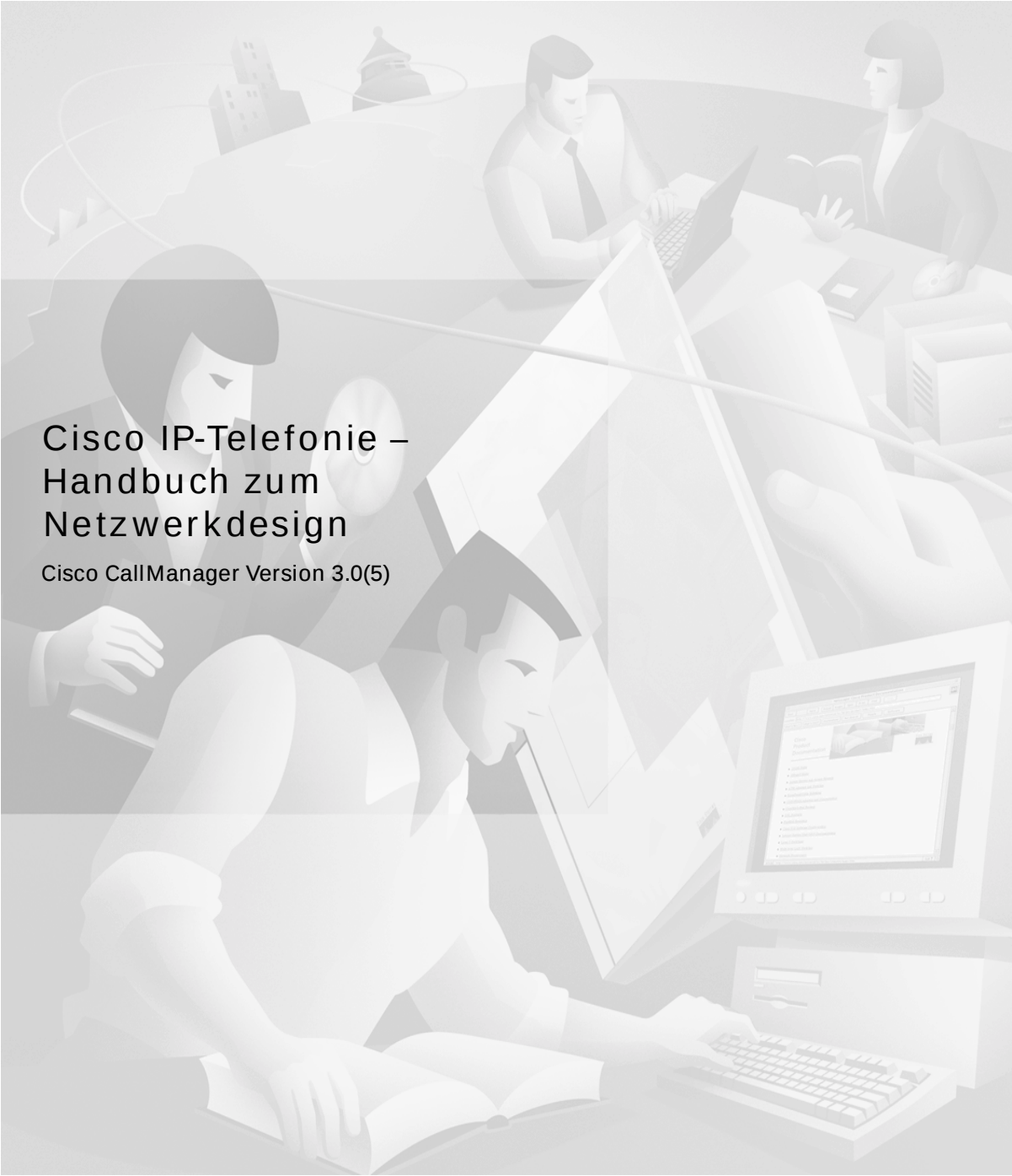




Cisco IP-Telefonie – Handbuch zum Netzwerkdesign

Cisco CallManager Version 3.0(5)



Vorwort ix

Ziel ix

Zielgruppe ix

KAPITEL 1

Einführung 1-1

Allgemeine Designmodelle 1-1

Modell mit einem einzigen Standort 1-3

Mehrere Standorte mit unabhängiger Anrufverarbeitung 1-5

Multisite-IP-WAN mit verteilter Anrufverarbeitung 1-7

Multisite-IP-WAN mit zentraler Anrufverarbeitung 1-9

KAPITEL 2

Informationen zur Campus-Infrastruktur 2-1

Übersicht 2-1

Strategien zum Schutz vor Stromausfall 2-3

Netzwerkinfrastruktur 2-3

Hohe Verfügbarkeit 2-5

Optionen der physikalischen Konnektivität 2-6

Stromversorgung für IP-Telefone 2-7

 Inline-Strom 2-7

 Aufbauen der Stromverbindung für IP-Telefone 2-8

 Weitere Hinweise zum Inline-Strom 2-9

 Strom vom externen Patch Panel 2-10

 Strom aus der Steckdose 2-12

 Zusammenfassung der Empfehlungen 2-12

IP-Adressierung und Management 2-12

 CDP-Verbesserungen 2-13

 VVID-Feld 2-14

 Trigger-Feld 2-14

 Stromanforderungsfeld 2-14

 Zusatz-VLANs und Daten-VLANs 2-14

 Verbindung mit dem Netzwerk 2-15

 Beispieladressierungsplan und Empfehlungen 2-16

Quality of Service	2-17
Klassifizierungsarten für Netzwerkverkehr	2-18
Vertrauensgrenzen	2-18
Klassifizierung des Verkehrs auf Schicht 2	2-19
Klassifizierung des Verkehrs auf Schicht 3	2-22
Klassifizierung auf Schicht 3 für den Cisco Catalyst 6000	2-22
Zusammenfassung der Leistungsmerkmale und Empfehlungen	2-23

KAPITEL 3
Cisco CallManager-Cluster 3-1

Richtlinien für die Verwendung und Skalierbarkeit von Clustern	3-1
Gewichtung der Geräte	3-2
Intracuster-Kommunikation	3-4
Cisco CallManager-Redundanz	3-4
Konfiguration von Redundanzgruppen	3-5
Richtlinien für Campus-Cluster	3-7
Intercluster-Kommunikation	3-9
Cluster-Nutzung im Campus	3-9
Cluster für Multisite-WAN mit verteilter Anrufverarbeitung	3-10
Cluster für Multisite-WAN mit zentraler Anrufverarbeitung	3-12
Transparente Intracuster- und Intercluster-Funktionen	3-15

KAPITEL 4
Gateway-Auswahl 4-1

Unterstützte Protokolle	4-1
IOS H.323-Gateways	4-2
Standort-spezifische Gateway-Anforderungen	4-3

KAPITEL 5
Architektur und Konfiguration von Wählplänen 5-1

Architektur des Cisco CallManager-Wählplans	5-1
Route-Muster	5-4
Route-Liste	5-4
Route-Gruppe	5-5
Geräte	5-5
Ziffernübersetzungstabellen	5-6
On-Net-Route-Muster	5-7
Ausgehende Anrufe über PSTN/ISDN	5-8

Konfigurieren von Gruppen und Anrufeinschränkungen für den Wählplan	5-8
Partitionen	5-9
Anrufauswahlzone	5-9
Die Rolle eines Gatekeepers	5-12

KAPITEL 6

Multisite-WAN mit verteilter Anrufverarbeitung 6-1

Verteiltes Anrufverarbeitungsmodell	6-1
Anrufzugangskontrolle	6-3
Betriebsmodell	6-7
Interaktion zwischen Cisco CallManager und dem Gatekeeper	6-8
Hinweise zur Verwendung eines Gatekeepers	6-11
Hinweise zu Wählplänen	6-11
Auswahl des Gatekeepers und Redundanz	6-13
Bandbreitenauslastung gewählter Nummern	6-13
Hinweise zu Cisco CallManager-Clustern	6-15
Bereitstellung von DSP-Ressourcen für das Transcoding und Conferencing	6-15
Hinweise zu Voice Messaging	6-17

KAPITEL 7

Multisite-WAN mit zentraler Anrufverarbeitung 7-1

Zentrale Anrufverarbeitung	7-1
Anrufgangskontrolle	7-2
Einschränkungen bei der standortbasierten Anrufzugangskontrolle	7-3
Informationen zu Cisco CallManager-Clustern	7-4
DSP-Ressourcenzuweisung für Transcoding und Conferencing	7-5
Informationen zum Voice Messaging	7-7

KAPITEL 8

Quality of Service 8-1

QoS-Standortmodell	8-1
Verkehrsklassifizierung	8-2
Interface-Queueing	8-2
QoS-WAN-Modell	8-3
WAN-Versorgung	8-4
WAN-QoS-Tools	8-4
Setzen von Prioritäten für den Verkehr	8-5
Verbindungseffizienztechniken	8-7

- Verkehrssteuerung 8-8
- Ideale Vorgehensweisen 8-9
- Anrufzugangskontrolle 8-10

KAPITEL 9
Catalyst DSP-Ressourcen 9-1

- Erläuterungen zu Catalyst DSP-Ressourcen 9-1
- Catalyst Conferencing 9-3
 - Details zum Conferencing-Design 9-3
 - Conferencing-Einschränkungen 9-5
- Catalyst MTP-Transcoding 9-5
 - Details zum MTP-Transcoding-Design 9-6
 - IP-to-IP-Packet-Transcoding und -Sprachkomprimierung 9-6
 - Sprachkomprimierung, IP-to-IP-Packet-Transcoding und Conferencing 9-7
 - IP-to-IP-Packet-Transcoding über Intercluster-Trunks 9-8
 - Einschränkungen der MTP-Transcoding 9-10
- Catalyst 4000-Sprachdienste 9-10
- Catalyst 6000-Sprachdienste 9-12

KAPITEL 10
Migration auf ein IP-Telefonie-Netzwerk 10-1

- Netzwerkmodelle 10-1
- PBX- und Voice Messaging-Schnittstellen und -Protokolle 10-2
- Einfache Umstellungssequenz auf ein IP-Netzwerk 10-3
- Referenzmodelle für Umstellungskonfigurationen 10-6
 - Detaillierte Beschreibung von Modell A 10-7
 - Detaillierte Beschreibung von Modell B 10-10
 - Detaillierte Beschreibung von Modell C 10-13
 - Detaillierte Beschreibung von Modell D 10-14

KAPITEL 11
Netzwerkmanagement 11-1

- Remote-Bediensbarkeit für Cisco CallManager 11-1
 - SNMP-Instrumentierung auf dem Cisco CallManager-Server 11-2
- Systemprotokollierungskomponenten 11-3
 - Syslog Collector 11-3
 - Syslog-Verwaltungsschnittstelle 11-4

CiscoWorks2000 Sprachverwaltungsfunktionen	11-6
Campus Manager	11-8
User Tracking	11-9
Verfolgungspfadanalyse	11-10
Resource Manager Essentials	11-12
Inventarkontrolle und Reporting	11-12
Systemprotokollierungsverwaltung	11-13
Syslog Message Filtering	11-14
Warnungen	11-15

ANHANG

Konventionen	1
Zusätzliche Informationen	2
Bezug der Dokumentation	3
World Wide Web	3
Dokumentation auf CD-ROM	3

GLOSSAR

INDEX



Vorwort

In diesem Vorwort werden der Zweck, die Zielgruppe, die Organisation sowie die Konventionen für das Cisco IP-Telefonie – Handbuch zum Netzwerkdesign beschrieben.

Ziel

Dieses Dokument dient als Implementierungshandbuch für Cisco AVVID (Architektur für Sprache, Video und integrierte Daten)-Netzwerke, die auf Cisco CallManager Version 3.0(5) basieren. Da ein großes Interesse der Industrie an IP-Telefonie besteht, suchen Kunden stets mit Nachdruck nach Cisco-Lösungen sowohl für große als auch für kleine Netzwerke. Mit Lösungen, die auf Cisco CallManager Version 3.0(5) basieren, bietet Cisco IP-Telefonie-Systeme in großem Maßstab und mit zahlreichen Funktionen und Anwendungsmöglichkeiten.

Dabei darf jedoch nicht übersehen werden, dass der erfolgreiche Einsatz dieser Systeme innerhalb gewisser Grenzen erfolgen muss. Dieses Dokument dient als Richtlinie für alle Aspekte zum Entwurf von Cisco AVVID-Netzwerken und umfasst Beispiele für funktionierende Konfigurationen. Die vielen neuen Hard- und Software-Funktionen in Cisco CallManager Version 3.0(5) werden detailliert in den unterschiedlichen Lösungs- und Nutzungsmodellen beschrieben. Wichtige Komponenten wie z. B. die Mindestanforderungen für die Cisco IOS Version oder empfohlene Plattformen werden für jedes Modell aufgeführt.

Zielgruppe

Dieses Handbuch richtet sich an Systemingenieure, -berater sowie andere Personen, die für das Entwerfen von Cisco AVVID-Netzwerken, die auf Cisco CallManager Version 3.0(5) basieren, verantwortlich sind.



Vorsicht

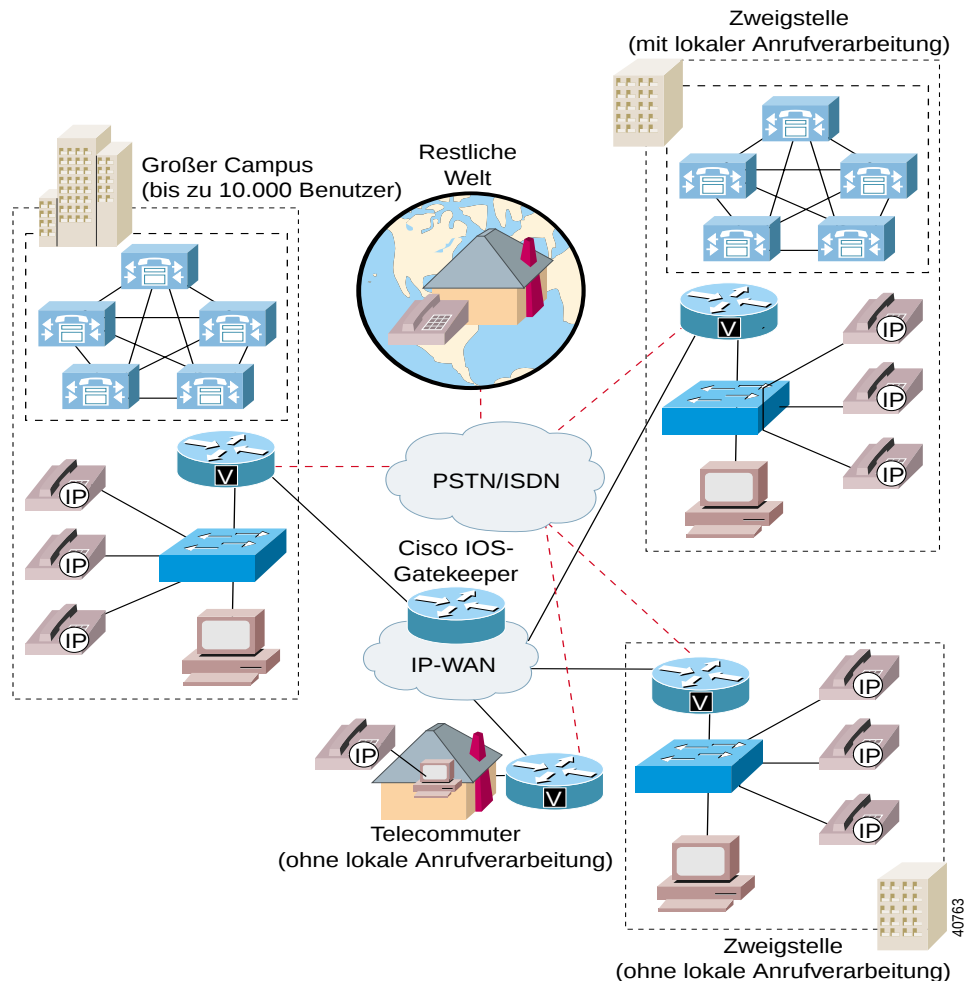
Die Entwurfsrichtlinien in diesem Dokument begründen sich auf dem besten derzeitig verfügbaren Wissen über die Funktionen und den Betrieb der Cisco AVVID-Komponenten. Die Informationen in diesem Dokument können jederzeit ohne vorherige Ankündigung geändert werden.

Einführung

Allgemeine Designmodelle

Abbildung 1-1 erläutert in einem zusammenfassenden Beispiel die Ziele dieses Handbuchs und veranschaulicht die Netzwerkdesignmodelle. In dieser Darstellung werden die Möglichkeiten mit Cisco CallManager Version 3.0(5) dargestellt.

Abbildung 1-1 Allgemeines Modell



Die folgenden Ziele sind allen IP-Telefonie-Netzwerken gemein:

- End-to-End IP-Telefonie
- IP-WAN als primärer Sprachpfad und das öffentliche Fernsprechwahlnetz oder das Integrated Services Digital Network (ISDN) als sekundärer Sprachpfad zwischen den Standorten
- Niedrigere Gesamtbetriebskosten mit größerer Flexibilität
- Neue Anwendungsmöglichkeiten

Für IP-Telefonienetzwerke, die auf Cisco CallManager Version 3.0(5) basieren, gibt es vier allgemeine Designmodelle, die auf die Mehrzahl aller Implementierungen zutreffen:

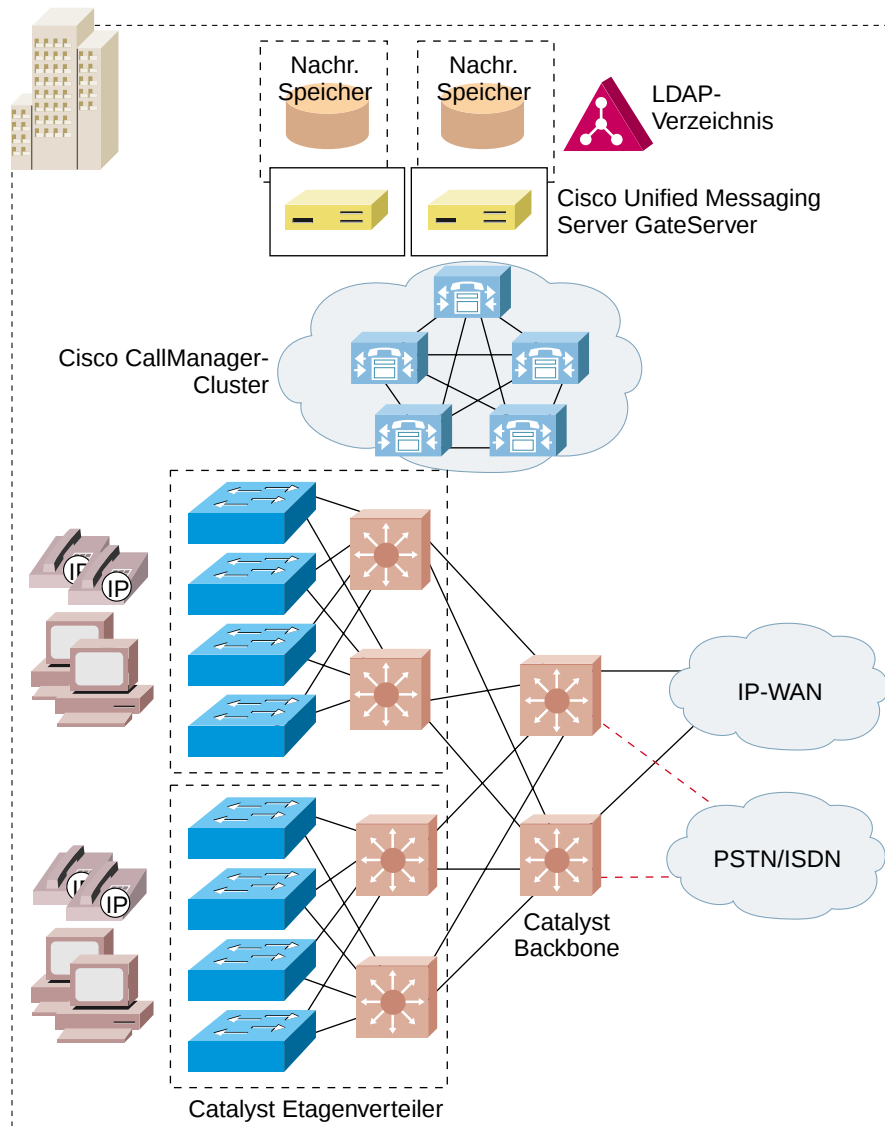
- Modell mit einem einzigen Standort, Seite 1-3
- Mehrere Standorte mit unabhängiger Anrufverarbeitung, Seite 1-5
- Multisite-IP-WAN mit verteilter Anrufverarbeitung, Seite 1-7
- Multisite-IP-WAN mit zentraler Anrufverarbeitung, Seite 1-9

In den folgenden Abschnitten werden die Designziele und Richtlinien für die Implementierung für jedes dieser Modelle zusammengefasst.

Modell mit einem einzigen Standort

In Abbildung 1-2 wird das Modell für ein IP-Telefonienetzwerk an nur einem Standort dargestellt.

Abbildung 1-2 Modell mit Einzelstandort



Das Modell mit einem Einzelstandort verfügt über die folgenden Designcharakteristika:

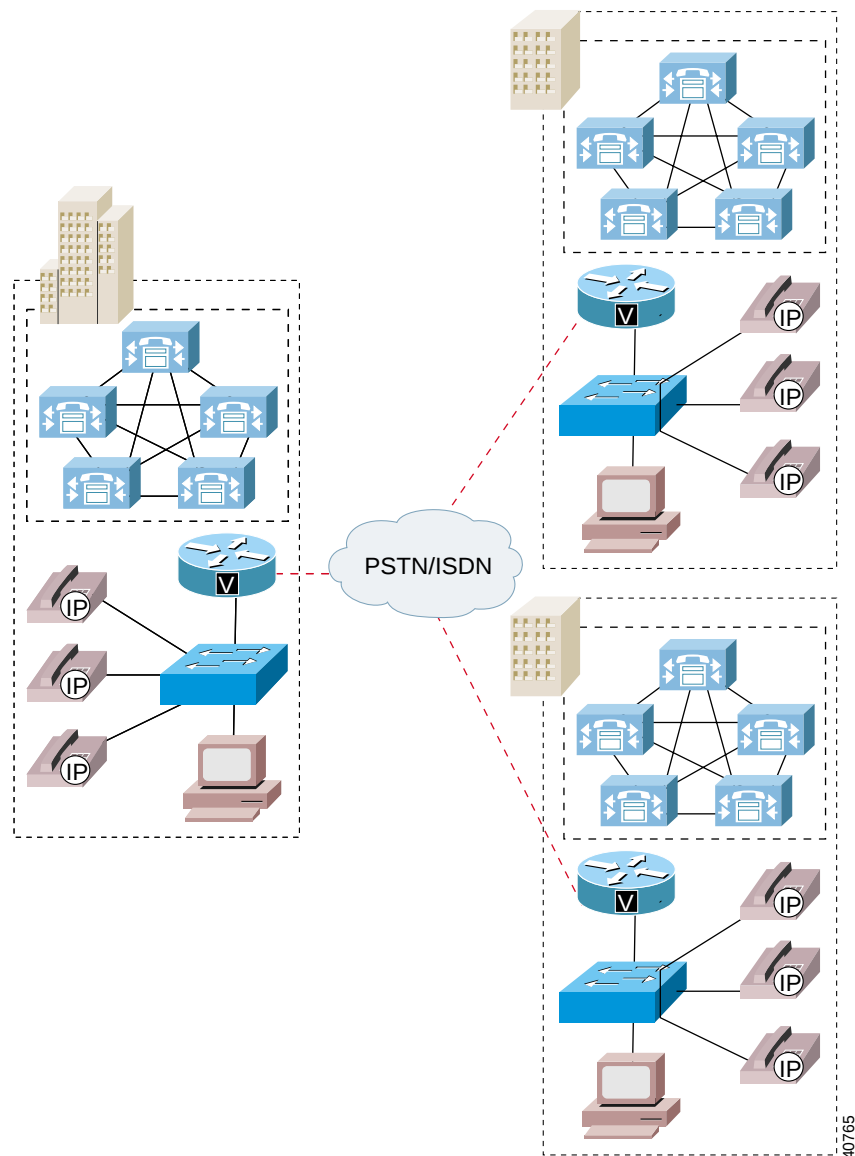
- Ein einzelner Cisco CallManager oder ein einziges Cisco CallManager-Cluster.
- Maximal 10.000 Benutzer pro Cluster.

- Maximal acht Server in einem Cisco CallManager-Cluster (vier Server für die primäre Anrufverarbeitung, zwei für Redundanz, ein Datenbankveröffentlichungs-Server und ein TFTP-Server).
- Maximal 2.500 Benutzer, die jeweils gleichzeitig bei einem Cisco CallManager registriert sein können.
- PSTN/ISDN nur für externe Gespräche.
- Digitale Signalprozessor (DSP)-Ressourcen für Conferencing.
- Voicemail und einheitliche Nachrichtendienstkomponenten.
- G.711-Codec für alle IP-Telefongespräche (80 KBit/s, IP-Bandbreite pro Anruf, nicht komprimiert).
- Verwenden Sie Cisco-LAN-Switches mit mindestens zwei Warteschlangen, um eine zufriedenstellende Sprachqualität zu garantieren. Weitere Einzelheiten hierzu finden Sie unter Kapitel 2, "Informationen zur Campus-Infrastruktur",.

