), bend radius, cable routing, termination components or trays, labeling standards, patch cord routing, and organization and building conduit requirements. All fibers should be tested following termination to ensure high quality and minimal signal loss. Campus cabling should generally also offer diversity to prevent disasters caused by cable cuts.

Hardware and Software Considerations

Hardware and software evaluation is also an essential area during the network readiness assessment. This includes evaluating hardware and software resiliency that will be involved in transporting VoIP traffic:

- **Device selection:** Network infrastructure devices identified for an IP telephony infrastructure should have the recommended features for IP telephony and faster network convergence for high availability. IP telephony features include inline power, 802.1Q/p support, hardware priority queuing, and QoS. Availability features includes spanning-tree convergence features such as uplink fast and backbone fast. Devices should also generally have improved backplane capacity, latency, and increased bandwidth. This section also looks at the Mean Time Between Failure (MTBF) of the chosen devices to determine theoretical availability. If the number of total devices is known, Cisco can also provide an expected annual failure rate for the devices.
- **Hardware redundancy:** Redundant modules and chassis are a major contributor to network resiliency and enable normal or frequent maintenance on network equipment without service-affecting outages in addition to minimizing power, hardware, or software failure impact. Redundant chassis can also provide load-sharing capabilities used with routing protocols. The default gateway chassis can be redundant when used with HSRP. Many organizations have redundant backbone chassis and redundant distribution models. Redundant modules include power modules, supervisor modules, and interface modules. Redundant modules ensure that individual module failure does not affect network availability. It is recognized that in many cases, redundant chassis are cost-prohibitive at the access layer because of port density, especially with the introduction of IP telephony. However, the link redundancy between access layer switches and distribution layer devices becomes even more vital considering the lack of hardware redundancy at the access layer.

- **Software resiliency:** The software chosen must support the required features for IP telephony and provide the overall operational reliability. Software reliability is a factor of software configuration and software version control. Software reliability essentially means that there are no bugs with high impact such as crashes, routing errors, call control feature errors, and memory leaks. For the most part, software reliability is the responsibility of software development and testing groups within software vendors such as Cisco. However, the organization deploying VoIP must still validate whether the software is appropriate for its environment by testing or piloting the intended versions and consulting with a professional services organization or a deployment partner assisting it with the VoIP rollout. Where possible, Cisco recommends general deployment versions. The network architect must ensure that these target versions of code have been widely deployed in many customer environments and it is believed that critical and major bugs have been resolved.
- **Software version control:** Software version control is the process of testing, validating, and maintaining authorized software releases within the network. Most organizations require a handful of versions because of different platform and feature requirements. A process should be in place to choose release candidates, review potential impacting bugs, test or pilot-release candidate software, deploy authorized software, and review version accounting information to ensure that software version control is being maintained as expected. The version accounting information will contain information about the software release details, including installation date, testing information, features list, and typically when it will be retired based on the software vendor support calendar for releases. Large organizations without software version control processes can potentially end up with well over 70 software versions within the network, resulting in a higher number of software bugs, unexpected behaviors, and hardware/software incompatibility problems. Organizations requiring high availability should also weigh feature requirements with known software stability in general deployment software. Another issue is software age. Older general deployment software is considered more reliable than recently released newer versions with an untested production history.

Power and Environment

Power requirements and environmental conditions including physical security are very significant for VoIP deployment and must be considered as part of network readiness assessment:

- **Power protection:** Power protection is often a concern in IP telephony environments and might be needed to provide parity to legacy telephone systems. Power protection for IP telephony includes the use of inline power to provide backup power to phones for uninterruptible power supply (UPS)–protected LAN switching gear and power protection of all critical networking components. In addition, key networking equipment should have redundant power supplies with connectivity to separate power distribution units to prevent power loss because of a tripped circuit or Power Distribution Unit (PDU) failure. This can range from a 10-minute UPS to prevent failure because of more common short-term power outages to UPS arrays with backup