Mehrere Standorte mit unabhängiger Anrufverarbeitung

In Abbildung 1-3 ist das Modell für mehrere isolierte Standorte dargestellt, die nicht durch ein IP-WAN miteinander verbunden sind. In diesem Modell hat jeder Standort seinen eigenen Cisco CallManager oder sein eigenes Cisco CallManager-Cluster zur Abwicklung der Anrufverarbeitung für diesen Standort.

Abbildung 1-3 Mehrere unabhängige Standorte



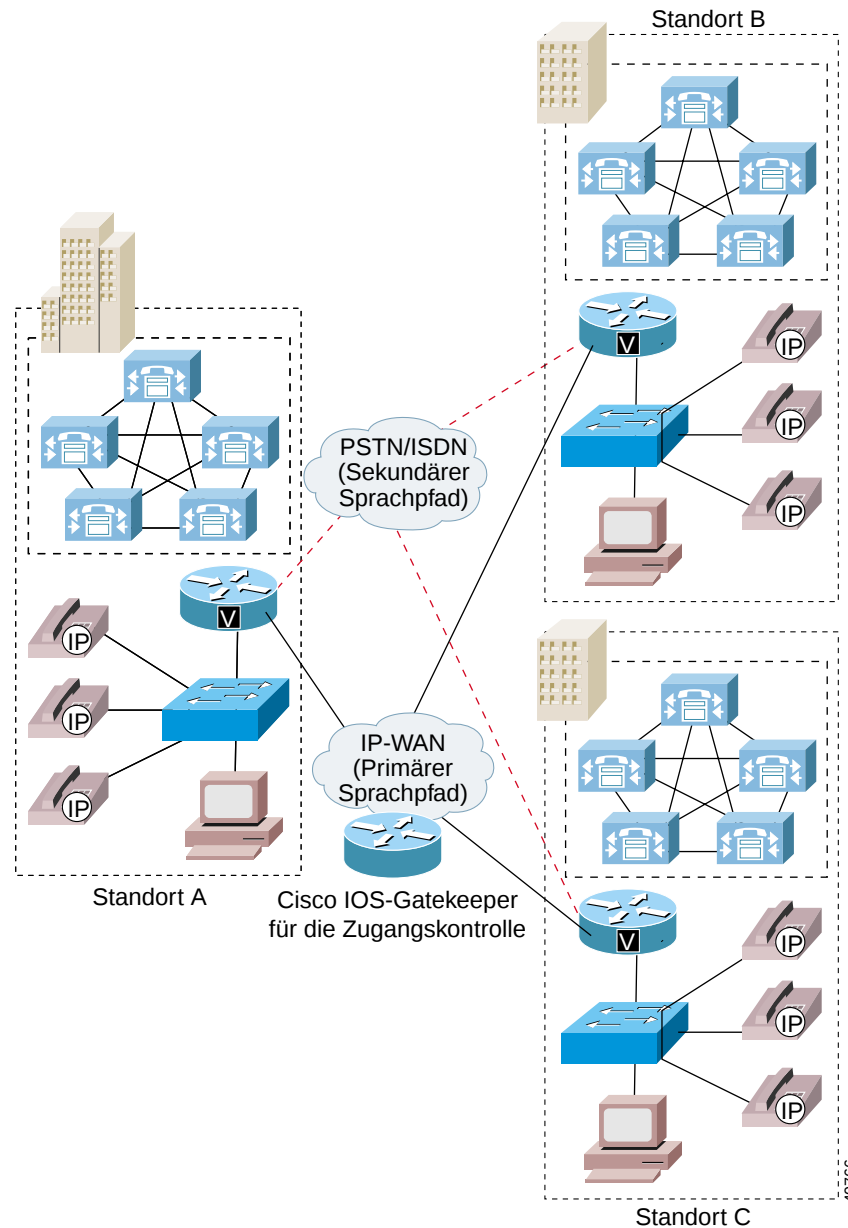
Das Modell für mehrere unabhängige Standorte hat die folgenden Designcharakteristika:

- Cisco CallManager oder Cisco CallManager-Cluster an jedem Standort, um eine skalierbare Anrufkontrolle zu bieten.
- Maximal 10.000 IP-Telefone pro Cluster.
- Unbegrenzte Anzahl von Clustern.
- Verwendung von PSTN/ISDN zur Vernetzung mehrerer Standorte und für alle externen Gespräche.
- DSP-Ressourcen für Konferenzschaltungen an jedem Standort.
- Sprachmitteilungs- oder einheitliche Nachrichtendienstkomponenten an jedem Standort.
- Sprachkomprimierung nicht erforderlich.

Multisite-IP-WAN mit verteilter Anrufverarbeitung

In Abbildung 1-4 ist das Modell für mehrere Standorte mit verteilter Anrufverarbeitung dargestellt.

Abbildung 1-4 Modell mit mehreren Standorten und verteilter Anrufverarbeitung



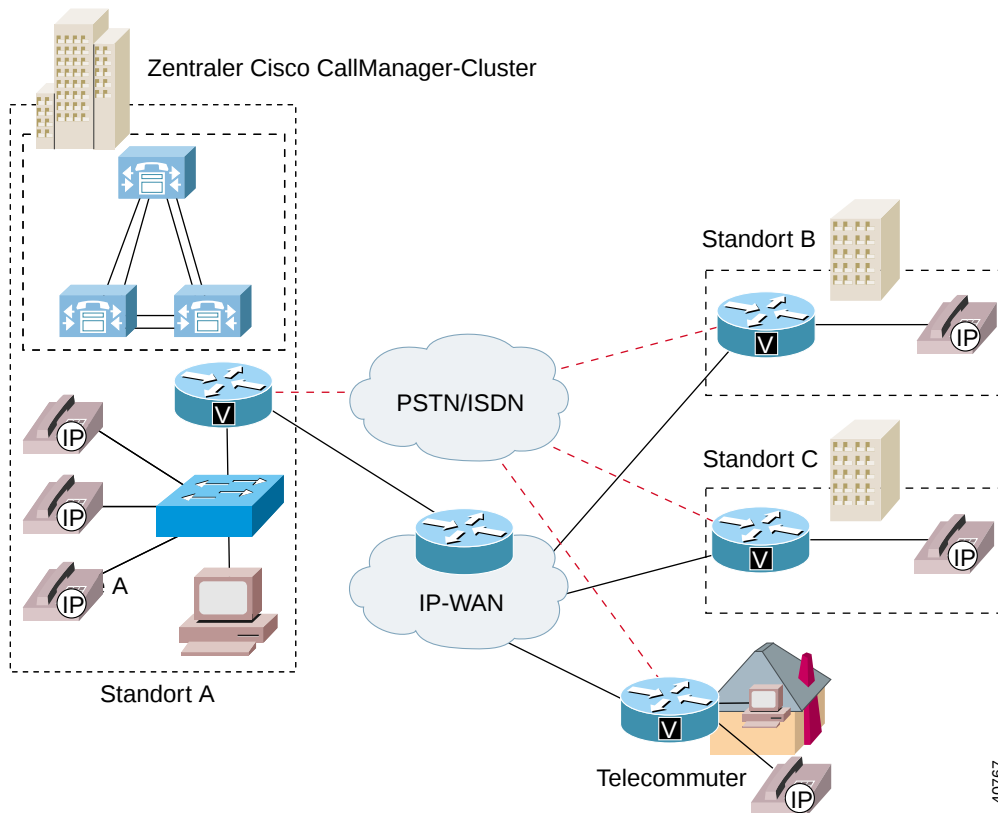
Das Multisite-IP-WAN mit verteilter Anrufverarbeitung verfügt über die folgenden Designcharakteristika:

- Cisco CallManager oder Cisco CallManager-Cluster an jedem Standort (maximal 10.000 Benutzer pro Standort).
- Cisco CallManager-Cluster werden an einem einzigen Standort aufgestellt und decken evtl. nicht das gesamte WAN ab.
- IP-WAN als primärer Sprachpfad zwischen den Standorten, und das öffentliche Fernsprechwahlnetz/ISDN als sekundärer Sprachpfad.
- Transparente Nutzung von PSTN/ISDN, falls das IP-WAN nicht verfügbar ist.
- Cisco IOS-Gatekeeper für Rufnummernadressauflösung.
- Cisco IOS-Gatekeeper als Zugangskontrolle zum IP-WAN.
- Maximal 100 Standorte, die mit Hilfe von Hub-and-Spoke-Topologien über das gesamte IP-WAN miteinander verbunden sind.
- Komprimierte Sprachanrufe werden im gesamten IP-WAN unterstützt.
- Der Einzel-WAN-Codec wird unterstützt.
- DSP-Ressourcen für Konferenzschaltungen und WAN-Transcoding an jedem Standort.
- Voicemail und einheitliche Nachrichtendienstkomponenten an jedem Standort.
- Für Sprach- und Datenverkehr werden mindestens 56 KBit/s benötigt. Für Sprache, interaktive bewegte Bilder und Daten werden mindestens 768 KBit/s benötigt. In jedem Fall sollte die Bandbreite, die Sprache, bewegten Bildern und Daten zugewiesen wird, 75 % der Gesamtkapazität nicht überschreiten.
- Entfernte Standorte können sowohl Cisco IOS basierte als auch Skinny basierte Gateways verwenden.

Multisite-IP-WAN mit zentraler Anrufverarbeitung

In Abbildung 1-5 ist das Modell für mehrere Standorte mit zentraler Anrufverarbeitung dargestellt.

Abbildung 1-5 Modell mit mehreren Standorten und zentraler Anrufverarbeitung



Das Multisite-IP-WAN und zentraler Anrufverarbeitung verfügt über die folgenden Designcharakteristika:

- Der zentrale Standort unterstützt nur einen aktiven Cisco CallManager. Ein Cluster kann einen sekundären und tertiären Cisco CallManager enthalten, solange alle IP-Telefone, die von dem Cluster verwaltet werden, jederzeit bei demselben Cisco CallManager registriert sind. Dies wird als zentraler Anrufverarbeitungs-Cluster bezeichnet.
- Jedes zentrale Anrufverarbeitungs-Cluster unterstützt maximal 2.500 Benutzer (die Anzahl der entfernten Standorte ist nicht begrenzt). Mehrere zentrale Anrufverarbeitungs-Cluster von jeweils 2.500 Benutzern an einem zentralen Standort können über H.323 miteinander verbunden werden.
- IP-Telefone an entfernten Standorten verfügen über keinen lokalen Cisco CallManager.

- Der Anrufzugangskontrollmechanismus basiert auf der Bandbreite pro Standort. Informationen hierzu finden Sie unter "Anrufzugangskontrolle" auf Seite 7-2.
- Komprimierte Sprachanrufe werden im gesamten IP-WAN unterstützt.
- Die manuelle Nutzung von PSTN/ISDN ist verfügbar, wenn das IP-WAN für Sprachverkehr voll ausgelastet ist (der Zugriffscode für PSTN/ISDN muss nach dem Besetztton gewählt werden).
- Eine Wähl-Backup ist für den IP-Telefondienst im gesamten WAN für den Fall eines Ausfalls des IP-WANs erforderlich.
- Voicemail, einheitliche Nachrichtendienste und DSP-Ressourcenkomponenten sind nur am zentralen Standort verfügbar.
- Für Sprach- und Datenverkehr werden mindestens 56 KBit/s benötigt. Für Sprache, interaktive bewegte Bilder und Daten werden mindestens 768 KBit/s benötigt. In jedem Fall sollte die Bandbreite, die Sprache, bewegten Bildern und Daten zugewiesen wird, 75 % der Gesamtkapazität nicht überschreiten.
- Entfernte Standorte können sowohl Cisco IOS basierte als auch Skinny basierte Gateways verwenden.
- Wenn Voicemail verwendet wird, muss jeder Standort über eindeutige Rufnummern verfügen. Interne Rufnummernpläne verschiedener entfernter Standorte dürfen sich nicht überlappen, wenn Voicemail benötigt wird. (Beispielsweise können nicht zwei Standorte zur gleichen Zeit 1XXX haben.)



Informationen zur Campus-Infrastruktur

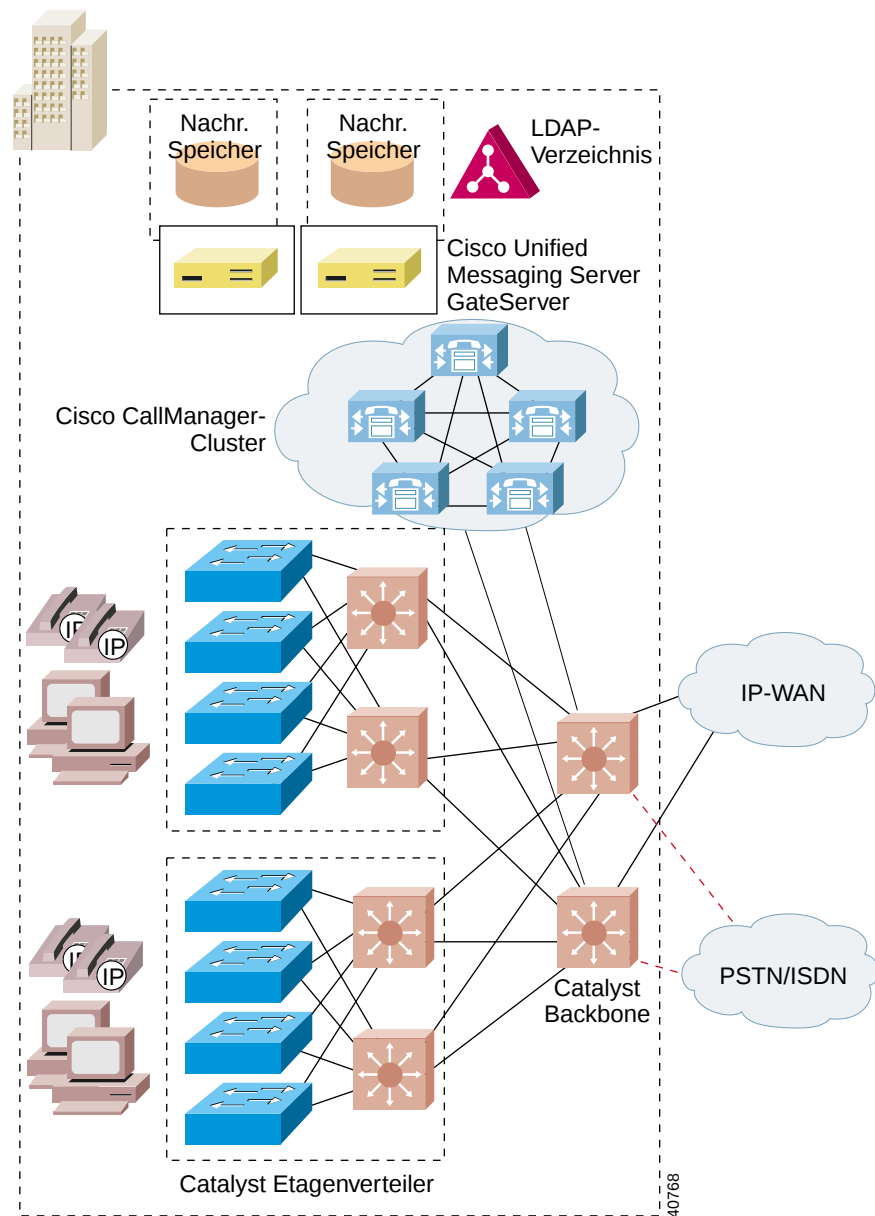
Damit die Cisco IP-Telefonielösungen erfolgreich implementiert werden können, müssen Sie sich zunächst mit der LAN-Infrastruktur befassen. Bevor Sie Sprachdaten über Ihr Netzwerk senden können, muss Ihr Datennetzwerk richtig konfiguriert sein.

Die beschriebenen Konzepte und Implementierungstechniken sind allgemein gültig und können in jedem Unternehmen angewendet werden, ganz gleich, ob es sich um eine Firmenzentrale mit mehreren tausend Benutzern oder eine kleine Zweigstelle mit weniger als hundert Benutzern handelt. Von der Größe des Netzwerks hängt es allerdings ab, welche Komponenten und Plattformen Sie auswählen müssen. Die Details im Hinblick auf Skalierbarkeit, Verfügbarkeit und Funktionalität des Netzwerks richten sich ebenfalls nach der Größe des Netzwerks.

Übersicht

Cisco IP-Telefonielösungen stützen sich auf die stabilen Cisco Multiprotokoll-Router und die Catalyst Multilayer-LAN-Switches, die als Bausteine in Unternehmensnetzwerken eingesetzt werden. Abbildung 2-1 zeigt ein allgemeines Modell eines Cisco IP-Telefonienetzwerks, in dem diese Komponenten integriert sind.

Abbildung 2-1 Allgemeines Übersichtsmodell zur Cisco IP-Telefonie



Strategien zum Schutz vor Stromausfall

Eine zuverlässige Stromversorgung ist für die IP-Telefonie unerlässlich. Eine unterbrechungsfreie Stromversorgung, die so genannte Uninterruptible Power Supply (UPS), wird zum Schutz vor Stromausfällen verwendet und gewährleistet dadurch eine zuverlässige Infrastruktur mit hoher Verfügbarkeit. Jede UPS verfügt über einen Akkuspeicher, der das Gerät über einen bestimmten Zeitraum mit Strom versorgen kann. Die UPS kann je nach gewünschtem Ergebnis mit einem entsprechend großen Akkuspeicher konfiguriert werden.



Vorsicht

Cisco empfiehlt die Bereitstellung einer Backup-Stromversorgung für das IP-Telefonienetzwerk. Die Cisco AVVID-Produkte verfügen im Allgemeinen nicht über eine Backup-Stromversorgung.

Es folgen einige allgemeine Strategien zur Benutzung der UPS:

- Sichern Sie die Switches am Etagenverteiler und die tiefer gelegenen Datenzentren mit der UPS. Diese Strategie stellt zwar sicher, dass die Telefone stets mit Strom versorgt werden, Geräte, die an Wandsteckdosen angeschlossen sind (z. B. PCs), können aber weiterhin von Stromausfällen betroffen sein.
- Sichern Sie das ganze Gebäude mit der UPS. Dadurch werden alle Geräte vor Stromausfall geschützt. Wegen der neuen Hochverfügbarkeits-Datenanwendungen ist es sinnvoll, PCs auf diese Weise zu schützen.
- Besorgen Sie einen separaten Stromgenerator (unabhängig vom Versorgungsunternehmen), und verwenden Sie diesen zur Absicherung der Stromversorgung. In diesem Fall kann die Verwendung der UPS dennoch sinnvoll sein, da der Generator im Normalfall einige Minuten benötigt, bis er anläuft. Der Vorteil bei dieser Lösung ist, dass für jede UPS weniger Akkuzeit benötigt wird.

Darüber hinaus kann die UPS mit Optionen wie der Simple Network Management Protocol (SNMP)-Verwaltung, der Remote-Überwachung, der Alarmbenachrichtigung usw. konfiguriert werden.

Netzwerkinfrastruktur

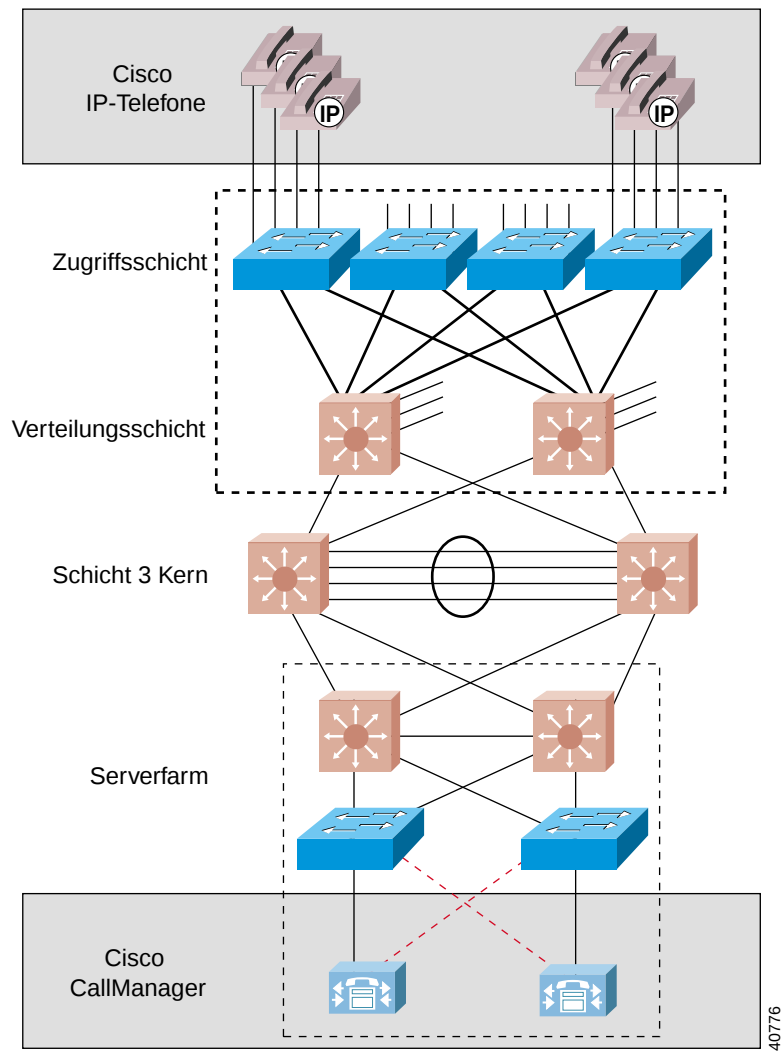
Wenn Sie ein End-to-End-IP-Telefoniesystem aufbauen, benötigen Sie eine IP-Infrastruktur, die auf Switches und Routern der Schichten 2 und 3 basiert. Geswitchte Verbindungen zum Arbeitsplatz müssen vorhanden sein. Netzwerk-Designer müssen sicherstellen, dass die Endpunkte mit geswitchten 10/100-Ethernet-Ports verbunden sind, wie in Abbildung 2-2 dargestellt.



Vorsicht

Cisco unterstützt nicht die Verwendung von Hubs für gemeinsame Konnektivität zu den Switches, da Shared Medium Ansätze den ordnungsgemäßen Betrieb des IP-Telefoniesystems stören können.

Abbildung 2-2 Geschwitchte 10/100-Ethernet-Netzwerkinfrastruktur



Cisco IP-Telefone, die mit dem Switch-Port verbunden sind, liefern auch Konnektivität für einen angeschlossenen Computer. Die Telefonelektronik, die einen Switch mit drei Ports umfasst, ermöglicht das geschaltete Konnektivitätsmodell für den Computer und stellt Quality of Service sowohl für das IP-Telefon als auch für den nachgeschalteten Computer sicher.

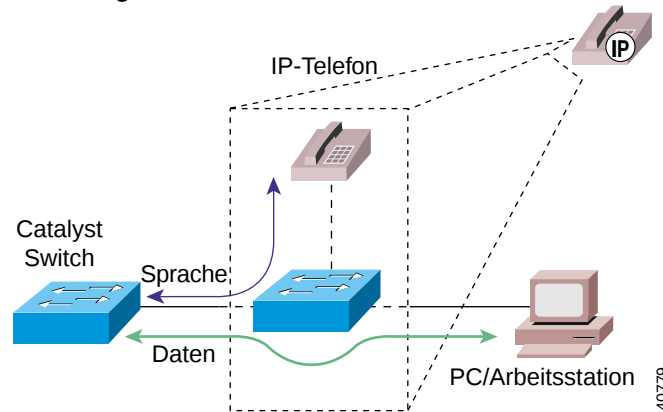


Hinweis Bei den drei Switch-Ports handelt es sich um zwei externe Ports und einen internen Port.

Abbildung 2-3 zeigt die zwei Hauptbestandteile des IP-Telefons – den Telefonschaltkreis und die Switching-Elektronik. Beide befinden sich in demselben Gehäuse. Zwei geschaltete Anschlüsse sind als RJ-45-Buchsen verfügbar: eine geht über ein nicht gekreuztes Kabel zum Switch im Etagenverteiler, über die andere wird ein PC oder eine

Arbeitsstation angeschlossen. Zwei weitere Anschlüsse (kein Ethernet) können zum Anschließen eines Kopfhörers und zur Fehlerbehebung verwendet werden.

Abbildung 2-3 Innenleben des Cisco IP-Telefons



Hohe Verfügbarkeit

Die verteilte Architektur einer Cisco IP-Telefonielösung sorgt für die Verfügbarkeit, die eine wichtige Voraussetzung für das Sprach-Networking ist. Cisco IP-Telefonielösungen sind darüber hinaus standardmäßig skalierbar, d. h. zusätzliche Kapazitäten für Infrastruktur, Dienste und Anwendungen können problemlos bereitgestellt werden.

Anders als bei PBX-Anlagen ist die Verfügbarkeit beim Konvergenz-Networking im verteilten System integriert und befindet sich nicht in einer separaten Box. Redundanz ist in den einzelnen Hardwarekomponenten für bestimmte Dienste verfügbar z. B. in Strom- und Supervisor-Modulen. Die Netzwerkredundanz wird jedoch aus einer Kombination aus Hardware, Software und intelligenten Netzwerkdesignpraktiken erzielt.

Netzwerkredundanz wird auf verschiedenen Schichten erreicht (siehe Abbildung 2-2). Physikalische Verbindungen verlaufen von den Zugangsswitches, an die IP-Telefone und Computer angeschlossen sind, zu zwei voneinander getrennten Geräten. Sollte einmal ein solches Gerät ausfallen oder aus irgendeinem Grund keine Konnektivität mehr bestehen (z. B. durch eine gebrochene Glasfaser oder durch einen Stromausfall), kann der Verkehr auf das andere Gerät umgeleitet werden. Durch die Bereitstellung von Cisco CallManager-Clustern für eine zuverlässige Anrufkontrolle können andere Server die Last aufnehmen, falls ein Gerät im Cluster ausfällt.

Mit erweiterten Protokollen der Schicht 3, wie Hot Standby Router Protocol (HSRP), oder schnell konvergierenden Routing-Protokollen, wie Open Shortest Path First (OSPF) und Enhanced Interior Gateway Routing Protocol (EIGRP), kann eine optimale Netzwerkschichtkonvergenz bei Ausfällen sichergestellt werden.

Erweiterte Tools sind ebenfalls für die MAC-Schicht (Schicht 2) verfügbar. Abstimmbare Spanning-Tree-Parameter und die Möglichkeit, einen Spanning-Tree pro VLAN zur Verfügung zu stellen, ermöglichen eine

schnelle Konvergenz. Zusätzliche Funktionen wie Uplink-Fast und Backbone-Fast ermöglichen eine weitere Verbesserung der Netzwerkkonvergenz bei Netzwerken mit intelligentem Design.

Die hohe Verfügbarkeit des Netzwerks spielt eine wichtige Rolle für die erfolgreiche Nutzung. Die Folge sind Redundanz, Zuverlässigkeit und schnelle Konvergenz.

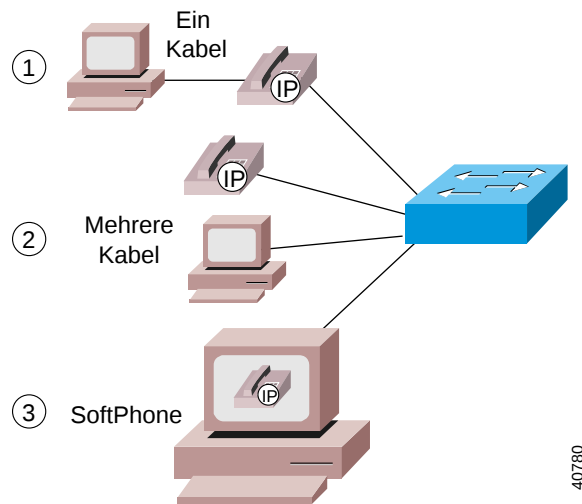
Weitere Informationen

Weitere Informationen zur hohen Verfügbarkeit finden Sie unter "Zusätzliche Informationen" auf Seite 2 im Anhang.

Möglichkeiten physikalischer Anbindung

In diesem Abschnitt werden die verschiedenen Möglichkeiten beschrieben, mit denen IP-Telefone und Computer in das Netzwerk eingebunden werden können (siehe Abbildung 2-4).

Abbildung 2-4 Möglichkeiten physikalischer Anbindung an das Netz



Bei der ersten Option (Abbildung 2-4) wird das IP-Telefon mit dem Switch und das Datengerät (Computer oder Arbeitsstation) mit dem geschalteten Ethernet-Port am IP-Telefon verbunden, wie unter "Netzwerkinfrastruktur" auf Seite 2-3 beschrieben. Dies ist die am häufigsten verwendete Art der Anbindung. Sie erreichen damit eine schnelle Nutzung der IP-Telefonie bei minimalen Modifikationen der vorhandenen Umgebung. Diese Option hat den Vorteil, dass nur ein Port am Switch verwendet wird, damit aber Konnektivität für beide Geräte erreicht wird. Es sind auch keine Veränderungen an der Verkabelung erforderlich, falls das Telefon mit Inline-Strom versorgt wird (siehe "Stromversorgung für IP-Telefone" auf Seite 2-7). Der Nachteil ist, dass beim Ausfall des IP-Telefons der Computer ebenfalls betroffen ist.

Die zweite Option (Abbildung 2-4) besteht darin, das IP-Telefon und den Computer über verschiedene Switch-Ports anzuschließen. Dadurch wird zwar pro Benutzer die doppelte Anzahl an Switch-Ports benötigt, es wird jedoch eine gewisse Redundanz für den Benutzer gewährleistet. Wenn das Telefon ausfällt, ist der PC davon nicht betroffen und umgekehrt. Sie können das Telefon und den PC auch an Ports verschiedener Module anschließen. Auf diese Weise erhalten Sie Redundanz auf einer anderen Ebene, denn eines der Geräte ist in jedem Fall gesichert, falls ein Modul ausfällt.

Die dritte Option (Abbildung 2-4) unterscheidet sich insofern von den anderen Optionen, als das Telefon kein Hardwaregerät ist, sondern eine JTAPI-Anwendung, die auf einem Computer ausgeführt wird. Diese Option, das Cisco IP SoftPhone, eignet sich besonders für Umgebungen, in denen nicht unbedingt ein Handapparat benötigt wird.

Stromversorgung für IP-Telefone

Cisco IP-Telefone unterstützen mehrere verschiedene Stromversorgungsoptionen. In diesem Abschnitt werden die drei verfügbaren Stromversorgungsschemen im Einzelnen beschrieben:

- Inline-Strom, Seite 2-7
- Strom vom externen Patch Panel, Seite 2-10
- Strom aus der Steckdose, Seite 2-12

Inline-Strom

Der Vorteil des Inline-Stroms liegt darin, dass keine lokale Steckdose erforderlich ist. Darüber hinaus besteht die Möglichkeit, die Stromversorgung zentral zu verwalten.

Bei Verwendung von Inline-Strom werden die Paare 2 und 3 (Pins 1, 2, 3 und 6) der vier Paare eines Kabels der Kategorie 5 verwendet, um den Strom (6,3 W) vom Switch zu transportieren. Diese Art der Stromversorgung wird manchmal als Phantomstrom bezeichnet, da die Stromversorgung über dieselben beiden Paare transportiert wird wie die Ethernet-Signale. Die Stromsignale sind für die Ethernet-Signale vollständig transparent und beeinträchtigen sie in keiner Weise.

Um die Inline-Stromversorgung nutzen zu können, benötigen Sie für den Switch ein entsprechendes Power Modul. Diese Module ist derzeit in folgenden Cisco Catalyst Systemen verfügbar:

- Switches der Catalyst 6000-Familie mit Cisco CatOS Version 5.5 oder höher.
- Switches der Catalyst 4000-Familie (Catalyst 4006 mit Power Entry Module und Auxiliary Power Shelf. Es werden mindestens zwei Stromquellen für die 240 Ports benötigt.) Cisco CatOS Version 6.1 oder höher.

- Catalyst 3524-PWR (Standalone-10/100, 24 Ports, 2-GB-Uplinks).
Cisco IOS Version 12.0(5).XU oder höher.

Abbildung 2-5 zeigt die neue Catalyst 6000 Inline Power Modul.

Abbildung 2-5 Catalyst 6000 Inline Power Modul



Bevor der Catalyst Switch Strom bereitstellt, prüft er, ob ein IP-Telefon am Port angeschlossen ist. Der Catalyst Switch prüft zunächst die eindeutigen Eigenschaften des Cisco IP-Telefons und stellt dann für einen kurzen Zeitraum unter Einhaltung eines niedrigen Stromlimits Strom bereit. Dadurch wird verhindert, daß andere Endgeräte mit 10/100 Ethernet NIC Cards beschädigt werden.

Aufbauen der Stromverbindung für IP-Telefone

Um das IP-Telefon mit Strom zu versorgen, muss der für die Stromversorgung zuständige Catalyst Switch folgende Schritte ausführen:

1. Um zu ermitteln, ob es sich bei dem Gerät um ein IP-Telefon handelt, sendet der Switch bestimmte Töne über das Kabel an das IP-Telefon. Wenn das IP-Telefon nicht mit Strom versorgt wird, werden diese Töne zurück an den Switch gesendet.

Wenn der Switch diese Töne empfängt, erkennt er, dass es sich bei dem angeschlossenen Gerät um ein Cisco IP-Telefon handelt und das Gerät problemlos mit Strom versorgt werden kann. Da sich ausschließlich Cisco IP-Telefone so verhalten, kann ausgeschlossen werden, dass andere Geräte, die ebenfalls an den Switch angeschlossen sind, mit Strom versorgt werden. Diese Hardwareprüfung wird in regelmäßigen Abständen vom System für jeden Port durchgeführt, bis ein LINK-Signal registriert wird. Das System kann allerdings auch so konfiguriert sein, dass für den Port kein Inline-Strom bereitgestellt werden soll.

2. Wenn der Switch ein Telefon anhand der Telefonerkennung ermittelt, wird das Gerät mit Strom versorgt. Das Cisco IP-Telefon schaltet sich ein, das Relais wird aktiviert, Loopbacks zwischen Übertragungs- und Empfangspaaren werden entfernt (im Normalfall wird ein geschlossenes Relais geöffnet). Außerdem wird ein LINK-Paket an den Switch gesendet. Ab diesem Punkt funktioniert das IP-Telefon wie ein normales 10/100-Ethernet-Gerät.

Wenn das LINK-Paket innerhalb von fünf Sekunden empfangen wird, folgert der Catalyst Switch, dass es sich bei dem angeschlossenen Gerät um ein Cisco IP-Telefon handelt. Die Stromzufuhr wird fortgesetzt. Andernfalls wird die Stromzufuhr unterbrochen und der Erkennungsprozess wird neu gestartet.

3. Sobald das Cisco IP-Telefon eingeschaltet ist und antwortet, wird der Erkennungsmechanismus in einen statischen Zustand versetzt. Wird das Telefon entfernt oder die Verbindung unterbrochen, startet der Erkennungsmechanismus neu. Der Port wird alle fünf Sekunden auf ein LINK-Paket hin geprüft. Ist kein solches Paket vorhanden, wird der Testton erzeugt.

Dieser Mechanismus bietet den Vorteil, dass der Strom für das Telefon wie in einer traditionellen Telefonieumgebung vom Switch bereitgestellt wird. Bei manchen Installationen sind nur zwei der vier Paare, die für den Datenfluss zwischen dem Etagenverteiler und dem Arbeitsplatz verfügbar sind, terminiert. In diesen Fällen können Kunden mit Inline-Strom die IP-Telefonie mit der vorhandenen Verkabelung ohne weitere Veränderungen nutzen.

Weitere Hinweise zum Inline-Strom

Stromverbrauch

Das Cisco IP-Telefon Modell 7960 verbraucht 6,3 W. Abhängig von der Anzahl der angeschlossenen oder geplanten Telefone, sollte das System eine Stromversorgung mit 1300 W besitzen oder die neue Stromversorgung verwenden, die 2500 W liefert.



Hinweis Die neue Stromversorgung für die Familie der Cisco Catalyst 6000-Switches benötigt 230 V, um 2500 W bereitzustellen. Bei 110 V werden nur 1300 W geliefert. Darüber hinaus benötigt die Stromversorgung 20 A, unabhängig davon, ob der Switch an 110 V oder 230 V angeschlossen ist.

Anschlüsse und Stromversorgung

Tabelle 2-1 zeigt, wieviele IP-Telefone mit der 1050-W-, 1300-W- oder 2500-W-Anschlußmodule für einen Cisco Catalyst 6509 mit Policy Feature Card (PFC) unterstützt werden.

Tabelle 2-1 Anzahl der IP-Telefone, die von den Anschlußmodulen unterstützt werden

Stromversorgung	IP-Telefone, die bei 6,3 W pro Telefon unterstützt werden
1050 W	60 IP-Telefone
1300 W	96 IP-Telefone (2 Module)
2500 W	240 IP-Telefone (5 Module)

Strom vom externen Patch Panel

Falls der Switch keine Stromversorgungs-Anschlußmodule besitzt bzw. für den verwendeten Switch keine Anschlußmodule erhältlich ist, kann ein Cisco Power Patch Panel (Abbildung 2-6) verwendet werden. Das Power Patch Panel kann im Etagenverteiler zwischen dem Ethernet-Switch und dem Cisco IP-Telefon eingefügt werden.

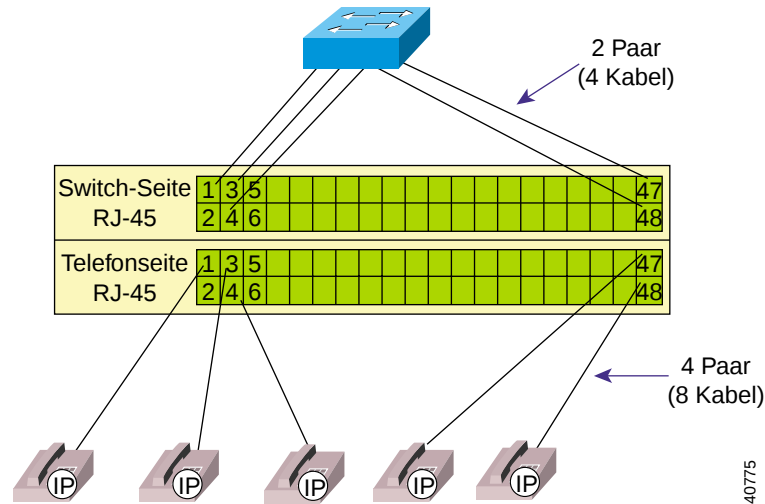
Abbildung 2-6 Cisco Power Patch Panel



Das Patch Panel liefert 250 W und bezieht seinen Strom von einer 230-V-Spannungsquelle. Es ist für maximal 48 Ports ausgerichtet und kann jeden der 48 Ports mit 6,3 W pro Cisco IP-Telefon (Modell 7960) beliefern. Es empfiehlt sich, als Absicherung eine Uninterruptible Power Supply (UPS) zu verwenden, falls einmal ein Stromausfall auftreten sollte.

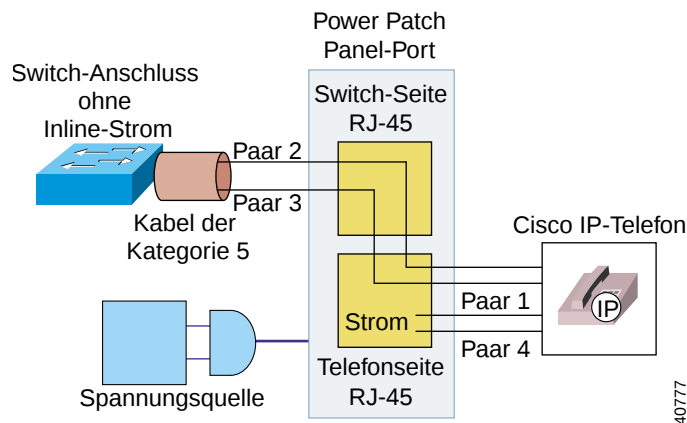
Wie in Abbildung 2-7 gezeigt, besitzt das Patch Panel zwei Anschlüsse pro Verbindung: einen auf der Switch-Seite und einen auf der Telefonseite.

Abbildung 2-7 Konnektivität zwischen dem Power Patch Panel und Cisco IP-Telefon



Wenn die Telefone so angeschlossen sind, werden bei Kategorie 5 Kabeln alle vier Paare verwendet. Anders als bei der Inline-Methode übertragen Ethernet-Paare keine Stromsignale. Stattdessen werden die anderen Paare des Kabels der Kategorie 5 für den Transport des Stroms vom Patch Panel verwendet (siehe Abbildung 2-8).

Abbildung 2-8 Externer Strom vom Power Patch Panel



Wie in Abbildung 2-8 gezeigt, sind die vom Switch kommenden Paare 2 und 3 nicht gekreuzt und direkt mit den Paaren 2 und 3 des Telefons verbunden. Die Paare 1 und 4 am Telefon enden am Patch Panel (bei Ethernet werden die Paare 1 und 4 nicht verwendet). Der Strom für das Telefon wird über diese beiden Paare bereitgestellt. Als eigentliche Leiter für Strom und Erdung werden die Pins 4 und 5 (Paar 1) sowie die Pins 7

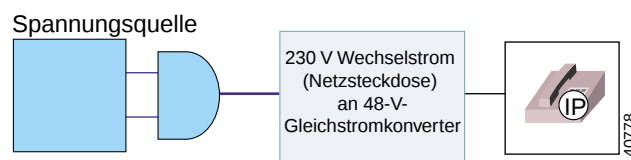
und 8 (Paar 4) verwendet. Das bedeutet, dass alle vier Paare des Kabels der Kategorie 5 am Arbeitsplatz des Benutzers und im Etagenverteiler terminiert werden müssen.

Das Cisco Power Patch Panel arbeitet im Erkennungsmodus. In diesem Modus versucht das Patch Panel festzustellen, ob das angeschlossene Gerät ein Cisco IP-Telefon ist. Dazu wird der Telefonerkennungsmechanismus verwendet, der auch bei der Inline-Stromversorgung eingesetzt wird. Hier wird der Testton allerdings vom Patch Panel und nicht vom Switch erzeugt.

Strom aus der Steckdose

Als letzte Option wird die Versorgung des Cisco IP-Telefons mit einem lokalen Netzteil beschrieben, das an eine nahe gelegene Steckdose (maximal 3 Meter) angeschlossen ist, wie in Abbildung 2-9 dargestellt.

Abbildung 2-9 Cisco IP-Telefon, das über die Steckdose mit Strom versorgt wird



Mit einer Kombination aus diesen Stromversorgungsoptionen können Sie redundanten Strom für Cisco IP-Telefone bereitstellen. Intern werden diese drei Quellen über Schutzdioden kombiniert, d. h. das Telefon wird mit Strom versorgt, ganz gleich, welche Kombination verwendet wird.

Zusammenfassung der Empfehlungen

Sie können sich Anschlußmodulen besorgen, mit denen Sie die IP-Telefone mit Strom versorgen. Wenn Sie IP-Telefone mit vorhandenen Switches nutzen möchten, können Sie entweder eine neue Anschlußmodule besorgen, die die IP-Telefone mit Strom versorgt, oder das externe Cisco Power Patch Panel zur Versorgung der Telefone verwenden, falls für den Switch keine Anschlußmodulen erhältlich sind. Schließlich haben Sie auch die Möglichkeit, die IP-Telefone über die Steckdose zu versorgen.

IP-Adressierung und Management

Jedes IP-Telefon benötigt neben einer IP-Adresse zusätzliche Informationen wie eine Subnetzmaske, ein Standard-Gateway usw. Dies bedeutet hauptsächlich, daß Sie doppelt so viele IP-Adressen benötigen, wenn Sie Benutzern IP-Telefone zuweisen.

Diese oben genannten Angaben können statisch auf dem IP-Telefon konfiguriert oder vom Dynamic Host Configuration Protocol (DHCP) bereitgestellt werden.

Im folgenden Abschnitt werden verschiedene Möglichkeiten beschrieben, wie die Anforderungen an die IP-Adressierung erfüllt werden können.

- Zuweisen von IP-Adressen mit demselben Subnetz wie für Datengeräte
- Ändern des IP-Adressierungsplans
- Erstellen eines separaten IP-Subnetzes für IP-Telefone

Zuweisen von IP-Adressen mit demselben Subnetz wie für Datengeräte

Sie können den IP-Telefonen IP-Adressen mit demselben Subnetz zuweisen wie für Datengeräte. Dies könnte für Ihre Situation die beste Lösung darstellen. Bei vielen Standorten sind allerdings bereits über 50 % der Subnetzadressen zugewiesen. Falls dies auch auf Ihr Netzwerk zutrifft, ist dies nicht die beste Lösung für Sie.

Ändern des IP-Adressierungsplans

Sie können den IP-Telefonen Adressen aus bestehenden Subnetzen zuweisen. In diesem Fall müssen Sie den IP-Adressierungsplan jedoch neu nummerieren. Dies ist nicht immer durchführbar.

Erstellen eines separaten IP-Subnetzes für IP-Telefone

Sie können ein separates IP-Subnetz für die IP-Telefone verwenden. Das neue Subnetz kann sich in einem registrierten Adressraum oder in einem privaten Adressraum, wie Netzwerk 10.0.0.0, befinden. Bei Anwendung dieses Schemas befände sich der PC in einem Subnetz, das für Datengeräte reserviert ist, während sich das Telefon in einem Subnetz befände, das für Sprache reserviert ist. Die Konfiguration am IP-Telefon kann auf ein Minimum beschränkt werden, indem so viele Informationen wie möglich dynamisch an das Telefon übermittelt werden. Aus diesem Grund sollte ein IP-Telefon beim Einschalten automatisch sein Sprachsubnetz erkennen, damit eine DHCP-Anfrage zu einer IP-Adresse an das Subnetz gesendet werden kann.

Der automatisierte Mechanismus, über den das IP-Telefon Informationen zu seinem Sprachsubnetz erhält, ist durch Verbesserungen des Cisco Discovery Protocol (CDP) möglich.

CDP-Verbesserungen

Cisco Discovery Protocol (CDP) ist ein Geräteerkennungsprotokoll, das auf allen Cisco Geräten ausgeführt wird. Mit CDP sendet jedes Gerät periodische Nachrichten an eine Multicast-Adresse und empfängt die periodischen Nachrichten anderer Geräte. Dadurch können sich die Geräte in einem Netzwerk gegenseitig erkennen und wichtige Informationen austauschen, beispielsweise verwendete Protokolle, Protokolladressen, ursprüngliches VLAN der verbundenen Ports usw. Über CDP werden auch einige Nachrichten der Schichten 2 und 3 gesendet.

Cisco IP-Telefone verwenden CDP, um mit dem Switch zu interagieren, damit der Switch erkennt, dass ein IP-Telefon angeschlossen ist. Um dies zu ermöglichen, wurden dem CDP drei neue Felder hinzugefügt:

- Voice-VLAN-ID (VVID) zur Übermittlung des Sprachsubnetzes an das IP-Telefon.
- Trigger-Feld zum Abrufen einer Antwort vom angeschlossenen Gerät.
- Stromanforderungsfeld zur Ermittlung der exakten Stromanforderung des Telefons.

VVID-Feld

Ein VLAN (Schicht 2) wird einem Subnetz (Schicht 3) als Broadcast-Domäne zugeordnet. Damit entspricht ein VLAN einem Subnetz. Die VVID wurde mit Version 5.5 der Catalyst Software eingeführt. Es handelt sich um das Voice-VLAN, das der Switch dem IP-Telefon in der CDP-Nachricht zuweist. Damit kann das IP-Telefon seine VLAN-ID automatisch ermitteln, wenn es an den Switch angeschlossen und ein VLAN für das Telefon konfiguriert ist. Wenn kein VLAN für das IP-Telefon konfiguriert ist, befindet sich das Telefon im ursprünglichen VLAN (Datensubnetz) des Switch.

Trigger-Feld

Mit dem Trigger-Feld wird eine Antwort vom angeschlossenen Gerät erzwungen. Unter normalen Bedingungen sendet ein Gerät CDP-Update-Nachrichten in konfigurierten Intervallen (Standard ist eine Minute). Wenn ein IP-Telefon zwischen CDP-Nachrichten angeschlossen wird, kann es seine VVID nicht empfangen. In diesem Fall löst das IP-Telefon einen Trigger in der CDP-Nachricht aus, die an den Switch gesendet wird. Dadurch wird der Switch gezwungen, mit einer VVID zu antworten.

Stromanforderungsfeld

Wenn der Switch ein IP-Telefon mit Inline-Strom versorgt, besteht keine Möglichkeit, um festzustellen, wieviel Strom das Telefon benötigt (dies ist von Modell zu Modell unterschiedlich). Der Switch stellt zunächst 10 W bereit und passt die Stromzufuhr anschließend an die Anforderungen an, die vom IP-Telefon in der CDP-Nachricht übermittelt werden.

Hilfs-VLANs und Daten-VLANs

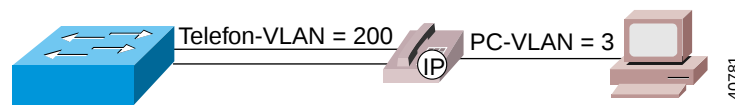
Das neue Voice-VLAN wird in der Command Line Interface (CLI) der Catalyst Software als Auxiliary-VLAN (Hilfs-VLAN) bezeichnet. Bei Verwendung von Switches befinden sich Datengeräte traditionell in einem Daten-VLAN. Mit dem neuen Auxiliary-VLAN werden andere Gerätearten gemeinsam repräsentiert. Heute handelt es sich bei diesen Geräten um IP-Telefone (daher die Bezeichnung Voice-VLAN), zukünftig werden jedoch auch andere Geräte, die keine Daten übertragen, in diesem

Zusatz-VLAN enthalten sein. So wie Datengeräte im ursprünglichen VLAN (Standard-VLAN) angesiedelt sind, werden IP-Telefone dem Auxiliary-VLAN zugeordnet, sofern eines auf dem Switch konfiguriert wurde.

Wenn das IP-Telefon eingeschaltet wird, kommuniziert es über CDP mit dem Switch. Anschließend übermittelt der Switch die konfigurierte VLAN-ID (Sprachsubnetz), auch Voice-VLAN-ID oder VVID genannt, an das Telefon. Währenddessen befinden sich die Datengeräte weiterhin im ursprünglichen VLAN (Standard-VLAN) des Switch. Ein Datengeräte-VLAN (Datensubnetz) wird als Port-VLAN-ID oder PVID bezeichnet.

Abbildung 2-10 zeigt ein IP-Telefon und einen PC in ihren VLANs.

Abbildung 2-10 Voice-VLAN-ID und Port-VLAN-ID



Verbindung mit dem Netzwerk

Im Folgenden werden die Schritte im Einzelnen beschrieben, die beim Einschalten eines IP-Telefons und beim Anschließen an das Netzwerk ausgeführt werden:

1. Das IP-Telefon beginnt einen CDP-Austausch mit dem Switch. Das Telefon gibt eine Trigger-CDP-Nachricht aus, um eine Antwort vom Switch zu erzwingen. Diese Antwort enthält die VVID des Telefons.
2. Wenn das IP-Telefon für DHCP (Standard) konfiguriert ist, gibt es eine DHCP-Anfrage an das Sprachsubnetz aus, das vom Switch übermittelt wurde. Dies ist der empfohlene Betriebsmodus. Die statische Adressierung kann zwar verwendet werden, mit ihr ist jedoch keine Mobilität möglich.
3. Das IP-Telefon erhält eine Antwort vom DHCP-Server im Netzwerk. Mit der DHCP-Antwort, in der die IP-Adresse des Telefons enthalten ist, kann auch die Adresse des TFTP-Servers übermittelt werden, der die Konfiguration des Telefons bereitstellt. Dazu muss Option 150 am DHCP-Server konfiguriert und die Adresse des TFTP-Servers angegeben werden. Der Cisco DHCP-Server unterstützt diese Funktionalität. Sie haben auch die Möglichkeit, die TFTP-Serveradresse manuell anzugeben. In diesem Fall müssen Sie jedoch Einschränkungen bei Hinzufügen oder Veränderungen im Netz in Kauf nehmen und auch sonst auf einige Vorteile verzichten.
4. Das IP-Telefon nimmt die Verbindung zum TFTP-Server auf und erhält eine Liste mit Adressen von Cisco CallManagern. In dieser Liste können bis zu drei Cisco CallManager angegeben werden. Dadurch wird Redundanz gewährleistet, für den Fall, dass der erste Cisco CallManager in der Liste nicht verfügbar ist.

5. Das IP-Telefon stellt nun eine Verbindung zum Cisco CallManager her und meldet sich an. Im Gegenzug erhält das Telefon eine Konfigurationsdatei und Laufzeitcode, der für den Betrieb des Telefons erforderlich ist. Für jede Konfiguration erhält das IP-Telefon eine Directory Number (DN) vom Cisco CallManager, die für Anrufe bei diesem IP-Telefon benötigt wird.
6. Mit dem IP-Telefon können nun Anrufe entgegengenommen und getätigt werden.

**Hinweis**

Dieser Vorgang dauert ca. 90 Sekunden. Um diesen Vorgang zu beschleunigen, aktivieren Sie Portfast, und deaktivieren Sie das Channeling und das Trunking für den Port. Dadurch wird der Vorgang auf 30 Sekunden verkürzt.

Beispieladressierungsplan und Empfehlungen

Abbildung 2-11 zeigt Beispiele der bevorzugten IP-Adressierung für Verbindungen zwischen IP-Telefonen und PCs.

Abbildung 2-11 Bevorzugte IP-Adressierungspläne

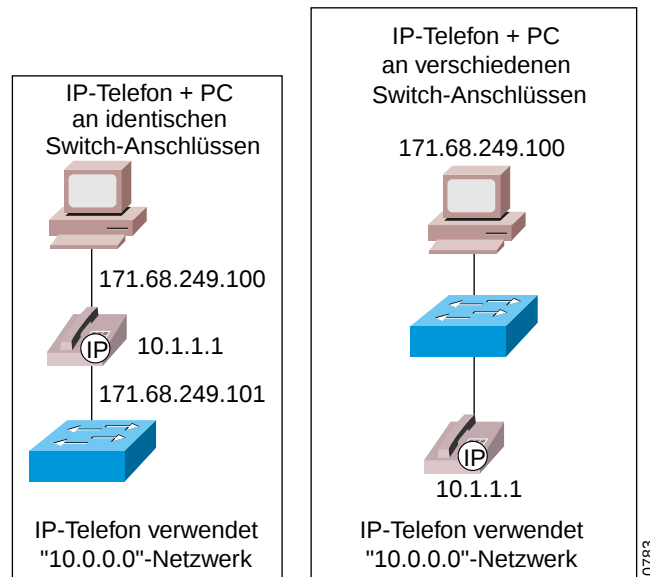
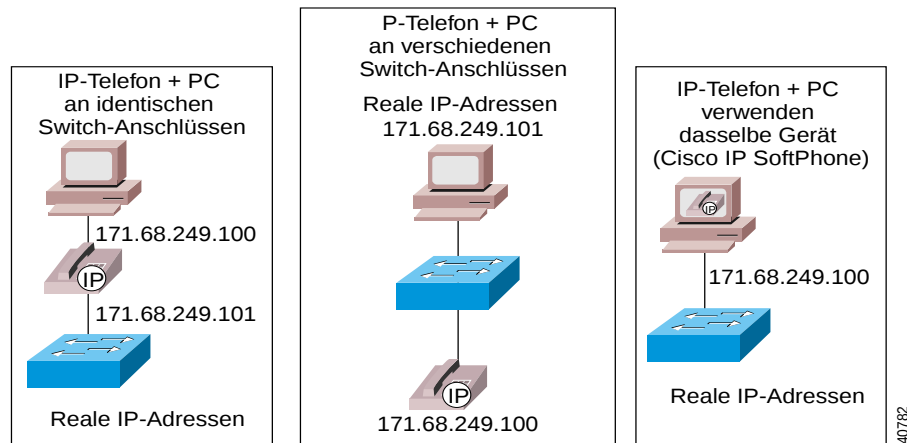


Abbildung 2-12 zeigt Beispiele der bevorzugten IP-Adressierung für Verbindungen zwischen IP-Telefonen, PCs und Cisco IP SoftPhones.

Abbildung 2-12 Optionale IP-Adressierungspläne



Es folgen einige allgemeine Empfehlungen im Hinblick auf die IP-Adressierung:

- Verwenden Sie die vorhandene Adressierung für Datengeräte.
- Fügen Sie IP-Telefone mit DHCP als Mechanismus für neue Adressen hinzu.
- Verwenden Sie einen eindeutigen Bereich für IP-Adressen (z. B. RFC 1918).
- Verwenden Sie nach Möglichkeit ein Zusatz-VLAN. Dazu benötigen Sie einen Switch mit verbesserter Software, der 802.1Q unterstützt.

Quality of Service

In einer Konvergenzumgebung werden verschiedene Verkehrsarten über eine einzige Transportinfrastruktur transportiert. Dennoch sind nicht alle Verkehrsarten gleich. Daten treten in Schüben auf, sind intolerant gegenüber Verlusten und nicht empfindlich gegenüber Latenzzeiten. Sprache tritt im Gegensatz dazu nicht in stoßweise auf und ist im Hinblick auf Verluste toleranter. Gegenüber Latenzzeiten ist Sprache allerdings sehr empfindlich. Das Ziel ist es, den Anforderungen jeder dieser Verkehrsarten gerecht zu werden.

Wenn sowohl Sprache als auch Daten in einem Netzwerk übermittelt werden, sind entsprechende Quality of Service (QoS)-Tools erforderlich, um den Verzögerungs- und Verlustparametern des Sprachverkehrs Rechnung zu tragen. Diese Tools sind in IP-Telefonen, Switches und Routern integriert.

Weitere Informationen zu QoS in WANs finden Sie in Kapitel 8, "Quality of Service",.

Klassifizierungsarten für Netzwerkverkehr

Um zu verhindern, dass der Sprachverkehr vom Datenverkehr unterdrückt wird, muss dem Sprachverkehr eine hohe Priorität zugewiesen werden. Anschließend muss festgelegt werden, dass der Verkehr mit hoher Priorität vor dem Verkehr mit niedriger Priorität übertragen wird. Die Klassifizierung erfolgt folgendermaßen auf der Schicht 2 oder 3:

- Auf Schicht 2 werden die drei Bits im 802.1p-Feld verwendet (auch Class of Service oder CoS genannt), das Teil des 802.1Q-Tag ist.
- Auf Schicht 3 werden die drei Bits des Differentiated Services Code Point (DSCP)-Feldes im Type of Service (ToS)-Byte des IP-Headers verwendet.

Die Klassifizierung ist der erste Schritt, um Quality of Service zu erzielen. Dieser Schritt sollte im Idealfall so nahe wie möglich an der Quelle erfolgen, in der Regel auf der Zugriffsschicht des Netzwerks.

Trust Boundaries - Vertrauensgrenzen

Das Vertrauensprinzip ist ein wichtiger Faktor bei der Implementierung von QoS. Sobald für die Endgeräte Class of Service (CoS)- oder Type of Service (ToS)-Einstellungen festgelegt sind, kann der Switch entscheiden, ob er ihnen vertraut oder nicht. Wenn der Switch den Einstellungen vertraut und sie für sicher hält, ist eine Neuklassifizierung nicht erforderlich. Falls die Einstellungen nicht als sicher gelten, muss eine Neuklassifizierung für die gewünschte QoS-Einstellung erfolgen.

Dieses Vertrauen bzw. die Einstufung als sicher oder nicht sicher bildet die Grundlage für Vertrauensgrenzen. Die Klassifizierung erfolgt im Idealfall so nahe wie möglich an der Quelle. Wenn das Endgerät diese Aufgabe übernehmen kann, bildet die Vertrauensgrenze für das Netzwerk die Zugriffsschicht im Etagenverteiler. Falls das Gerät seine Funktion nicht ausführen kann oder der Switch am Etagenverteiler der Klassifizierung des Endgeräts misstraut, kann die Vertrauensgrenze verschoben werden. Wie diese Verschiebung erfolgt, hängt von den Leistungsmerkmalen des Switch am Etagenverteiler ab. Wenn der Switch die Pakete neu klassifizieren kann, bildet der Etagenverteiler die Vertrauensgrenze. Wenn der Switch seine Funktion nicht ausführen kann, übernehmen andere Geräte im Netzwerk (in Richtung Backbone) diese Aufgabe. In diesem Fall sollte die Neuklassifizierung im Normalfall auf der Verteilungsschicht ausgeführt werden. Das bedeutet, die Vertrauensgrenze wurde auf die Verteilungsschicht verschoben. Es ist sehr wahrscheinlich, dass es auf der Verteilungsschicht einen High-End-Switch gibt, der diese Funktion unterstützt. Vermeiden Sie es, diesen Vorgang im Zentrum des Netzwerks auszuführen.

Im Allgemeinen sollten Sie versuchen, als Vertrauensgrenze den Etagenverteiler zu definieren. Falls erforderlich, können Sie sie von Fall zu Fall auf die Verteilungsschicht verschieben. Vermeiden Sie es jedoch, sie zum Zentrum des Netzwerks zu verschieben. Diese Empfehlung wird auch von der allgemeinen Richtlinie bestätigt, wonach Vertrauensgrenzen sich so nahe wie möglich an der Quelle befinden sollen.

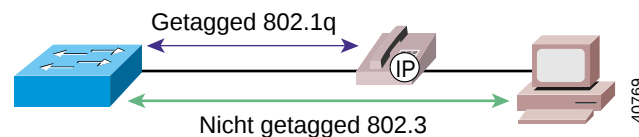


Hinweis Bei dieser Beschreibung wurde ein Netzwerkmodell mit drei Schichten zu Grunde gelegt, das sich als skalierbare Architektur erwiesen hat. Wenn sich bei einem kleinen Netzwerk die logischen Funktionen der Verteilungsschicht und der zentralen Schicht im selben Gerät befinden, kann sich die Vertrauensgrenze im Zentrum befinden, falls sie vom Etagenverteiler verschoben werden muss.

Klassifizierung des Verkehrs auf Schicht 2

Cisco IP-Telefone können Sprachpaketen über CoS oder ToS eine hohe Priorität zuweisen. Das Telefon sendet standardmäßig getaggte 802.1Q-Pakete mit dem CoS- und ToS-Wert 5. Abbildung 2-13 zeigt Pakete, die vom IP-Telefon als getaggte bzw. nicht getaggte Frames gesendet werden. Das 802.1p-Feld ist auf 5 gesetzt, und Frames vom PC werden nicht getaggt gesendet.

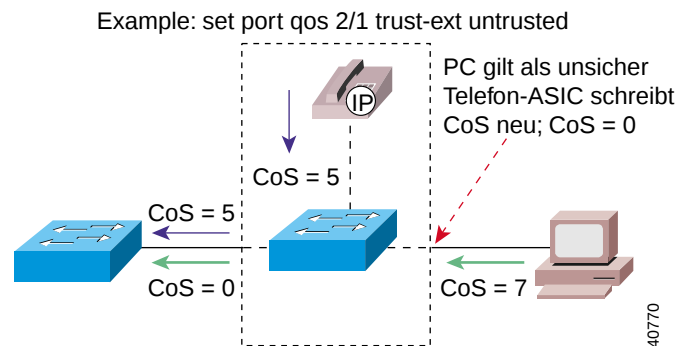
Abbildung 2-13 Frame-Tagging mit PVID und VVID



Da die meisten PCs keine Netzwerkkarte besitzen, die 802.1Q unterstützt, werden die Pakete nicht getaggt gesendet. Das bedeutet, dass die Frames kein 802.1p-Feld besitzen. Dieses Feld ist null, sofern die auf dem PC ausgeführten Anwendungen keine Pakete mit einem bestimmten CoS-Wert senden. Ein Sonderfall tritt ein, wenn der TCP/IP-Stapel im PC modifiziert wurde und alle Pakete mit einem anderen ToS-Wert als null gesendet werden. Dies ist normalerweise nicht der Fall, und der ToS-Wert ist null.

Wenn der PC getaggte Frames mit einem bestimmten CoS-Wert sendet, können Cisco IP-Telefone diesen Wert auf Null setzen, bevor sie die Frames an den Switch senden. Dieses Standardverhalten wird in Abbildung 2-14 veranschaulicht. Frames, die vom Telefon stammen, haben den CoS-Wert 5, während Frames, die vom PC stammen, den CoS-Wert 0 aufweisen. Wenn der Switch diese Frames empfängt, kann er diese Werte basierend auf seinen Leistungsmerkmalen zur weiteren Verarbeitung verwenden.

Abbildung 2-14 PC gilt als nicht sicher



Der Switch verwendet seine Queues (pro Port verfügbar) zum Zwischenspeichern von eingehenden Frames, bevor sie an die Switching-Engine gesendet werden. (Beachten Sie, dass Eingangs-Queuing nur bei Überlastungen auftritt.) Der Switch verwendet den bzw. die CoS-Werte, um die Frames den entsprechenden Queues zuzuordnen. Der Switch kann auch Mechanismen anwenden, wie Weighted Random Early Detection (WRED), um intelligente Drops in einer Queue zu ermöglichen (auch Überlastungsvermeidung genannt), und Weighted Round-Robin (WRR), um einigen Queues mehr Bandbreite zur Verfügung zu stellen als anderen (auch Überlastungsmanagement genannt).

Beispielszenario für den Catalyst 6000

Jeder Port an den Switches der Catalyst 6000-Familie hat eine Queue für den Empfang und zwei Queues für die Übertragung. Auf der Empfängerseite kommen alle Pakete in eine reguläre Queue. Tail Drop wird in dieser regulären Queue zur Vermeidung von Überlastungen verwendet. Dieser Mechanismus wird jedoch nur angewendet, wenn eine Überlastung auf der Empfängerseite besteht. In den meisten Fällen ist dies unwahrscheinlich, da bei einem Frame, der von einem 10/100-Ethernet- oder Gigabit-Ethernet-Port bei einem 32-GBit/s-Bus ankommt, keine Überlastung auftritt.

Auf der Übertragungsseite werden die CoS-Werte 0, 1, 2 und 3 der niedrigen regulären Queue zugeordnet, während die CoS-Werte 4, 5, 6 und 7 der hohen regulären Queue zugeordnet werden. Darüber hinaus kann WRED in jeder Queue dazu verwendet werden, intelligente Drops basierend auf dem CoS-Wert und dem Prozentsatz des Puffers, der bereits voll ist, vorzunehmen. Abschließend wird die WRR-Konfiguration auf die hohe und die niedrige reguläre Queue angewendet. Diese Queues sind konfigurierbar. Sie können beispielsweise ein Verhältnis von 25 zu 75 festlegen.



Hinweis Alle Werte für WRED, WRR und die Queue-Größe sind konfigurierbar.

Die bisherigen Erläuterungen haben sich mit der in Abbildung 2-14 dargestellten Konstellation befasst: Der Sprachverkehr weist den CoS-Wert 5 auf, und der PC-Verkehr wird auf Null reduziert, falls ein Tag vorhanden ist. In manchen Fällen können Sie dem CoS-Wert des PCs jedoch vertrauen (wenn getaggte Pakete gesendet werden) oder einen anderen Wert als null zuweisen. Dies ist mit Catalyst Switches ebenfalls möglich.

Abbildung 2-15 zeigt ein Szenario, in dem der PC als vollkommen sicher gilt. Der vorgegebene CoS-Wert wird akzeptiert.

Abbildung 2-15 PC gilt als sicher

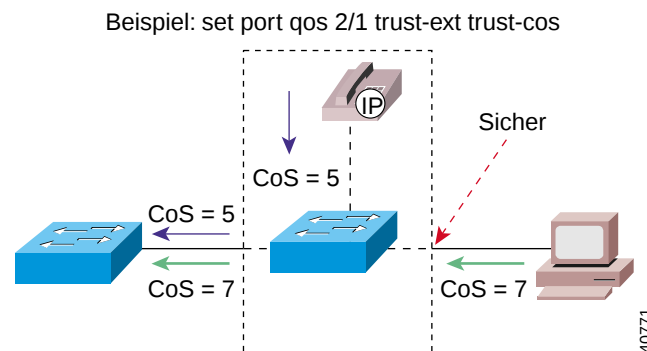
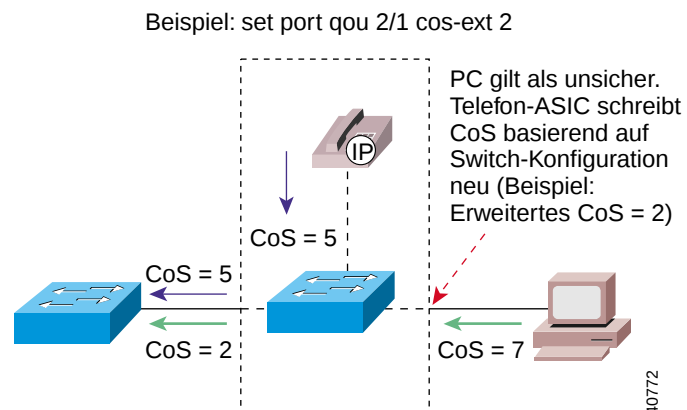


Abbildung 2-16 zeigt ein weiteres Szenario, in dem dem PC nicht vollständig vertraut wird. Die Servicestufe ist jedoch höher als mit CoS=0. Dies wird erreicht, indem der PC-Verkehr durch einen bestimmten CoS-Wert erweitert wird.

Abbildung 2-16 PC gilt nicht als sicher, erhält jedoch einen anderen CoS-Wert als null





Hinweis Alle beschriebenen Konfigurationen können für jeden Catalyst Switch verwendet werden, auf dem Cisco CatOS oder die ursprüngliche Cisco IOS-Software (z. B. Catalyst 3524XL) ausgeführt wird.

Klassifizierung des Verkehrs auf Schicht 3

Mit den 802.1p-Bits im 802.1Q-Tag erhalten Sie die gewünschten QoS-Ergebnisse auf Schicht 2. Wenn der Verkehr eine Grenze zur Schicht 3 überschreiten muss, ist es jedoch erforderlich, diese Mechanismen mit Parametern der Schicht 3 zu implementieren, etwa den 3 IP-Prioritäts-Bits (häufig ToS genannt) oder den neuen DSCP-Parametern, die die sechs höchstwertigen Bits im ToS-Byte des IP-Headers verwenden. Der Verkehr überschreitet dann eine Grenze zur Schicht 3, wenn die Pakete von Switches oder Routern der Schicht 3 zwischen Subnetzen geroutet werden. Der Verkehr überschreitet auch dann die Grenze zu Schicht 3, wenn die Pakete das Campus-Netzwerk verlassen und über Rand-Router in das WAN gelangen. In diesem Fall ist die Klassifizierung auf Schicht 2 ungeeignet. Um die gewünschte QoS-Ebene zu erreichen, ist eine Klassifizierung auf Schicht 3 erforderlich. Alle von den Routern angewendeten QoS-Techniken (einschließlich die wichtige WAN-QoS-Technik) basieren auf der Klassifizierung auf Schicht 3.

Die Klassifizierung auf Schicht 3 erfolgt über die geeigneten Plattformen im Campus. Mit den IP-Telefonen als Ausgangspunkt kommen die Pakete bereits mit den Werten CoS = ToS = 5 beim Switch an. Diese Klassifizierung auf Schicht 3 wird selbst dann beibehalten, wenn die Pakete bis zum WAN-Zugangsroutern transportiert werden, wo der Header der Schicht 2 entfernt wird. Wenn sich die Vertrauensgrenze also bei der Quelle (beim IP-Telefon) befindet, sind die ToS-Bits des Sprachverkehrs auf 5 gesetzt, und der Sprachverkehr wird zur Verarbeitung an die Netzwerkgeräte weitergeleitet. WAN-Router können diese Klassifizierung verwenden, um eine der Queuing-Techniken anzuwenden. Wenn die Vertrauensgrenze sich nicht bei der Quelle befindet und die Pakete neu klassifiziert werden müssen, sollte das Gerät, das diese Aufgabe übernimmt, dies auf der Schicht 3 tun, bevor Grenzen der Schicht 3 überschritten werden können.

Klassifizierung auf Schicht 3 für den Cisco Catalyst 6000

Die Switches der Cisco Catalyst 6000-Familie sind mit der Policy Feature Card (PFC) ausgestattet und führen die Klassifizierung auf Schicht 3 automatisch aus, wenn der Port als sicher gilt. Wenn ein Paket also mit dem Wert CoS = 5 bei einem sicheren Port ankommt, nimmt der Switch diesen Wert und setzt die ToS-Bits ebenfalls auf 5 zurück. Die Konfiguration ist damit abgeschlossen. Wenn der Port nicht als sicher gilt, wird dem Paket am Eingangs-Port ein CoS-Standardwert zugewiesen.

Anschließend können Sie eine Zugriffskontrollliste (Access Control List (ACL)) für QoS auf dem Switch konfigurieren und ToS basierend auf zutreffenden Kriterien auf einen gewünschten Wert einstellen.

In den ACLs für QoS können auch Informationen der Schicht 4 zur Klassifizierung einzelner Anwendungen enthalten sein. Switches der Cisco Catalyst 6000-Familie können den Verkehr auch basierend auf den Adressen der Schicht 3 und den Port-Nummern der Schicht 4 überwachen. Sie können beispielsweise einzelne HTTP-Ströme auf 1 MBit/s und alle HTTP-Ströme auf 25 MBit/s beschränken.


Tipps

Wenn sich die Vertrauensgrenze am Switch eines Etagenverteilers befindet, der keine Klassifizierung auf Schicht 3 vornehmen kann, können Sie die Vertrauensgrenze auf die Verteilungsschicht verschieben, auf der ein Gerät, das die Klassifizierung auf Schicht 3 vornimmt, mit größerer Wahrscheinlichkeit vorhanden ist.

Zusammenfassung der Leistungsmerkmale und Empfehlungen

Tabelle 2-2 bietet eine Übersicht über die Leistungsmerkmale der Switches der Cisco Catalyst Familie.

Tabelle 2-2 Übersicht über die QoS-Funktionalität der Switches der Cisco Catalyst Familie.

Plattform	Vertrauensfunktion	Neuklassifizierung CoS	Neuklassifizierung ToS	Überlastungsvermeidung (WRED)	Prioritäts-Queue	Mehrere Queues	Überlastungsmanagement (WRR)	Policing
Catalyst 6000	Ja	Ja	Ja	Ja	Nein	Ja	Ja	Ja
Catalyst 5000	Nein	Ja	Ja ¹	Ja	Nein	Nein	Nein	Nein
Catalyst 4000	Nein	Ja	Nein	Nein	Nein	Ja	Nein	Nein
Catalyst 3500	Ja	Ja	Nein	Nein	Ja	Ja	Nein ²	Nein

1. Mit Zusatzkonfiguration

2. Nur Round Robin


Hinweis

Die einzigen Cisco LAN-Switches, die ein Minimum von zwei Queues unterstützen und Sprachqualität gewährleisten, sind derzeit: Cisco Catalyst 8500, Catalyst 6XXX-Familie, Catalyst 4XXX-Familie, Catalyst 3500XL und Catalyst 2900XL.

Es folgen einige allgemeine Empfehlungen im Hinblick auf die QoS-Implementierung:

- Erstellen Sie eine Vertrauensgrenze am Netzwerkrand im Etagenverteiler. Geben Sie am Switch des Etagenverteiles, an dem die IP-Telefone angeschlossen sind, an, dass Ports sicher sind.
- Klassifizieren Sie ToS neu am Rand, wenn die Geräte nicht als sicher eingestuft werden können.
- Verlegen Sie die Vertrauensgrenze auf die Verteilungsschicht, und klassifizieren Sie ToS dort neu, wenn die Neuklassifizierung am Rand nicht möglich ist.
- Verwenden Sie nach Möglichkeit eine Prioritäts-Queue für Verkehr, der bei Verzögerungen empfindlich ist.
- Verwenden Sie ACLs für QoS für eine gröbere Klassifizierung der Pakete mit Informationen der Schicht 4.
- Verwenden Sie bei Bedarf Policing, um den Verkehr für einzelne Ströme bzw. zusammengefasste Ströme einzuschränken.
- Führen Sie für Verkehr zu WAN-Zuganggeräten, die Klassifizierung auf Schicht 3 durch, damit der Router ihn für verbesserte WAN-Queuing-Mechanismen verwenden kann.
- Verwenden Sie einen WAN-Zugang-Router zum Klassifizieren von sehr kleinen Remote-Netzwerken, bei denen kein Switch vorhanden ist, der eine Klassifizierung auf Schicht 3 vornimmt.



Cisco CallManager-Cluster

Richtlinien für die Verwendung und Skalierbarkeit von Clustern

Mit dem Cisco CallManager Version 3.0(5) kann ein Cluster bis zu acht Server enthalten, wovon sechs die Anrufverarbeitung übernehmen können. Die beiden anderen Server können als dedizierter Datenbank-Publisher und als dedizierter TFTP-Server konfiguriert werden.

Mit dem Datenbank-Publisher werden alle Konfigurationsänderungen vorgenommen und Datensätze mit Anrufrdetails erstellt. Der TFTP-Server vereinfacht das Downloaden von Konfigurationsdateien, Gerätedaten (Betriebscode) und Ruftontypen.

Für große Systeme werden ein dedizierter Datenbank-Publisher und ein dedizierter TFTP-Server empfohlen. Bei kleineren Systemen kann die Funktion des Datenbank-Publishers und des TFTP-Servers kombiniert werden. Tabelle 3-1 enthält Richtlinien für die Skalierung von Geräten mit Cisco CallManager-Clustern.

Tabelle 3-1 Richtlinien für Cisco CallManager-Cluster

Erforderliche Anzahl an IP-Telefonen im Cluster	Empfohlene Anzahl an Cisco CallManagern	Maximale Anzahl an IP-Telefonen pro Cisco CallManager
2.500	Insgesamt drei Server: • Publisher/TFTP (kombiniert) • Ein primärer Cisco CallManager • Ein Backup-Cisco CallManager	2.500

Tabelle 3-1 Richtlinien für Cisco CallManager-Cluster (Fortsetzung)

Erforderliche Anzahl an IP-Telefonen im Cluster	Empfohlene Anzahl an Cisco CallManagern	Maximale Anzahl an IP-Telefonen pro Cisco CallManager
5.000	Insgesamt vier Server: • Publisher/TFTP (kombiniert) • Zwei primäre Cisco CallManager • Ein Backup-Cisco CallManager	2.500
10.000	Insgesamt acht Server: • Datenbank-Publisher • TFTP-Server • Vier primäre Cisco CallManager • Zwei Backup-Cisco CallManager	2.500

Mit diesen Empfehlungen erhalten Sie eine optimale Lösung. Sie können die Redundanz auch reduzieren und benötigen dann weniger Server. Bei kleinen Systemen können der Datenbank-Publisher, der TFTP-Server und die Cisco CallManager-Backup-Funktion zusammengefasst werden.

Bei Verwendung der MCS-7835-Plattform können maximal 5000 Geräte bei einem Cisco CallManager angemeldet werden, d. h. maximal 2500 IP-Telefone, Gateways und Digital Signaling Processor (DSP)-Geräte, wie Transcoding- und Conferencing-Ressourcen. Falls einer der Cisco CallManager im Cluster ausfällt, bleibt die maximale Geräteanzahl, die pro Cisco CallManager angemeldet sein kann, 5000.

Gewichtung der Geräte

Es können sich viele verschiedene Gerätetypen bei einem Cisco CallManager anmelden. Für jede dieser Ressourcen – IP-Telefone, Voicemail-Anschlüsse, Telephony Application Programming Interface (TAPI)-Geräte, Java Telephony API (JTAPI)-Geräte, Gateways und DSP-Ressourcen für Transcoding und Conferencing – ist die Gewichtung anders. Tabelle 3-2 zeigt die Gewichtung der einzelnen Ressourcentypen basierend auf der Speicher- und CPU-Nutzung.

Tabelle 3-2 Gewichtung nach Gerätetyp

Gerätetyp	Gewichtung pro Sitzung/ Sprachkanal	Sitzung/DS0 pro Gerät	Summe Gerätegewichtung
IP-Telefon	1	1	1
Analoge Gateway-Anschlüsse	3	Variiert	3 pro DS0
E1-Gateway	3	30	90 pro E1
Transcoding-Ressource	3	Variiert	3 pro Sitzung
Software-MTP	3	48	144 ¹
Konferenzressource (Hardware)	3	Variiert	3 pro Sitzung
Konferenzressource (Software)	3	48	144 ¹
CTI-Port (TAPI und JTAPI)	20	1	20
Cisco SoftPhone	20	1	20
Messaging (Voicemail)	3	Variiert	3 pro Sitzung
Intercluster-Trunk	3	Variiert	3 pro Sitzung

1. Bei Installation auf demselben Server wie der Cisco CallManager sind es maximal 48 Sitzungen.

Es hängt von der Serverplattform ab, wieviele Geräte ein Cisco CallManager steuern kann. Tabelle 3-3 bietet eine Übersicht über die maximale Geräteanzahl pro Plattform.

Tabelle 3-3 Maximale Geräteanzahl pro Serverplattform

Eigenschaften der Serverplattform	Maximale Geräteanzahl pro Server	Maximale Anzahl IP-Telefone pro Server
MCS-7835-1000 ¹ PIII 1000MHz, 1G RAM	5000	2500
MCS-7825-800 ¹ PIII 800 MHz, 512 M RAM	1000	500

1. Diese Serverplattform ab dem ersten Quartal 2001 erhältlich.

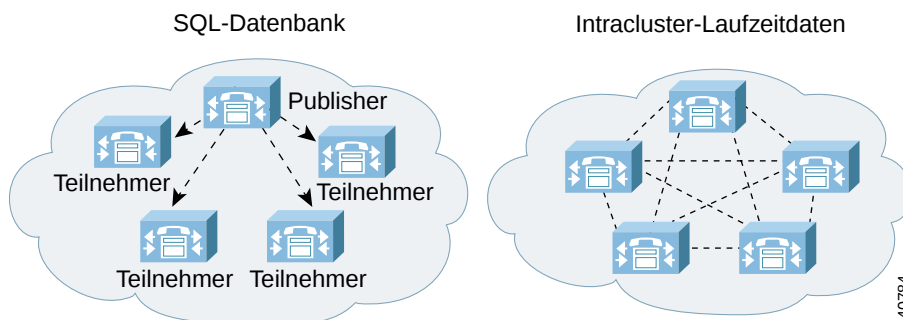
Mit der MCS-7835-Plattform können maximal 2500 IP-Telefone bei einem Cisco CallManager angemeldet werden, auch dann, wenn IP-Telefone die einzigen angemeldeten Geräte sind. Um die Anzahl der IP-Telefone zu berechnen, die bei einem Cisco CallManager angemeldet werden können, subtrahieren Sie den Gewichtungswert für alle anderen Ressourcen als IP-Telefone von der maximal für diese Plattform zulässigen Geräteanzahl. Bei der MCS-7835-Plattform beträgt die maximale Geräteanzahl 5000.

Intracuster-Kommunikation

Es gibt zwei grundlegende Arten der Intracuster-Kommunikation in einem Cisco CallManager-Cluster (Abbildung 3-1). Bei der ersten handelt es sich um einen Mechanismus zur Verteilung der Datenbank, die alle Informationen zur Gerätekonfiguration enthält. Die Konfigurationsdatenbank (Microsoft SQL 7.0) wird auf einem Publisher gespeichert und auf die Subscriber-Mitglieder des Clusters repliziert. Änderungen am Publisher werden an die Subscriber-Datenbanken übertragen. Dadurch wird gewährleistet, dass die Konfiguration für alle Cluster-Mitglieder konsistent bleibt. Darüber hinaus wird eine bessere räumliche Redundanz der Datenbank sichergestellt.

Die zweite Intracuster-Kommunikationsart betrifft die Übertragung und Replikation von Laufzeitdaten, etwa die Anmeldung von IP-Telefonen, Gateways und DSP-Ressourcen. Diese Informationen werden allen Mitgliedern eines Clusters mitgeteilt. Auf diese Weise wird ein optimales Routing von Anrufen zwischen Cluster-Mitgliedern und zugehörigen Gateways sichergestellt.

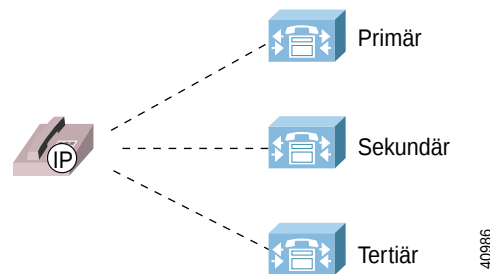
Abbildung 3-1 Intracuster-Kommunikation



Cisco CallManager-Redundanz

In einem Cluster kann jedem angemeldeten IP-Telefon eine Prioritätsliste mit maximal drei Cisco CallManagern, die zur Anrufverarbeitung zur Verfügung stehen, zugewiesen werden. Gemeinsam genutzte Ressourcen, wie Gateways, die das Skinny Gateway Protocol verwenden, können dieses Redundanzschema ebenfalls anwenden. Das Media Gateway Control Protocol (MGCP) liefert mit einem ähnlichen Prinzip ebenfalls räumliche Redundanz für die Anrufverarbeitung. Peer-to-Peer-Protokolle wie H.323 erleichtern ebenfalls das Bereitstellen von Redundanz.

Abbildung 3-2 zeigt das Redundanzschema mit drei Cisco CallManagern.

Abbildung 3-2 Cisco CallManager-Redundanzgruppe

Jedes IP-Telefon führt aktive TCP-Sitzungen mit seinem primären und sekundären Cisco CallManager. Diese Konfiguration vereinfacht das Umschalten, falls der primäre Cisco CallManager einmal ausfallen sollte. Sobald der primäre Cisco CallManager wieder betriebsbereit ist, wird er wieder verwendet.

Konfiguration von Redundanzgruppen

Sie erreichen eine Anrufverarbeitungsredundanz für Ihr System, indem Sie Cisco CallManager-Redundanzgruppen konfigurieren. Eine Cisco CallManager-Redundanzgruppe ist eine Prioritätsliste mit maximal drei Cisco CallManagern. Sie können einer bestimmten Cisco CallManager-Redundanzgruppe einzelne Geräte zuweisen. Eine Cisco CallManager-Redundanzgruppe ist eine Untergruppe eines Clusters, d. h. die Mitglieder einer Redundanzgruppe sind immer auch Mitglieder eines Clusters.



Hinweis Die Größe von Clustern und Redundanzgruppen kann sich in zukünftigen Versionen des Cisco CallManagers ändern.

Folgende Empfehlungen gelten für die Konfiguration von Redundanzgruppen für den Cisco CallManager Version 3.0(5):

- Cisco CallManager-Cluster für maximal 2500 Benutzer:
 - Server A ist ein dedizierter Datenbank-Publisher und TFTP-Server.
 - Server B ist der primäre Cisco CallManager für alle angemeldeten Geräte.
 - Server C ist der Backup-Cisco CallManager für alle angemeldeten Geräte.

In der oben beschriebenen Konfiguration wird nur eine Cisco CallManager-Redundanzgruppe für die Server B und C benötigt.

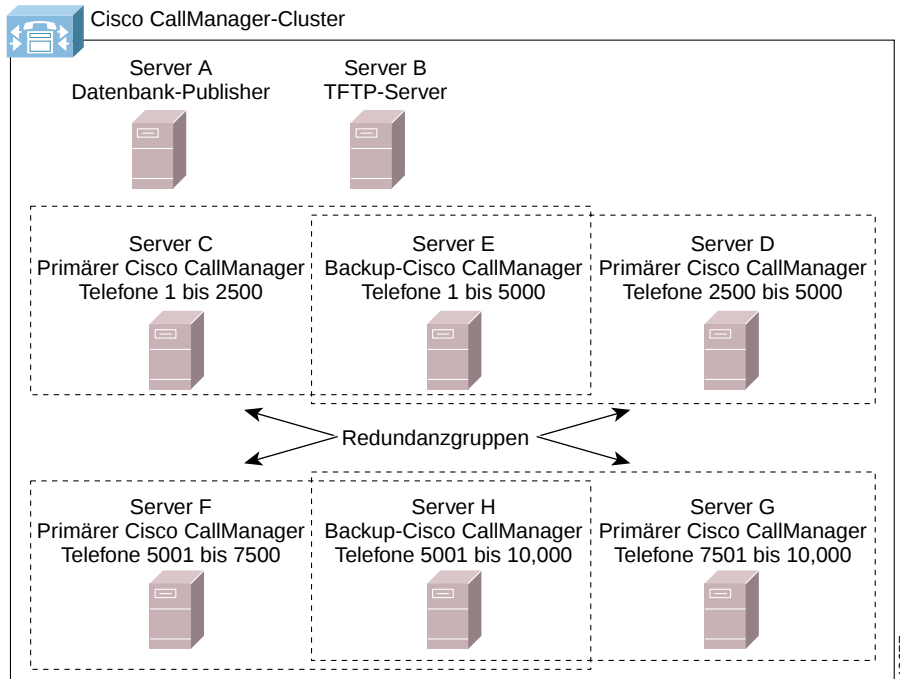
- Cisco CallManager-Cluster für maximal 5000 Benutzer:
 - Server A ist ein dedizierter Datenbank-Publisher und TFTP-Server.

- Server B ist der primäre Cisco CallManager für die IP-Telefone 1 bis 2500.
- Server C ist der primäre Cisco CallManager für die IP-Telefone 2501 bis 5000.
- Server D ist der Backup-Cisco CallManager für alle angemeldeten Geräte.

In der oben beschriebenen Konfiguration werden zwei Cisco CallManager-Redundanzgruppen für die Server BD und CD benötigt.

- Cisco CallManager-Cluster für maximal 10.000 Benutzer:
 - Server A ist ein dedizierter Datenbank-Publisher.
 - Server B ist ein dedizierter TFTP-Server.
 - Server C ist der primäre Cisco CallManager für die IP-Telefone 1 bis 2500.
 - Server D ist der primäre Cisco CallManager für die IP-Telefone 2501 bis 5000.
 - Server E ist der Backup-Cisco CallManager für die IP-Telefone 1 bis 5000.
 - Server F ist der primäre Cisco CallManager für die IP-Telefone 5001 bis 7500.
 - Server G ist der primäre Cisco CallManager für die IP-Telefone 7501 bis 10.000.
 - Server H ist der Backup-Cisco CallManager für die IP-Telefone 5001 bis 10.000.

In der oben beschriebenen Konfiguration werden vier Cisco CallManager-Redundanzgruppen für die Server CE, DE, FH und GH benötigt. In Abbildung 3-3 wird diese Konfiguration dargestellt. Um dreifache Redundanz zu erhalten, müssen Sie die Redundanzgruppen als CEH, DEH, FHE und GHE konfigurieren.

Abbildung 3-3 Redundanzgruppen für große Systeme


Hinweis Falls ein Cisco CallManager einmal ausfällt, werden Anrufe unter Umständen unterbrochen und müssen neu getätigt werden.

Richtlinien für Campus-Cluster

Alle Mitglieder eines Cisco CallManager-Clusters müssen über ein LAN verbunden werden. Für Cisco CallManager Version 3.0(5) werden WANs nicht unterstützt.

Sie müssen Folgendes beachten, wenn Sie ein IP-Telefonienetzwerk für einen Campus konfigurieren:

- Beim Cisco CallManager Version 3.0(5) sind maximal acht Server pro Cluster zulässig.
- Es können maximal 10.000 Geräte angemeldet werden.
- Pro Cisco CallManager sind maximal 2500 angemeldete IP-Telefone oder 5000 Geräte zulässig. Dabei sind auch Geräte enthalten, die unter Fehlerbedingungen angemeldet wurden.
- Geswitchte Infrastruktur zum Arbeitsplatz (gemeinsam genutzte Medien werden nicht unterstützt).

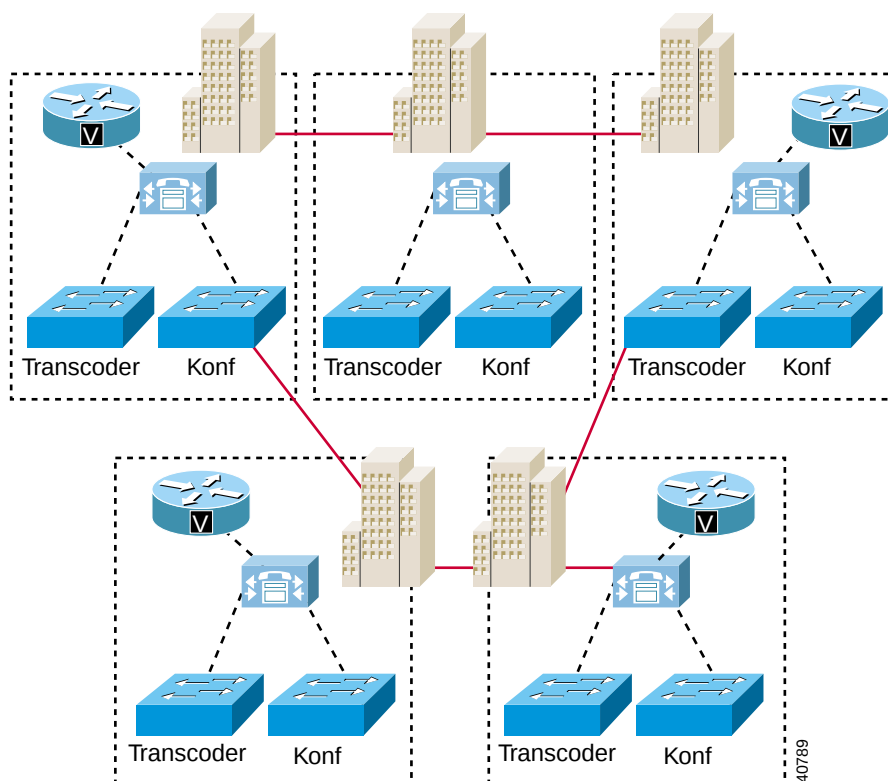
In einer geswitchten Campus-Infrastruktur können Sie generell davon ausgehen, dass die Bandbreite für Sprachanwendungen ausreicht. Diese Bandbreitenverfügbarkeit ist abhängig vom Design und der

Kapazitätenplanung im Campus. Weitere Faktoren sind die Vertrauensgrenze und das erforderliche Queuing (siehe Kapitel 2, "Informationen zur Campus-Infrastruktur"). Bei einem Campus-Cluster ist keine Anrufzugangskontrolle erforderlich.

Cisco CallManager-Server sollten auf dem Campus verteilt werden, damit räumliche Redundanz und Zuverlässigkeit sichergestellt sind. Bei vielen Standorten in Städten oder Campus-Gebäuden gibt es nur ein Kabelrohr, das für die IP-Konnektivität anderer Cluster-Mitglieder verwendet wird. Wenn in einem solchen Fall die IP-Konnektivität unterbrochen wird, muss ein lokaler Server die lokale Anrufverarbeitung vornehmen. Gateway-Ressourcen für den PSTN/ISDN-Zugriff sollten ebenfalls an strategischen Stellen platziert werden, um eine möglichst hohe Verfügbarkeit zu erzielen.

Abbildung 3-4 zeigt einen typischen Campus- oder Metropolitan Area Network (MAN)-Cluster.

Abbildung 3-4 Campus- oder MAN-Cluster



In Abbildung 3-4 befindet sich in jedem der fünf Gebäude (Standorte) ein Cisco CallManager. Mit dieser Konfiguration ist bei einem Ausfall die lokale Anrufverarbeitung an jedem Standort möglich. Wenn die Glasfaserkabel so verlegt sind, dass kein lokaler Cisco CallManager erforderlich ist, kann die Anrufverarbeitung in einem oder mehreren Datenzentren erfolgen.

Ressourcen, wie Transcoding- und Conferencing-DSP, sind keine gemeinsam genutzten Ressourcen und müssen jedem Cisco CallManager zugewiesen werden. Auch hier gilt: Wenn Fehlertoleranzen erforderlich sind, müssen diese Ressourcen dupliziert werden, außerdem empfiehlt sich räumliche Redundanz. Dies kann dadurch erreicht werden, dass die Ressourcen in strategisch günstig gelegenen Multilayer-Switches positioniert werden.

Intercluster-Kommunikation

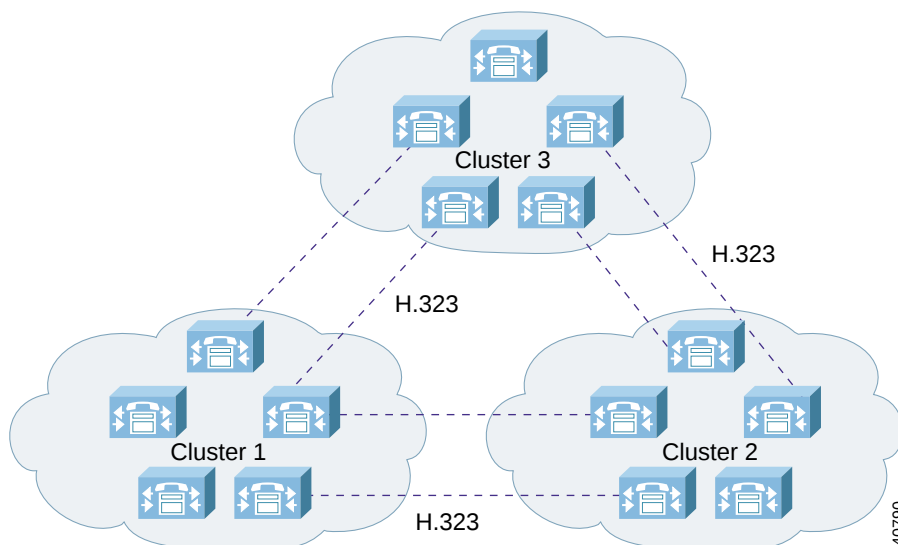
Die folgenden Abschnitte befassen sich mit der Intercluster-Kommunikation und mit Adressen für Cluster in abgeschlossenen Campus-Umgebungen, Multisite-WANs mit verteilter Anrufverarbeitung und Multisite-WANs mit zentraler Anrufverarbeitung.

Cluster-Nutzung im Campus

Wenn in einem Campus-Netzwerk mehr als 10.000 Benutzer vorhanden sind, sind zusätzliche Cluster erforderlich. Wenn für die lokale Anrufverarbeitung an den einzelnen Standorten bzw. in den einzelnen Gebäuden mehr als die maximale Anzahl an zulässigen Cisco CallManagern in einem Cluster erforderlich ist, sind ebenfalls zusätzliche Cluster nötig.

Die Kommunikation zwischen Clustern erfolgt über die standardbasierte H.323-Signalisierung. Bei einem großen Campus oder MAN, bei dem in der Regel die mehr Bandbreite als nötig verfügbar ist, ist die Intercluster-Anrufzugangskontrolle nicht erforderlich. Abbildung 3-5 zeigt diese Konnektivität zwischen Clustern in einem LAN.

Abbildung 3-5 Campus-Intercluster-Kommunikation mit H.323



In Abbildung 3-5 entsprechen die Punklinien den H.323-Intercluster-Verbindungen, die in Paaren konfiguriert werden, um für Redundanz zu sorgen, für den Fall, dass die IP-Konnektivität zu einem Mitglied des Clusters verloren geht. Falls gewünscht, können Sie diese Verbindungen vollmaschig konfigurieren. Cisco empfiehlt allerdings, die Intercluster-Konfiguration auf zwei Peers zu beschränken. Dadurch erhalten Sie in den meisten Fällen ausreichende Sicherheit. Wenn ein Gatekeeper verwendet wird, empfiehlt Cisco nur eine H.323-Verbindung pro Cluster. Sie können Redundanz implementieren, indem Sie eine Cisco CallManager-Redundanzgruppe verwenden, die dem Gatekeeper zugewiesen ist.

Im Gegensatz zu früheren Versionen ist für den Cisco CallManager Version 3.0(5) kein MTP erforderlich, um zusätzliche Dienste für H.323-Geräte bereitzustellen. Der Cisco CallManager 3.0(5) verwendet das "Empty Capabilities Set" von H.323v2, um das Öffnen und Schließen von logischen Kanälen zwischen H.323-Geräten wie Cisco CallManager-Clustern und Cisco IOS-Gateways, auf denen Cisco IOS Version 12.0(7)T oder höher ausgeführt wird, zu erleichtern.

Cluster für Multisite-WAN mit verteilter Anrufverarbeitung

Wenn Cluster über ein WAN miteinander verbunden sind, besteht ein erhöhtes Risiko, dass es zu Überlastungen kommt. Das Netzwerk sollte so aufgebaut sein, dass das Sprachverkehrsaufkommen problemlos bewältigt werden kann. In diesen Fällen wird eine Anrufzugangskontrolle benötigt. Da Cluster mit H.323 verbunden sind, kann ein Cisco IOS-Gateway verwendet werden, um diese Gatekeeper-Funktion zu erleichtern. Jeder Cluster kann als Zone mit maximal konfigurierter Bandbreite für Sprachanrufe ausgewiesen werden.

Wenn ein Gatekeeper verwendet wird, benötigt der Cisco CallManager eine Bandbreite von 128 KBit/s pro G.711-Intercluster-Anruf und 20 KBit/s pro G.729a-Intercluster-Anruf. Im Allgemeinen empfiehlt Cisco die Konfiguration von einem Codec für Anrufe, die das WAN durchlaufen, da dadurch das Bereitstellen von Bandbreite vereinfacht wird.

Tabelle 3-4 und Tabelle 3-5 enthalten Empfehlungen für die Bandbreitenkonfiguration bei Intercluster-Anrufen.

Tabelle 3-4 Empfohlene Bandbreitenkonfiguration für Intercluster-Anrufe mit G.729

Anzahl der Intercluster-Anrufe	Benötigte Bandbreite pro Anruf		Benötigte Bandbreite bei WAN-Verbindungen (LLQ/CBWFQ ¹)		Konfigurierte Bandbreite (am Gatekeeper)	
	Ohne cRTP ²	Mit cRTP	Ohne cRTP	Mit cRTP	Ohne cRTP	Mit cRTP
2	24 KBit/s	12 KBit/s	48 KBit/s	24 KBit/s	40 KBit/s	40 KBit/s
5	24 KBit/s	12 KBit/s	120 KBit/s	60 KBit/s	100 KBit/s	100 KBit/s
10	24 KBit/s	12 KBit/s	240 KBit/s	120 KBit/s	200 KBit/s	200 KBit/s

1. Low Latency Queuing/Class Based Weighted Fair Queuing

2. Komprimiertes Echtzeit-Transportprotokoll (Compressed Real-time Transport Protocol)

Tabelle 3-5 Empfohlene Bandbreitenkonfiguration für Intercluster-Anrufe mit G.711

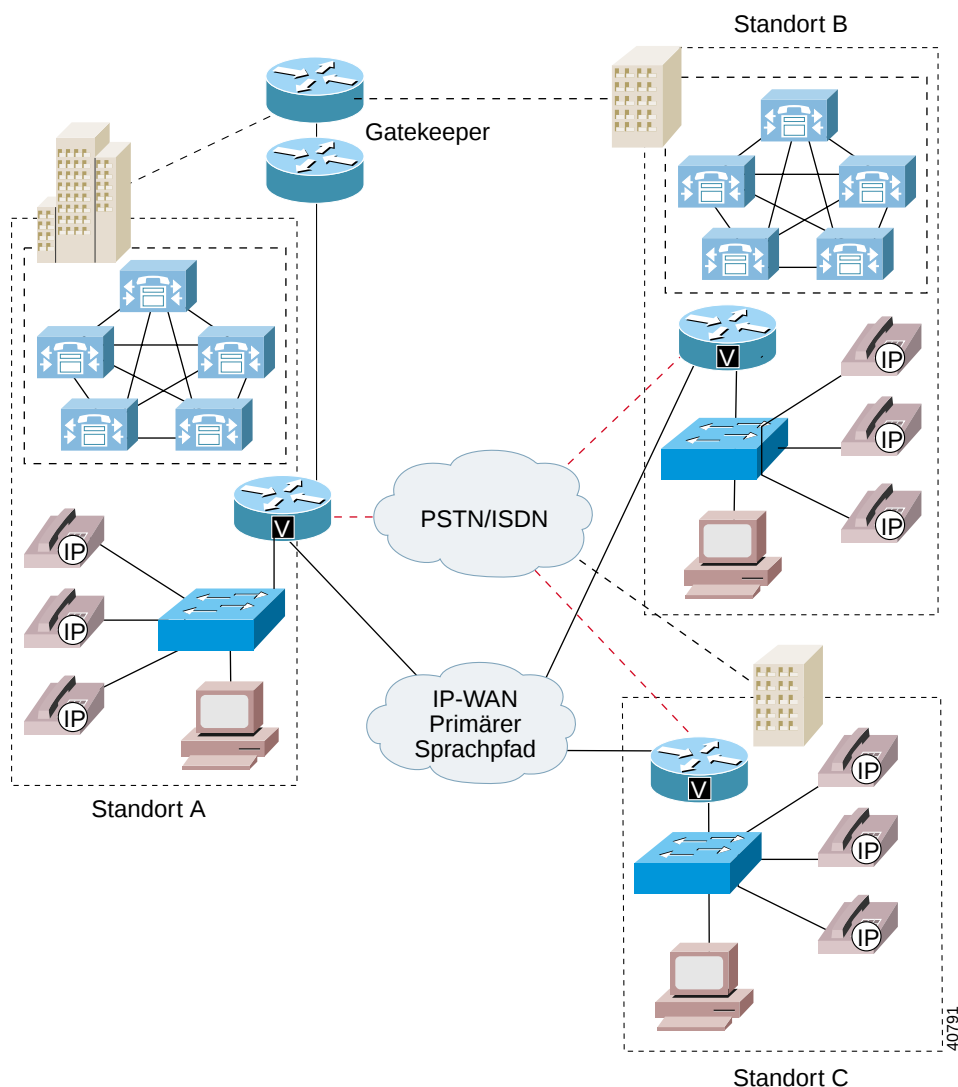
Anzahl der Intercluster-Anrufe	Erforderliche Bandbreite pro Anruf	Benötigte Bandbreite bei WAN-Verbindungen (LLQ/CBWFQ)	Konfigurierte Bandbreite (am Gatekeeper)
2	80 KBit/s	160 KBit/s	256 KBit/s
5	80 KBit/s	400 KBit/s	640 KBit/s
10	80 KBit/s	800 KBit/s	1280 KBit/s

Wenn Sie einen Gatekeeper verwenden, wird die Anrufzugangskontrolle sowohl für eingehende als auch für ausgehende Anrufe durchgeführt. Mit dem Cisco CallManager Version 3.0(5) können sich maximal 100 Cisco CallManager bei einem Gatekeeper anmelden. Diese Methode der Anrufzugangskontrolle ist auf einen aktiven Gatekeeper pro Netzwerk beschränkt. Redundanz kann mit dem Hot Standby Routing Protocol (HSRP) zwischen zwei Gatekeepern erzielt werden.

Die Gatekeeper-Anrufzulassungskontrolle ist ein Policy-based Verfahren. Dafür ist eine statische Konfiguration der verfügbaren Ressourcen erforderlich. Netzwerktopologien können nicht erkannt werden. Daher müssen Sie die Gatekeeper-Anrufzugangskontrolle auf Hub-und-Spoke-Topologien einschränken, wobei sich ein oder mehrere redundante Gatekeeper (HSRP) am Hub befinden müssen. Sie müssen ein WAN verwenden, und die Prioritäts-Queue für Sprachanrufe muss so eingerichtet werden, dass alle zugelassenen Anrufe unterstützt werden.

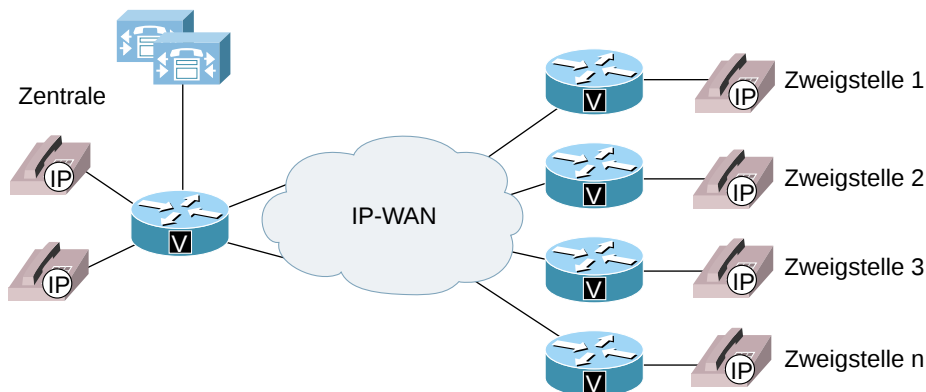
Abbildung 3-6 veranschaulicht dieses Modell.

Abbildung 3-6 Intercluster-Kommunikation mit Gatekeepern



Cluster für Multisite-WAN mit zentraler Anrufverarbeitung

Wie bereits erwähnt, müssen Cisco CallManager in einem Cluster über ein LAN verbunden werden. Mit dem Cisco CallManager kann die Anrufzugangskontrolle auch an den einzelnen Standorten durchgeführt werden. Dieses Verfahren eignet sich für kleine Zweigstellen und Telecommuter, für die die entfernte Anrufverarbeitung akzeptabel ist. Abbildung 3-7 veranschaulicht dieses Modell.

Abbildung 3-7 Anrufzugangskontrolle an den einzelnen Standorten

In Abbildung 3-7 wird die Anrufverarbeitung ausschließlich am zentralen Standort verwaltet. Die Geräte in den Zweigstellen sind einem Standort zugeordnet und entsprechend konfiguriert. Beispiel: In Zweigstelle 1 gibt es 12 IP-Telefone, die alle für den Standort der Zweigstelle 1 konfiguriert sind. Der Cisco CallManager kann so ermitteln, wieviel Bandbreite pro Standort genutzt wird bzw. noch verfügbar ist. Die WAN-Anrufe können entsprechend zugelassen oder abgewiesen werden.

Dieses Schema wurde im Cisco CallManager Version 3.0(5) erweitert, so dass für die zentrale Anrufverarbeitung nun bis zu 2500 Remote-Geräte zulässig sind. Um diese Lösung mit dem Cisco CallManager Version 3.0(5) zu implementieren, wird ein dedizierter Cisco CallManager-Cluster mit einem aktiven Cisco CallManager benötigt. Damit kann der Anrufstatus aufrechterhalten und die Anrufzugangskontrolle durchgeführt werden.



Hinweis Bei dieser Art der zentralen Konfiguration sind maximal 2500 Benutzer pro Cluster zulässig. Dabei spielt die Anzahl der Cisco CallManager im Cluster (1, 2 oder 3 aus Redundanzgründen) keine Rolle. Außerdem kann in einem zentralen Cluster immer nur ein Cisco CallManager aktiv sein.

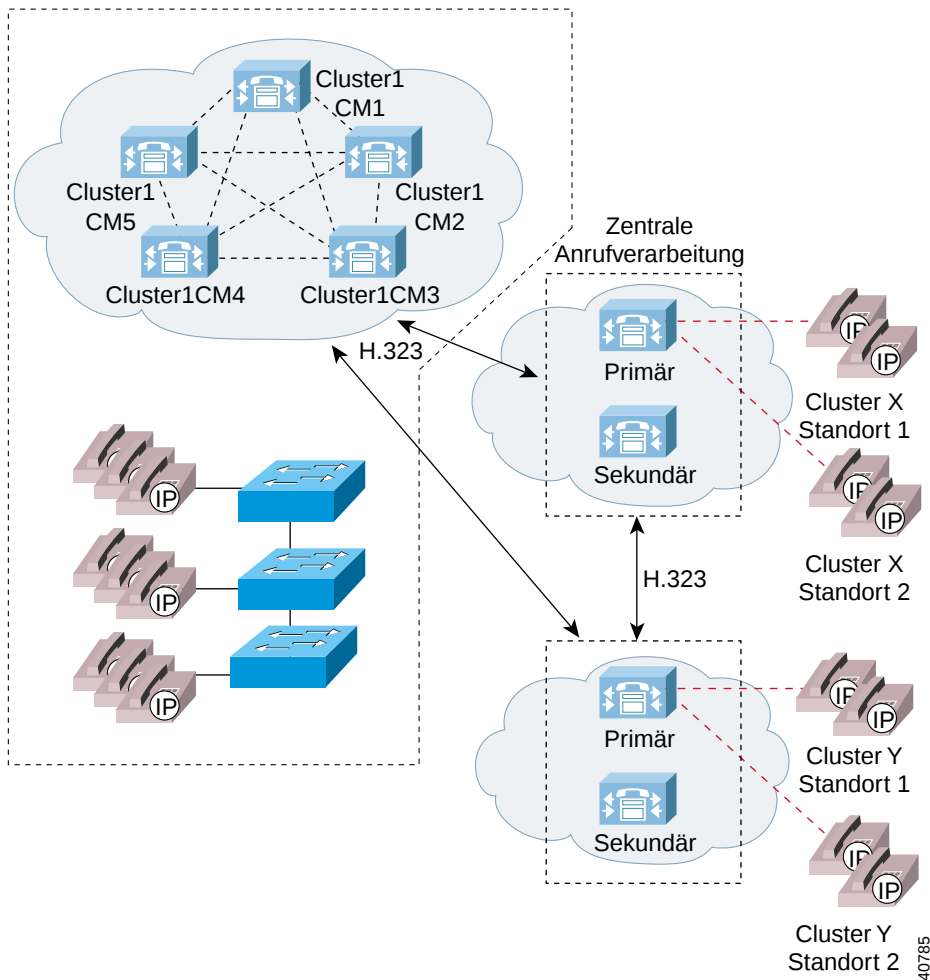
Um dies zu gewährleisten, sollten alle Geräte einer Cisco CallManager-Redundanzgruppe zugewiesen werden. Diese Cisco CallManager-Redundanzgruppe besteht aus einer Prioritätsliste mit maximal drei Cisco CallManagern. Für einen Cluster mit zentraler Anrufverarbeitung wird nur eine Cisco CallManager-Redundanzgruppe empfohlen. Diese sollte die Standardgruppe sein. In dem Beispiel aus Abbildung 3-8 besteht die Redundanzgruppe aus drei Cisco CallManagern, wobei A der primäre, B der sekundäre und C der tertiäre Cisco CallManager ist.

Abbildung 3-8 Konfiguration der Cisco CallManager-Redundanzgruppen



Bei einem typischen Modell mit zentraler Anrufverarbeitung ist es möglich, nur zwei Cisco CallManager zu verwenden. In diesem Fall empfiehlt Cisco, den normalerweise inaktiven (sekundären) Cisco CallManager als Publisher zu verwenden. Bei einem Cluster mit drei Cisco CallManagern sollte ein dedizierter Publisher (tertiär) verwendet werden, wobei IP-Telefone und Gateways dem primären und sekundären Cisco CallManager zugewiesen werden sollten.

Abbildung 3-9 zeigt ein Hybrid-Modell, bei dem ein Campus-Cluster mit zwei Clustern verbunden ist, die die zentrale Anrufverarbeitung durchführen. Dieses Beispiel zeigt, dass mehrere zentrale Anrufverarbeitungs-Cluster verwendet und über H.323 verbunden werden können. Konnektivität mit dem Campus-Cluster wird ebenfalls über H.323 hergestellt. Wenn die Intercluster-Anrufzugangskontrolle erforderlich ist, kann ein Gatekeeper zugewiesen werden.

Abbildung 3-9 Cluster mit zentraler Anrufverarbeitung, der mit zwei Clustern verbunden ist

Transparente Intracenter- und Intercenter-Funktionen

Die verteilte Architektur eines Cisco CallManager-Clusters bietet folgende wichtige Vorteile für die Anrufverarbeitung:

- Räumliche Redundanz
- Zuverlässigkeit
- Verfügbarkeit
- Beständigkeit

Darüber hinaus bietet ein Cluster transparente Unterstützung von Benutzerfunktionen für alle Geräte im Cluster. Das bedeutet, dass die verteilte IP-Telefonie und all ihre Funktionen problemlos auf dem gesamten Campus oder in einem Hochgeschwindigkeits-MAN genutzt werden können.

Durch die Intercluster-Kommunikation über H.323 kann ein Teil der Funktionen zwischen Clustern ausgetauscht werden. Folgende Funktionen können derzeit zwischen Clustern ausgetauscht werden:

- Allgemeines Anruf-Setup
- G.711- und G.729-Anrufe
- Konferenzschaltungen mit mehreren Teilnehmern
- Halten von Anrufen
- Makeln von Anrufen
- Rufnummernanzeige

Das Parken von Anrufen ist zwar in einem Cluster, aber nicht zwischen Clustern möglich.



Gateway-Auswahl

Unterstützte Protokolle

Bei Cisco CallManager Version 3.0(5) werden drei Typen von Gateway-Protokollen unterstützt:

- Skinny Gateway Protocol – Dieses Protokoll wird von digitalen Gateways einschließlich dem Cisco Access Digital Trunk Gateway DT-24+ und DE-30+ sowie dem Cisco Catalyst 6000 Voice Gateway-Modul verwendet.
- Media Gateway Control Protocol (MGCP) – Dieses Protokoll wird von Cisco CallManager zur Steuerung des neuen analogen Standalone-Gateways Cisco Voice Gateway 200 (VG200) verwendet.
- H.323 – Dieses Protokoll wird von Cisco IOS-integrierten Router-Gateways zur Kommunikation mit Cisco CallManager verwendet.

Von diesen drei Typen können heute nur die Cisco IOS H.323-Gateways alle Routing-Funktionen und -Fähigkeiten sowie VoIP-Gateway-Funktionen bieten. Beide Gateways, die auf dem Skinny Gateway Protocol und dem VG200 MGCP-Gateway basieren, fungieren als anwendungsspezifische Standalone-Gateways.

In Tabelle 4-1 wird dargestellt, welche Protokolle von jedem Gateway unterstützt werden. In den folgenden Abschnitten wird erörtert, wie jedes dieser Protokolle Unterstützung für die wichtigsten Gateway-Funktionsmerkmale bietet.

Tabelle 4-1 Cisco IP-Telefonie-Gateways und unterstützte Protokolle

Gateway	Skinny Gateway Protocol	H.323	MGCP
VG200	Nein	Ja	Ja
DT-24+ und DE-30+	Ja	Nein	Nein
Catalyst 4000 WS-X4604-GWY Gateway-Modul	Ja, für Konferenzschaltungs- und MTP Transcoding-Service	Ja, für Schnittstellen zu PDTN/ISDN	Zukünftig
Catalyst 6000 WS-X6608-E1 Gateway-Modul	Ja	Nein	Zukünftig

Tabelle 4-1 Cisco IP-Telefonie-Gateways und unterstützte Protokolle (Fortsetzung)

Gateway	Skinny Gateway Protocol	H.323	MGCP
Cisco 1750	Nein	Ja	Nein
Cisco 3810 V3	Nein	Ja	Zukünftig
Cisco 2600	Nein	Ja	Zukünftig
Cisco 3600	Nein	Ja	Zukünftig
Cisco 7200	Nein	Ja	Nein
Cisco 7500	Nein	Zukünftig	Nein
Cisco AS5300	Nein	Ja	Nein

IOS H.323-Gateways

Nur H.323 Version 1 wurde vor Cisco CallManager Version 3.0 unterstützt. Es war nicht möglich, das Ziel eines Echtzeit-Transportprotokoll (RTP)-Datenstroms nach der Einrichtung eines H.323 Version 1-Anrufs zu ändern. Somit konnten keine zusätzlichen Dienste, wie z. B. Halten der Verbindung, Weiterleiten und Übertragen, bereitgestellt werden. Da H.323 Version 1 keine Funktionen zum Verschieben eines RTP-Datenstroms von einem Ziel zu einem anderen nach der ursprünglichen Anrufeinrichtung bietet, wurde das Software-MTP-Tool für Unterstützung für zusätzliche Dienste auf den Cisco IOS-Gateways verwendet.

MTP, das als Software-Prozess entweder auf dem Cisco CallManager oder auf einem separaten Windows NT 4.0-Server ausgeführt wird, terminiert RTP-Signale des Cisco IOS-Gateways und RTP-Signale eines IP-Telefons. Somit kann ein IP-Telefon zusätzliche Dienste unterstützen, wenn ein Cisco IOS-Gateway verwendet wird, da die RTP-Signale vom MTP zum Cisco IOS-Gateway nicht geändert werden, bis der Anruf beendet wird. Alle Änderungen der RTP-Signale werden auf der Seite der Skinny Station der MTP-Verbindung vorgenommen. Ein weiterer entscheidender Nachteil des Software-MTPs besteht darin, dass es nur G.711-Sprachsignale unterstützt, jedoch keine komprimierten Sprachanrufe. Hierdurch werden WAN-Systeme stark eingeschränkt.

Durch die Verwendung von H.323 Version 2 in Cisco IOS Version 12.0(7)T und höher (besonders die Funktionsmerkmale OpenLogicalChannel, CloseLogicalChannel und emptyCapabiliySet) mit Cisco IOS-Gateways und Cisco CallManager Version 3.0(5) wird für zusätzliche Dienste kein MTP mehr benötigt. Da MTP nicht mehr zur Terminierung des G.711 RTP-Datenstroms von IP-Telefonen und dem Cisco IOS-Gateway benötigt wird, werden jetzt auch komprimierte Sprachanrufe (G.723.1 und G.729a) zwischen Cisco IOS-Gateways und Cisco CallManager-Endpunkten unterstützt.

Wenn ein H.323v2-Anruf zwischen einem Cisco IOS-Gateway und einem IP-Telefon mit dem Cisco CallManager als H.323-Proxy eingerichtet ist, kann das IP-Telefon eine Änderung der Trägerverbindung anfordern. Da der RTP-Datenstrom direkt mit dem IP-Telefon vom Cisco IOS-Gateway verbunden ist, kann ein unterstützter Voice Codec verhandelt werden.

Durch die folgenden Schritte wird der Prozess verdeutlicht, der auftritt, wenn ein IP-Telefon 1 den Anruf vom Cisco IOS-Gateway auf das IP-Telefon 2 übertragen möchte.

1. IP-Telefon 1 sendet mithilfe des Skinny Station Protocols eine Übertragungsanfrage an Cisco CallManager.
2. Cisco CallManager übersetzt diese Anfrage in eine H.323 Version 2-CloseLogicalChannel-Anfrage an den Cisco IOS-Gateway nach der richtigen Sitzungs-ID.
3. Der Cisco IOS-Gateway schließt den RTP-Kanal zu IP-Telefon 1.
4. Cisco CallManager sendet über das Skinny Station Protocol eine Anfrage an IP-Telefon 2, eine RTP-Verbindung zu dem Cisco IOS-Gateway herzustellen. Gleichzeitig sendet Cisco CallManager eine OpenLogicalChannel-Anfrage mit den neuen Zielparametern, jedoch mit derselben Sitzungs-ID, an den Cisco IOS-Gateway.
5. Wenn der Cisco IOS-Gateway die Anfrage akzeptiert hat, wird ein Trägerkanal für RTP-Sprachdaten zwischen IP-Telefon 2 und dem Cisco IOS-Gateway eingerichtet.

Standort-spezifische Gateway-Anforderungen

Die folgende Liste führt beispielhafte Fragen bezüglich der erforderlichen Funktionsmerkmale auf, die vor der Auswahl eines Cisco IP-Telefonie-Gateways geklärt werden sollten.

- Wird ein analoger oder ein digitaler Gateway benötigt?
- Welche Kapazität ist für den Gateway erforderlich?
- Welche Verbindungsart soll der Gateway verwenden (beispielsweise FXO Basisstart, E1-R2, netzwerkseitige oder benutzerseitige PRI)?
- Welche Arten von zusätzlichen Diensten werden gewünscht?
- Ist Sprachkomprimierung ein Teil des Konzepts? Wenn ja, welche Arten?
- Wird eine direkte Einwahl benötigt?

Die direkte Einwahl ist ein Funktionsmerkmal von Nebenstellenanlagen (PBX) und Nebenstellendiensten über das Fernsprechamt, bei denen abgehende Anrufe ohne einen Vermittler direkt über eine Teilnehmerleitung getätigt werden können.

- Wird eine Rufnummernanzeige (Calling Line ID = CLID) benötigt?

CLID ist ein Dienst, der in digitalen Telefonnetzen verfügbar ist und über den dem angerufenen Teilnehmer die Rufnummer des Anrufers angezeigt wird. Die Geräte der Zentrale identifiziert die Telefonnummer des

Anrufers, so dass Informationen über den Anrufer zusammen mit dem Anruf selbst gesandt werden können. Ein anderer Begriff für CLID ist ANI (automatische Nummernidentifizierung).

- Wird eine Umleitung zum Faxgerät benötigt?
- Welche Art von Netzwerkmanagement schnittstelle wird bevorzugt?
- In welches Land soll die Hardware geliefert werden?
- Ist für alle benötigten Gateways, Router und Switches genügend Raum für das Rack vorhanden?

Diese Liste der Funktionsmerkmale könnte zwar noch beliebig erweitert werden, bietet jedoch so einen Ausgangspunkt, durch den die mögliche Auswahl beschränkt werden kann.

Zu einer weiteren Beschränkung der Anforderungen kann die standortspezifische Liste mit Tabelle 4-2 und Tabelle 4-3 verglichen werden, in denen analoge und digitale Gateways mit den von ihnen unterstützten Funktionsmerkmalen einander gegenübergestellt werden.

Tabelle 4-2 Analoge Gateways nach standortspezifischen Funktionsmerkmalen

Gateway	FXS	FXO	E & M ¹	Analoges DID/CLID
Cisco 1750	Ja	Ja	Ja	Zukünftig
Cisco 3810 V3	Ja	Ja	Ja	12.1(3)T/12.1(2)XH
Cisco 2600	Ja	Ja	Ja	12.1(3)T/12.1(2)XH
Cisco 3600	Ja	Ja	Ja	12.1(3)T/12.1(2)XH
Cisco 7200	Nein	Nein	Nein	Nicht verfügbar
Cisco 7500	Nein	Nein	Nein	Nicht verfügbar
Cisco AS5300	Nein	Nein	Nein	Nicht verfügbar
Catalyst 4000 WS-X4604-GWY Gateway-Modul	Ja	Ja	Ja	12.1(5)T/12.1(5)T
Catalyst 6000 WS-X6608-E1 Gateway-Module	Ja	Nein	Nein	Nein/Ja

1. PBX-Signalisierung. Die überwachende E&M-Signalisierung verwendet separate Pfade für Sprache und Signale, anstatt sowohl Sprache als auch Signale über denselben Draht zu senden. Die Buchstaben E&M stehen für die englischen Begriffe Ear and Mouth (Ohr und Mund), als Signalempfänger bzw. -sender.



Hinweis

Für ein angegebenes Funktionsmerkmal, beispielsweise FXS oder FXO, ist mindestens eine bestimmte Cisco IOS-Version erforderlich.

Tabelle 4-3 Digitale Gateways nach Standort-spezifischen Funktionsmerkmalen

Gateway	T1 CAS ¹	E1/R2	E1 CAS	PRI auf Benutzer-seite ²	PRI auf Netzwerk-seite	BRI auf Benutzer-seite ³	BRI auf Netzwerk-seite	Digitale DID ⁴ /CLID ⁵
Cisco 1750	Nein	Nein	Nein	Nein	Nein	Zukünftig	Zukünftig	Nicht verfügbar
Cisco 3810 V3	Ja	Nein	Ja	Nein	Nein	Ja	Nein	Ja
Cisco 2600	Ja	12.1(3)T	12.1(3)T	12.1(3)T	12.1(3)T	Ja	12.2(1)T	Ja/Ja ⁶
Cisco 3600	Ja	12.1(3)T	12.1(3)T	12.1(3)T	12.1(3)T	Ja	12.2(1)T	Ja/Ja ⁶
Cisco 7200	Ja	12.1(3)T	12.1(3)T	12.1(3)T	12.1(3)T	Nein	Nein	Ja/Ja ⁶
Cisco 7500	Ja	12.1(3)T	12.1(3)T	12.1(3)T	12.1(3)T	Nein	Nein	Ja/Ja ⁶
Cisco AS5300	Ja	Ja	Ja	Ja	12.0.7T	Nein	Nein	Ja/Ja
Catalyst 4000 WS-X4604-GWY Gateway-Modul	Ja	Ja	Ja	Ja	Ja	Zukünftig	Zukünftig	Ja/Ja ⁶

1. Channel Associated Signaling
2. Primary Rate Interface
3. Basic Rate Interface
4. Direkte Einwahl
5. Rufnummernanzeige
6. Für E1 CAS CLID wird FG-D benötigt. FG-D ist ein lokaler Zugriffs- und Transportbereich (local access transport area = LATA) auf Seite der Trunk-Leitung, der eine Überwachung von Anrufen für einen Austauschträger (Interexchange Carrier = IC), einen einheitlichen Zugriffscode (10XXX), optionale Identifizierung des Anrufers, die Aufzeichnung der Zugriffskostendetails sowie eine Vorabanmeldung bei einem Kunden-definierten IC bietet. FG-D wird außerdem für 800 eingehende großflächige Telekommunikationsdienste und Travel Card-Dienste verwendet und bietet die automatische Nummernidentifizierung (ANI) zu Rechnungszwecken.

In Tabelle 4-4 werden die Gateways jedes Typs mit den zugehörigen Datenschnittstellen, Schnittstellen zum öffentlichen Fernsprechwahlnetz/ISDN und unterstützter Sprachkomprimierung aufgeführt.

Tabelle 4-4 Gateways mit unterstützten Schnittstellen und Kompressionsarten

Gateway-Typ	Gateway	Datenschnittstellen	Analoge Schnittstellen zum öffentlichen Fernsprechwahlnetz/ISDN	Digitale Schnittstellen zu PSTN/ISDN in DS0s	Sprachkomprimierung
Skinny Gateway Protocol	Catalyst 6000 WS-X6624-FXS	10/100/1000-Ethernet	24	0	G.711, G.729a
	Catalyst 6000 WS-X6608-E1	10/100/1000-Ethernet, POS/FlexWAN	0	240	G.711, G.729a
H.323	Cisco 1750	10BaseT, T1/E1 seriell	4	0	G.711, G.729
	VG200	100BaseT	4	48/60	G.711, G.729a, G.723.1
	Cisco 2600	10/100BaseT, Token Ring, T1/E1 seriell	4	48/60	G.711, G.729a, G.723.1
	Cisco 3620	10/100BaseT, Token Ring, T1/E1 seriell, E1-OC3 ATM	4	48/60	G.711, G.729a, G.723.1
	Cisco 3640	10/100BaseT, Token Ring, T1/E1 seriell, E1-OC3 ATM	12	136/180	G.711, G.729a, G.723.1
	Catalyst 4000	10/100/1000-Ethernet	6 bei FCS	48/60	G.711, G.729a, G.723.1
	Cisco 3660	10/100BaseT, Token Ring, T1/E1 seriell, E1-OC3 ATM, HSSI	24	288/360	G.711, G.729a, G.723.1
	Cisco 7200	10/100BaseT, Token Ring, T1/E1 seriell, E1-OC12 ATM	0	288/360	G.711, G.729a, G.723.1



Architektur und Konfiguration von Wählplänen

In diesem Kapitel werden Architektur und Anwendung des Cisco CallManager-Wählplans beschrieben sowie Empfehlungen im Hinblick auf das Design gegeben. Ein Wählplan ist im Wesentlichen eine Schnittstelle für ein Telefonesystem, die es den Benutzern erlaubt, sich gegenseitig problemlos durch die Eingabe von Wählfolgen zu erreichen, die vom System an verschiedene Standorte weitergeleitet werden.

Architektur des Cisco CallManager-Wählplans

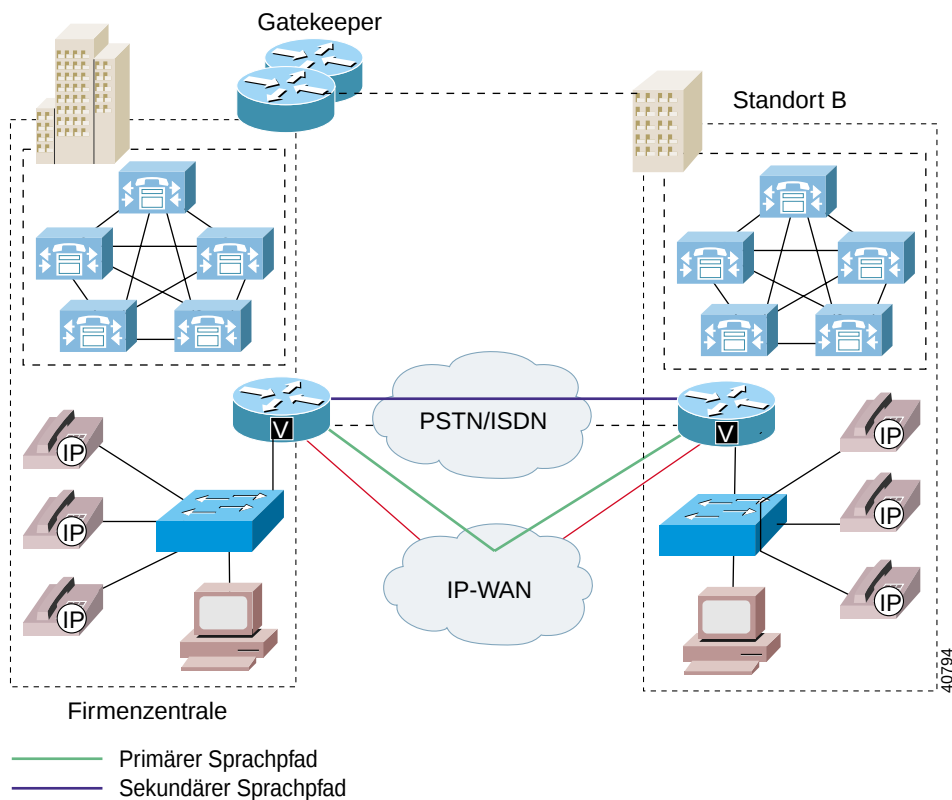
Dieser Abschnitt befasst sich mit der Architektur und den funktionalen Komponenten des Wählplans. Da es mehrere Möglichkeiten gibt, einen Wählplan zu konfigurieren, werden auch die empfohlenen Konfigurationen beschrieben.

Zu den Anforderungen an einen Wählplan können beispielsweise die Unterstützung von Kurzwahlnummern, wie vier- oder fünfstellige Durchwahlen, gehören, oder redundante Pfade, die für den Anrufer sichtbar sind. Der Wählplan im Cisco CallManager Version 3.0 wurde verbessert und ermöglicht eine noch höhere Skalierbarkeit und Flexibilität sowie eine einfachere Bedienung. Gleichzeitig können durch die bessere Integration von Cisco CallManagern und Cisco IOS-Gateways größere Netzwerke aufgebaut werden.

Die Architektur des Cisco CallManager Wählplans ist für zwei allgemeine Anruftypen eingerichtet:

- Interne Anrufe bei Cisco IP-Telefonen, die beim Cisco CallManager-Cluster angemeldet sind.
- Externe Anrufe über ein PSTN/ISDN-Gateway oder bei einem anderen Cisco CallManager-Cluster über das IP-WAN.

Abbildung 5-1 zeigt ein Netzwerk, über das diese beiden Anruftypen abgewickelt werden können. Bei einem gut strukturierten Wählplan verwenden Sprachanrufe vorzugsweise das IP-WAN und werden nur über das PSTN/ISDN-Gateway geleitet, wenn das IP-WAN heruntergefahren oder nicht verfügbar ist. Dieses Routing ist für den Benutzer sichtbar.

Abbildung 5-1 Ziel eines gut strukturierten Wählplans


Der Wählplan für interne Anrufe bei IP-Telefonen, die bei einem Cisco CallManager-Cluster angemeldet sind, ist relativ einfach. Bei der Anfangskonfiguration wird dem IP-Telefon eine Directory Number (DN) zugewiesen, die für dieses Telefon an jedem beliebigen Ort gültig ist. Wenn sich das IP-Telefon beim Cisco CallManager-Cluster anmeldet, wird der Cisco CallManager-Cluster dynamisch mit der neuen IP-Adresse aktualisiert. Die Directory Number bleibt jedoch die gleiche. Die interne Wähllänge (Anzahl der gewählten Ziffern) für interne Anrufe ist konfigurierbar.



Hinweis IP-Telefone sind nicht die einzigen Geräte, die hierfür geeignet sind. Es können sich auch andere Geräte beim Cisco CallManager anmelden und eine Directory Number erhalten, z. B. Cisco IP SoftPhones, analoge Telefone sowie Faxgeräte, die an Gateways angeschlossen sind, welche MGCP oder das Skinny Gateway Protocol verwenden.

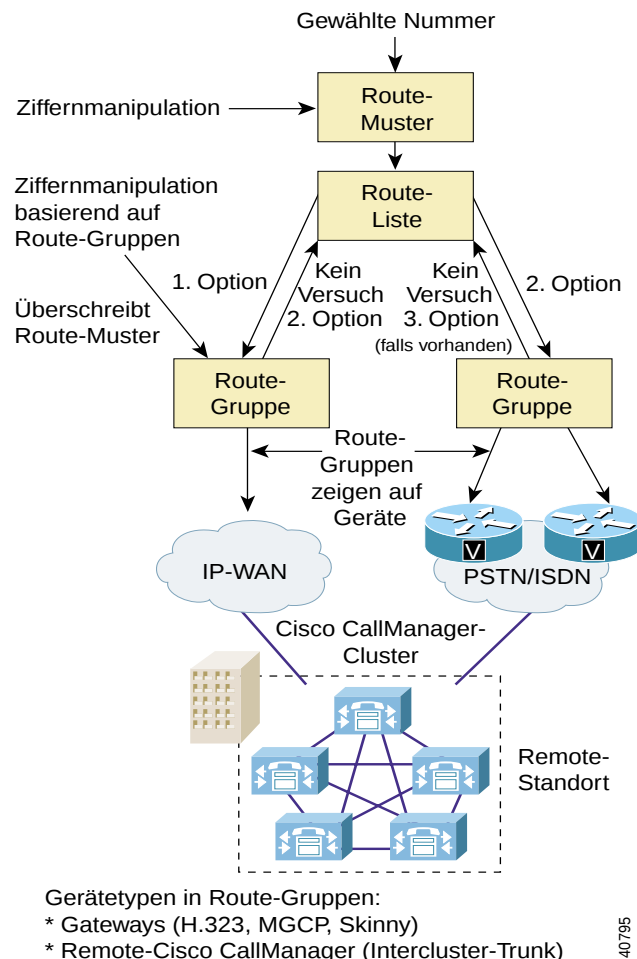
Wenn Sie den Cisco CallManager für externe Anrufe konfigurieren möchten, benötigen Sie ein Route-Muster. In den meisten Fällen wird das Route-Muster dazu verwendet, Anrufe an ein PSTN/ISDN-Gateway weiterzuleiten, es kann jedoch auch für IP-WAN-Anrufe bei einem Remote-Cisco CallManager verwendet werden. Die Architektur des Wählplans im Cisco CallManager Version 3.0 ist ein dreistufiger Entscheidungsbaum, der mehrere Routen für eine gewählte Rufnummer sowie die Ziffernmanipulation basierend auf den

Netzwerkanforderungen zulässt. Bei der Ziffernmanipulation werden der ursprünglich gewählten Rufnummer Ziffern hinzugefügt bzw. Ziffern weggelassen, um Wählgewohnheiten des Benutzers oder Gateway-Anforderungen Rechnung zu tragen. Sie können auch Funktionen wie Trunk-Gruppen für Gateway-Redundanz und eine Form des preisgünstigsten Routens (Least Cost Routings) konfigurieren.

Bei der Auswahl einer alternativen Route wird als Pfad zu einer bestimmten gewählten Rufnummer als erste Option das IP-WAN und als zweite Option das PSTN/ISDN-Gateway verwendet, falls das IP-WAN heruntergefahren ist oder nicht genügend Ressourcen besitzt. Die Wählplankriterien für die Verwendung einer alternativen Route könnten auf einem Hinweis der Anrufzugangskontrolle basieren, wonach ein Gateway nicht genügend Trunks besitzt. Das bedeutet, dass das IP-WAN den Anruf nicht entgegennehmen kann.

Abbildung 5-2 zeigt die Architektur des Wählplans im Cisco CallManager Version 3.0, der die Auswahl alternativer Routen unterstützt. Die Elemente in dieser Architektur werden in den folgenden Abschnitten genauer beschrieben.

Abbildung 5-2 Architektur des Cisco CallManager-Wählplans



40795

Route-Muster

Das Route-Muster identifiziert eine gewählte Rufnummer und verwendet die zu Grunde liegenden Konfigurationen für Route-Liste und Route-Gruppe, um zu bestimmen, wie der Anruf geroutet wird. Ein Route-Muster kann als Nummer oder als Nummernbereich (häufiger) eingegeben werden. Wenn ein Route-Muster für einen Nummernbereich eingegeben wird, kann dadurch die Anzahl der erforderlichen Einträge reduziert werden.

Wenn ein Route-Muster einer gewählten Rufnummer entspricht, wird der Anruf an die Route-Liste weitergegeben, die diesem Route-Muster zugewiesen ist. Bevor der Anruf an die Route-Liste weitergegeben wird, kann eine Ziffernmanipulation erfolgen, falls Ziffern dem zugehörigen Route-Muster hinzugefügt bzw. Ziffern weggelassen werden müssen. Die Route-Liste entscheidet anschließend basierend auf der festgelegten Priorität, welche nachgeschalteten Route-Gruppen (Trunk-Gruppen) den Anruf erhalten sollen.

**Hinweis**

Die Ziffernmanipulation erfolgt im Route-Muster nur für ausgehende Anrufe, bevor sie an die Route-Liste und Route-Gruppen gesendet werden. Für die einzelnen nachgeschalteten Route-Gruppen können für dasselbe Route-Muster individuelle Ziffermanipulationen festgelegt werden. Dies ist besonders hilfreich, wenn verschiedene Routen zu einer bestimmten Rufnummer verschiedene Ziffernmanipulationen benötigen. Beispielsweise kann es notwendig sein, dass Benutzer sieben Ziffern wählen müssen, um einen Remote-Standort zu erreichen, der einen internen vierstelligen Wählplan besitzt. Bei Verwendung des IP-WANs müssten die ersten drei Ziffern weggelassen werden, damit die letzten vier Ziffern in der ursprünglichen Länge der internen Wählfolge an den Remote-Cisco CallManager übermittelt werden können. Falls das IP-WAN heruntergefahren ist oder keine weiteren Sprachanrufe akzeptieren kann, muss den sieben Ziffern die Vorwahl vorangestellt werden, damit der angerufene Teilnehmer über PSTN/ISDN erreicht wird. Ein Route-Muster ist nur einer Route-Liste zugeordnet.

Route-Liste

Eine Route-Liste definiert den Weg eines Anrufs. Route-Listen werden so konfiguriert, dass sie auf eine oder mehrere Route-Gruppen zeigen, die effektiv als Trunk-Gruppen fungieren. Die Route-Liste sendet einen Anruf nach der konfigurierten Präferenz an eine Route-Gruppe. Beispiel: Bei der primären Route-Gruppe sind die Kosten für Anrufe niedriger, die sekundäre Route-Gruppe wird nur dann verwendet, wenn die primäre nicht verfügbar ist, weil alle Trunks besetzt sind oder die IP-WAN-Ressourcen nicht ausreichen.

Route-Gruppe

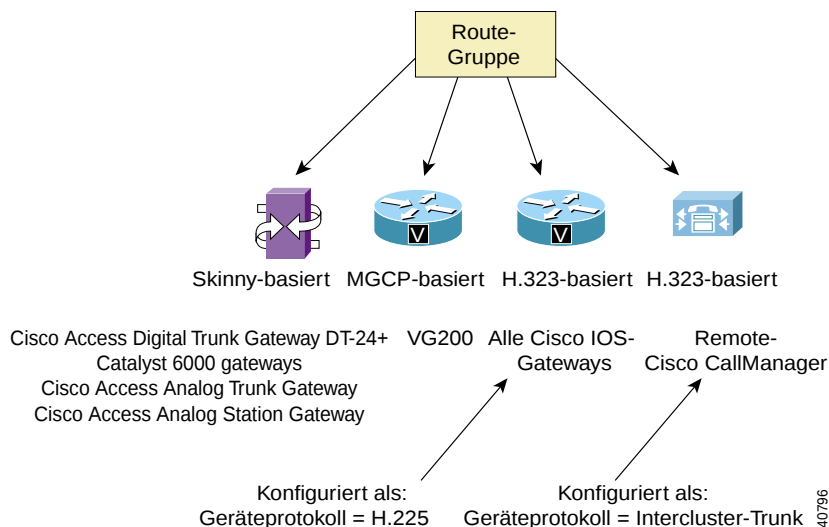
Route-Gruppen steuern bestimmte Geräte, wie beispielsweise Gateways. Gateways können auf dem Skinny Gateway Protocol, auf MGCP oder H.323 basieren. Endpunkte wie NetMeeting-Clients oder Remote-Cisco CallManager im IP-WAN werden als H.323-Gateways konfiguriert. Die Route-Gruppe zeigt auf eines oder mehrere Geräte und wählt die Geräte für das Anruf-Routing nach Präferenz aus. Die Route-Gruppe kann alle Anrufe an das primäre Gerät leiten und die sekundären Geräte verwenden, falls das primäre nicht verfügbar ist. Diese Gruppe fungiert effektiv als Trunk-Gruppe.

Es können eine oder mehrere Route-Listen auf dieselbe Route-Gruppe zeigen. Alle Geräte in einer bestimmten Route-Gruppe weisen dieselben Eigenschaften wie Pfad und Ziffernmanipulation auf. Route-Gruppen können die Ziffernmanipulation durchführen und die Ziffernmanipulation von Route-Mustern überschreiben (siehe "Route-Muster" auf Seite 5-4).

Geräte

Alle IP-Endpunkte gelten als Geräte, es können jedoch nur bestimmte Geräte in eine Route-Gruppe aufgenommen werden. Abbildung 5-3 zeigt die Gerätearten, die sich in einer Route-Gruppe befinden können.

Abbildung 5-3 Gerätearten, auf die Route-Gruppen zeigen



Folgende Hinweise gelten für die Geräte in Abbildung 5-3:

- Ein H.323-Gateway kann so konfiguriert werden, dass es vom Gatekeeper gesteuert wird. Das bedeutet, bevor ein Anruf an ein H.323-Gerät weitergeleitet wird, muss eine erfolgreiche Gatekeeper-Abfrage durchgeführt werden. Nur H.323-Geräte, die Remote-Cisco CallManager sind, sollten vom Gatekeeper gesteuert werden.

- Um den Codec zu bestimmen, der von Anrufen beim Gerät verwendet werden soll, platzieren Sie das Gerät in einer Region, die den gewünschten Codec verwendet.
- H.323-Gateways können von mehreren Clustern für eingehende und ausgehende Anrufe gemeinsam genutzt werden, während Gateways, die auf MGCP oder dem Skinny Gateway Protocol basieren, für nur einen Cisco CallManager-Cluster vorgesehen sind.

Ein wichtiges Merkmal der Wählstruktur eines Route-Musters ist, dass sie in der Regel verwendet wird, wenn Anrufe von IP-Telefonen an Gateways oder Remote-Cisco CallManager geleitet werden sollen, die H.323 verwenden. In diesen Fällen können alternative Routen verwendet werden, falls der primäre Pfad zu einem Ziel nicht verfügbar ist. Dieses Schema wird in Kapitel 6, "Multisite-WAN mit verteilter Anrufverarbeitung", beschrieben. Alle internen Anrufe an einem Standort verwenden das IP-WAN als primären Pfad und das PSTN/ISDN-Gateway als sekundären Pfad.

Anrufe zwischen IP-Telefonen eines Cisco CallManagers oder Cisco CallManager-Clusters verwenden nicht die Wählstruktur des Route-Musters und können daher auch keine alternativen Routen verwenden, wenn keine Konnektivität gegeben ist. Wenn die IP-Konnektivität zwischen zwei IP-Telefonen nicht mehr besteht, liegt dies mit hoher Wahrscheinlichkeit daran, dass für eines der Telefone keine Konnektivität mehr mit seinem Cisco CallManager besteht. Dies kann beispielsweise passieren, wenn für Multisite-WANs die zentrale Anrufverarbeitung verwendet wird. In diesen Fällen gibt es keine alternative Routen zwischen den Standorten.

Ziffernübersetzungstabellen

Der Cisco CallManager unterstützt die Ziffernübersetzung. Damit wird die Möglichkeit bezeichnet, die angerufene oder anrufende Nummer in andere Nummern umzuwandeln oder die Anzahl der Ziffern zu ändern. Die Ziffernübersetzung kann sowohl für interne als auch für externe und für eingehende und ausgehende Anrufe angewendet werden.

Die Übersetzungstabelle kommt häufig zum Einsatz, um nicht zugewiesene Nummern des Direct Inward Dialing (DID) an einen bestimmten Teilnehmer weiterzuleiten, wenn solche Nummern gewählt werden. Angenommen, Sie haben einen DID-Bereich von 1000 bis 1999 und möchten festlegen, dass alle Anrufe bei nicht zugewiesenen DID-Nummern an die Durchwahl 1111 weitergeleitet werden. Für diesen Fall können Sie eine Übersetzungstabelle mit 1XXX konfigurieren, die auf eine Übersetzungsmaske 1111 zeigt:

Übersetzungstabelle	Übersetzungsmaske
1XXX	1111

In diesem Beispiel verwendet der Cisco CallManager Platzhalter, um nach der längsten Entsprechung zu suchen. Wenn ein IP-Telefon mit einer übereinstimmenden Directory Number im Bereich 1000-1999 existiert, sendet der Cisco CallManager den Anruf an dieses Telefon. Wenn keine entsprechende IP-Rufnummer im Bereich 1000-1999 existiert, gibt es eine Übereinstimmung in der 1XXX-Übersetzungstabelle, und der Anruf wird an die Durchwahl 1111 weitergeleitet.

Die Ziffernübersetzung kann in der Struktur des Route-Musters auch mit der Anrufer-/Empfängerumwandlung durchgeführt werden. Damit wird die Ziffernübersetzung auf eingehende und ausgehende Anrufe angewendet. Das bedeutet, dass in einem Route-Muster drei Arten der Ziffernmanipulation für eine angerufene Rufnummer möglich sind:

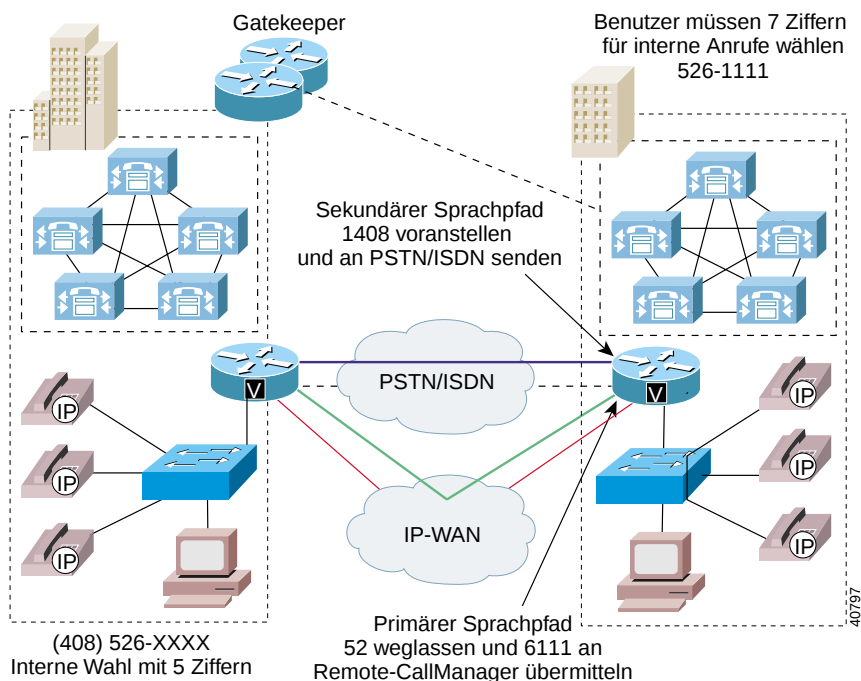
- Weglassen von Ziffern
- Anwenden der Empfänger-Umwandlungsmaske
- Voranstellen von Ziffern

Beachten Sie, dass die Anrufer-Umwandlungsmaske nur für anrufende Nummern und die anderen Masken für angerufene Nummern angewendet werden können. Der Cisco CallManager entfernt zunächst Ziffern, wendet anschließend die Umwandlungsmaske an und stellt schließlich Ziffern voran.

On-Net-Route-Muster

Abbildung 5-4 zeigt On-Net-Anrufe im IP-WAN, wobei PSTN/ISDN als Backup dient. Für jeden Pfad ist eine andere Ziffernmanipulation erforderlich.

Abbildung 5-4 Anrufe im IP-WAN mit unterschiedlicher Ziffernmanipulation pro Pfad



Ausgehende Anrufe über PSTN/ISDN

Wenn Sie den Timer für die Ziffernwahl in den Cisco CallManager-Dienstparametern herabsetzen (beispielsweise auf 3 Sekunden), kann ein Anruf bereits vor Ablauf der 10 Sekunden gesendet werden. Das Risiko besteht allerdings darin, dass der Cisco CallManager den Wählvorgang unter Umständen vorzeitig für beendet hält, wenn der Benutzer während des Wählvorgangs eine Pause macht.

Option 2: Route-Muster = 0.#!#

- 0. Entspricht dem lokalen PSTN/ISDN-Zugriffscode.
- ! Steht für eine beliebige Ziffer und eine beliebige Anzahl an Ziffern. Dieses Zeichen bedeutet auch, dass der Cisco CallManager den Wählvorgang erst als beendet betrachtet, wenn 10 Sekunden (Standard) lang keine Ziffer empfangen wurde. Der Anruf wird dann gesendet.
- # Gibt an, dass der Cisco CallManager den Wählvorgang als beendet betrachtet und den Anruf sofort sendet, wenn das Nummernzeichen (#) gedrückt wird.

Bei dieser Option wird der Benutzer aufgefordert, die #-Taste zu drücken, um die Wählfolge zu beenden und den Anruf sofort zu tätigen. Diese Vorgehensweise ist etwas gewöhnungsbedürftig und entspricht nicht dem herkömmlichen Wählverhalten der Benutzer. Sie ist allerdings vergleichbar mit der Bestätigungstaste auf Mobiltelefonen.

Konfigurieren von Gruppen und Anrufeinschränkungen für den Wählplan

Eine neue Funktion im Cisco CallManager Version 3.0 ermöglicht es, Anrufeinschränkungen für jedes Telefon festzulegen und zusammengehörige Wählplangruppen im selben Cisco CallManager zu erstellen. Benutzer im selben Cisco CallManager können zu Interessengruppen mit identischen Anrufeinschränkungen und Wählplänen zusammengeschlossen werden. Die verschiedenen Interessengruppen können unabhängig handeln, verwenden jedoch dieselben Gateways und überlappende Wählpläne. Für diese neuen Funktionen, die besonders für Multisite-IP-WANs mit zentraler Anrufverarbeitung interessant sind, benötigen Sie Partitionen und Anrufauswahlzonen.

Partitionen

Eine Partition ist eine Gruppe von Geräten mit ähnlichen Erreichbarkeitsmerkmalen. IP-Telefone, Directory Numbers und Route-Muster können einer Partition zugewiesen werden. Die Partitionsnamen sollten so gewählt werden, dass sie eindeutig der zugehörigen Benutzergruppe zugeordnet werden können. Für Benutzer, die im Gebäude D in San Jose arbeiten, können Sie beispielsweise eine Partition mit der Bezeichnung SJ-D erstellen.

Anrufauswahlzone

Eine Anrufauswahlzone ist eine Liste mit den Partitionen, die ein Benutzer durchsuchen kann, bevor er einen Anruf tätigen darf. Anrufauswahlzonen sind Geräten zugeordnet, die Anrufe tätigen können. Dazu gehören IP-Telefone, Cisco SoftPhones und Gateways.

Anrufeinschränkungen können leicht umgesetzt werden, da Benutzer nur die Partitionen in der Anrufauswahlzone anrufen können, denen sie zugewiesen sind. Wenn eine Directory Number außerhalb der Partition gewählt wird, ertönt ein Besetztzeichen.

Sie können Partitionen und Anrufauswahlzonen mit Routern und Zugriffskontrollliste (Access Control Lists (ACLs)) vergleichen. Stellen Sie sich eine Partition als ein IP-Subnetz vor, dem die Benutzer zugeordnet werden. Eine Anrufauswahlzone ist vergleichbar mit einer ACL für eingehenden Verkehr, mit der festgelegt wird, welches Subnetz Sie erreichen können.

Abbildung 5-5 veranschaulicht die Parallelen zwischen Partitionen und Anrufauswahlzonen und ACLs.

Abbildung 5-5 Gemeinsamkeiten von Partitionen/Anrufauswahlzonen und Subnetzen/ACLs

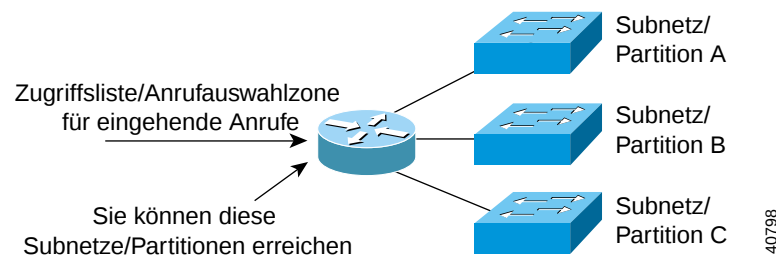
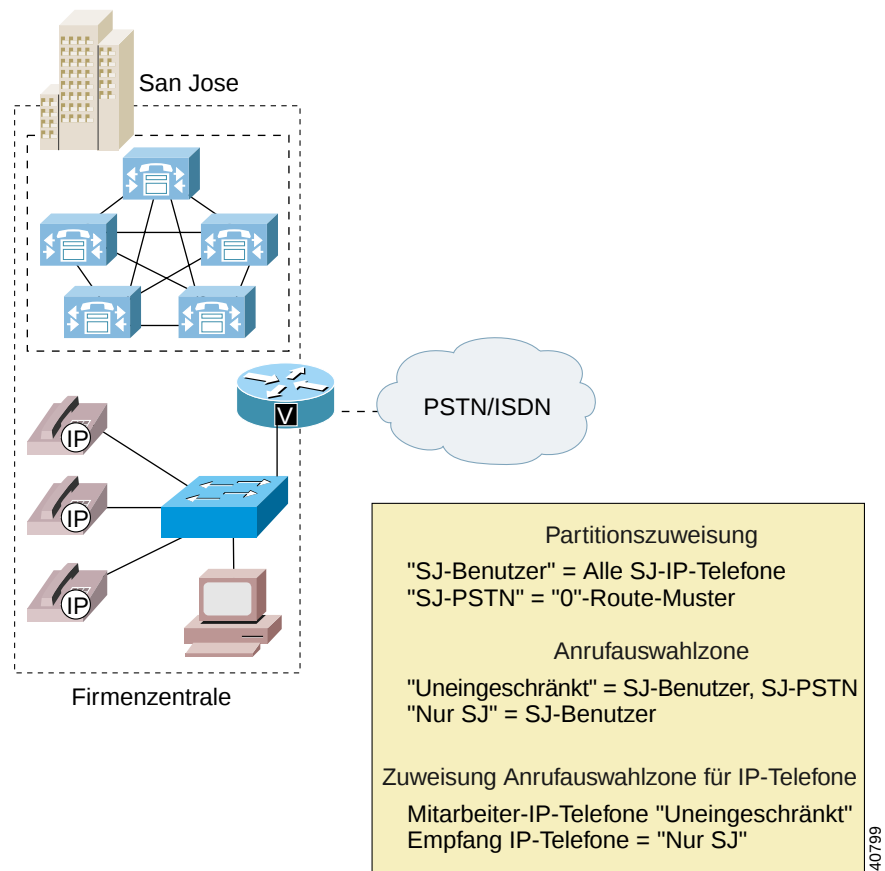


Abbildung 5-6 zeigt ein einfaches Beispiel, wie Partitionen und Anrufauswahlzonen zum Festlegen von Anrufeinschränkungen verwendet werden können.

Abbildung 5-6 Verwendung von Partitionen und Anrufauswahlzonen für Anrufeinschränkungen



Mitarbeiter: Beliebige Nummer kann gewählt werden
 Telefone Empfang: Nur interne Benutzer können gewählt werden

In Abbildung 5-6 können Mitarbeiter jede beliebige Nummer wählen. Mit den Telefonen im Empfangsbereich können dagegen nur Nummern am lokalen Standort angerufen werden. Alle IP-Telefone befinden sich in der Partition "SJ-Benutzer", und das Route-Muster 9 für PSTN/ISDN ist "SJ-PSTN/ISDN" zugewiesen. Es werden zwei Anrufauswahlzonen mit verschiedenen Wählmerkmalen erstellt. Zum einen die Anrufauswahlzone "Uneingeschränkt", die sowohl die Partition "SJ-Benutzer" als auch die Partition "SJ-PSTN/ISDN" enthält. Zum anderen die Anrufauswahlzone "Nur SJ", die nur die "SJ-Benutzer" enthält. Die IP-Telefone der Mitarbeiter in San Jose werden der Anrufauswahlzone "Uneingeschränkt" zugeordnet, d. h. sie können jede beliebige Nummer wählen. Die Telefone im Empfangsbereich werden der Anrufauswahlzone "Nur SJ" zugewiesen, d. h. sie können nur Telefone am lokalen Standort anwählen.

Eine Übersicht über die Zuweisung der Partitionen und Anrufauswahlzonen für das beschriebene Beispiel finden Sie in Tabelle 5-1 und Tabelle 5-2. Zwei Partitionen definieren die

Erreichbarkeitsmerkmale für den angegebenen Standort, eine für interne Benutzer am lokalen Standort und eine für externe Anrufe. Geräte und Route-Muster werden diesen Partitionen zugewiesen.

Tabelle 5-1 Partitionszuweisung

Partitionsname	Zugewiesene Geräte
SJ-Benutzer	Alle IP-Telefone am Standort San Jose
SJ Extern	Alle Route-Muster mit externem Ziel (lokales PSTN/ISDN-Gateway)

Tabelle 5-2 Zuweisung der Anrufauswahlzonen

Anrufauswahlzone	Partitionen	Zugewiesen
Uneingeschränkt	SJ-Benutzer SJ Extern	Geräte, mit denen interne und externe Anrufe möglich sind
Nur SJ	SJ-Benutzer	Geräte, mit denen nur interne Anrufe möglich sind

Dieses Beispiel ist vielleicht die einfachste Konfiguration im Hinblick auf die Anforderungen der lokalen Anrufverarbeitung bei Multisite-WANs. Bei einem aufwendigeren Wählplan ist es eventuell notwendig, zusätzlich folgende Aspekte zu berücksichtigen:

- Nur interne Anrufe
- Nur interne Anrufe und Notrufe
- Nur interne Anrufe und Anrufe innerhalb des Standorts
- Nur interne Anrufe und Anrufe innerhalb des Standorts sowie Notrufe
- Nur interne Anrufe und Anrufe innerhalb des Standorts sowie Notrufe und lokale PSTN/ISDN-Anrufe
- Nur interne Anrufe und Anrufe innerhalb des Standorts sowie Notrufe und nationale PSTN/ISDN-Ferngespräche
- Uneingeschränkte Anrufe einschließlich internationalen Rufnummern

Partitionen und Anrufauswahlzonen lassen unabhängige Wählbereiche für jede einzelne Partition zu. Das bedeutet, dass Durchwahlnummern und Zugriffscodes in verschiedenen Partitionen überlappende Nummern aufweisen und dennoch unabhängig sein können. Dieses Prinzip wird am häufigsten in einer zentralen

Anrufverarbeitung angewendet, bei der alle Standorte und Benutzer denselben Cisco CallManager verwenden. Aber jeder Standort kann eine 9 für den lokalen PSTN/ISDN-Zugriff wählen. Diese Funktion ist neu im Cisco CallManager Version 3.0. In vorherigen Versionen war für jeden entfernten Standort ein eindeutiger PSTN/ISDN-Zugriffscod erforderlich.

Folgende Bedingungen gelten, wenn sich Benutzer und Durchwahlnummern an verschiedenen Standorten überlappen und die Anrufverarbeitung zentral erfolgt:

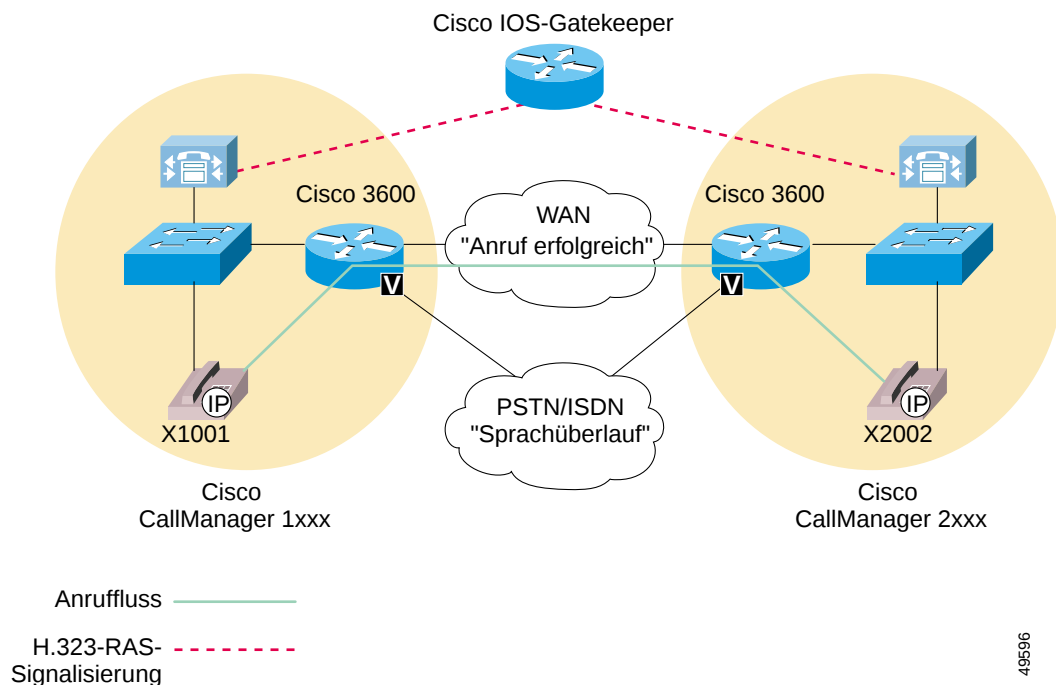
- Überlappende interne Wählpläne an verschiedenen Standorten werden nur unterstützt, wenn keine Voicemail benötigt wird. Wenn der Cisco CallManager einen Anruf an eine Voicemail sendet, kann er nicht feststellen, für welche Partition (und welchen Voicemail-Benutzer) der Anruf bestimmt ist. Benutzer 1111 am Standort kann beispielsweise nicht von Benutzer 1111 am Standort B unterschieden werden, wenn der Anruf an eine Voicemail gesendet wird. Voicemail-Benutzer benötigen eindeutige IDs.
- Wenn keine Voicemail erforderlich ist, können Benutzer mit derselben Durchwahl an verschiedenen Standorten folgendermaßen erreicht werden:
 - PSTN/ISDN – Durch Wählen des lokalen Zugriffscodes gefolgt von der gültigen Directory Number.
 - IP-WAN – Durch Verwendung von Übersetzungstabellen. Damit kann identischen Nummern ein eindeutiger Code vorangestellt werden, der entfernt wird, wenn der Anruf an die Zielpartition übergeben wird.

Die Rolle eines Gatekeepers

In einer Umgebung mit verteilter Anrufverarbeitung können Sie einen Gatekeeper verwenden, um die Anrufzugangskontrolle über das WAN vorzunehmen. Mit der Einführung des Cisco CallManagers Version 3.0(5) können Sie einen Gatekeeper auch dazu verwenden, Wählpläne zwischen Cisco CallManagern zu vereinfachen.

Angenommen, zwei Cisco CallManager-Server sind über ein WAN miteinander verbunden. Ein Cisco CallManager besitzt den Durchwahlbereich 1XXX, der andere den Durchwahlbereich 2XXX. Beide melden sich zum Zweck der Anrufzugangskontrolle bei einem Gatekeeper an. Jeder Cisco CallManager hat einen entsprechenden Eintrag in der Route-Muster-Konfiguration des Wählplans, der die Funktion Anonymous Calls Device verwendet, um dem Gatekeeper den Durchwahlbereich des anderen Cisco CallManagers mitzuteilen. In der Praxis bedeutet das, wenn Subscriber 1001 Subscriber 2002 anwählt, sendet der Cisco CallManager 1XXX den Wert 2002 zur Adressauflösung an den Gatekeeper. Der Gatekeeper sendet wiederum die IP-Adresse des Cisco CallManagers 2XXX an den Cisco CallManager 1XXX, um die IP-Adresse für 2002 festzustellen. Wenn die Kriterien der Anrufzulassung erfüllt sind, wird der Anruf vom Gatekeeper ermöglicht. Abbildung 5-7 veranschaulicht dieses Beispiel.

Abbildung 5-7 Verwendung eines Gatekeepers zur Anrufzugangskontrolle



Wenn das WAN in diesem Szenario nicht verfügbar ist, kann der Anruf nicht durchgehen. Es ist kein automatisches Fallback möglich, denn wenn der Cisco CallManager 1XXX einmal darüber informiert ist, dass der Anruf nicht möglich ist, gibt es keinen weiteren Mechanismus für eine intelligente Ziffernmanipulation. (Beispiel: Der Cisco CallManager kann nicht erkennen, welche Vorwahl an die ursprünglich gewählten Ziffern angehängt werden muss.) Zu diesem Zeitpunkt muss der sendende Subscriber versuchen, den Anruf über eine alternative Route, etwa ein PSTN/ISDN-Gateway, zu tätigen.



Multisite-WAN mit verteilter Anrufverarbeitung

In diesem Kapitel erhalten Sie Richtlinien für den Entwurf von Multisite-WAN-Systemen, die ihre Anrufverarbeitung über Cisco CallManager abwickeln. In diesem Zusammenhang werden mit besonderer Aufmerksamkeit Themen erörtert, die für das verteilte Anrufverarbeitungsmodell spezifisch sind, wobei auch auf relevantes Material aus anderen Abschnitten dieses Handbuchs Bezug genommen wird.

Verteiltes Anrufverarbeitungsmodell

In einem verteilten Anrufverarbeitungssystem (siehe Abbildung 6-1) verfügt jeder Standort über seinen eigenen Cisco CallManager sowie seine eigenen Ressourcen für Voice Messaging und Digital Signal Processors (DSPs).

Der größte Vorteil dieses Nutzungsmodells besteht darin, dass er durch die Verwendung der lokalen Anrufverarbeitung unabhängig davon, ob das IP-WAN verfügbar ist, immer dieselben Funktionen und Fähigkeiten bieten kann. Jeder Standort kann je nach der Anzahl der Benutzer bis zu acht

Cisco CallManager-Server im Cluster haben. Dies ist das vorwiegend genutzte Modell für Standorte mit mehr als 50 Benutzern, wobei jeder Standort bis zu 10.000 Benutzer unterstützen kann. Außerdem muss nicht auf Dienste verzichtet werden, wenn das IP-WAN außer Betrieb ist.

Anrufzugangskontrolle

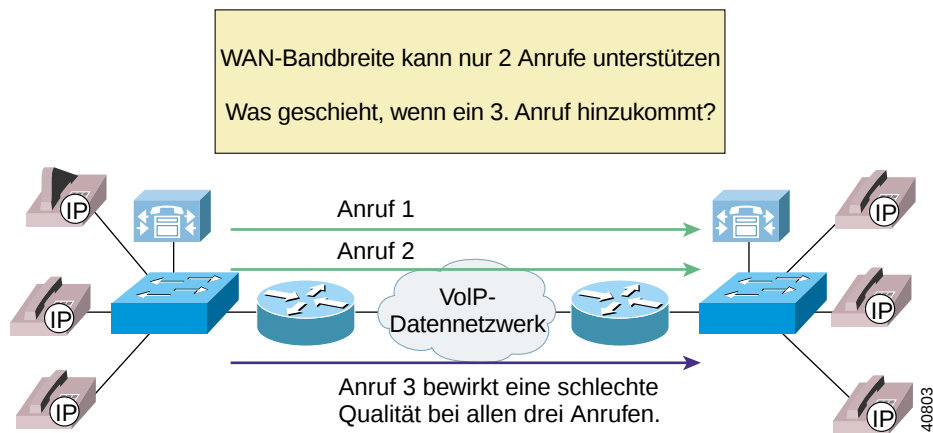
Die Anrufszugangskontrolle ist ein Mechanismus, durch den einem neuen Anruf Quality of Service (Dienstqualität) gewährt wird, während auch bestehenden Anrufen weiterhin Quality of Service geboten wird. Dies wird erreicht, indem die Verfügbarkeit von Netzwerkressourcen auf Call-by-Call-Basis sichergestellt wird, bevor der neue Anruf aufgebaut wird.

In einem konvergenten Netzwerkparadigma werden alle Verkehrstypen (Sprache, Bilder und Daten) über eine gemeinsame IP-fähige Infrastruktur übertragen. Aufgrund dieser Mischung aller Verkehrstypen muss das Netzwerk in der Lage sein, die Anforderungen jedes einzelnen Verkehrstyps in Bezug auf Paketverluste, Latenzzeiten und Jitter zu erfüllen. In einer solchen Umgebung gewinnen zwei Hauptaufgaben an Wichtigkeit:

- Das Setzen von Prioritäten für einen Verkehrstyp über den anderen
- Der Schutz des Echtzeitverkehrs, wie z. B. Sprache oder Bilder, vor einer Überlastung der Bandbreite des Netzwerks

Die erste Aufgabe wird durch Quality of Service (QoS) erreicht; nähere Informationen hierzu finden Sie in Kapitel 8, "Quality of Service"..

Die zweite Aufgabe wird durch Anrufzugangskontrollmechanismen ausgeführt. Der Bedarf an einer Anrufzugangskontrolle in der IP-Telefonie wird bedeutend durch die Tatsache erhöht, dass alle IP-Telefone über einen offenen Pfad zum WAN verfügen, während Toll Bypass-Netzwerke die Anzahl der physischen Trunk-Leitungen begrenzen können, die die Möglichkeit eines Verbindungsaufbaus über das WAN bieten. In Abbildung 6-2 wird dargestellt, warum eine Anrufzugangskontrolle benötigt wird.

Abbildung 6-2 Gründe für die Notwendigkeit einer Anrufzugangskontrolle

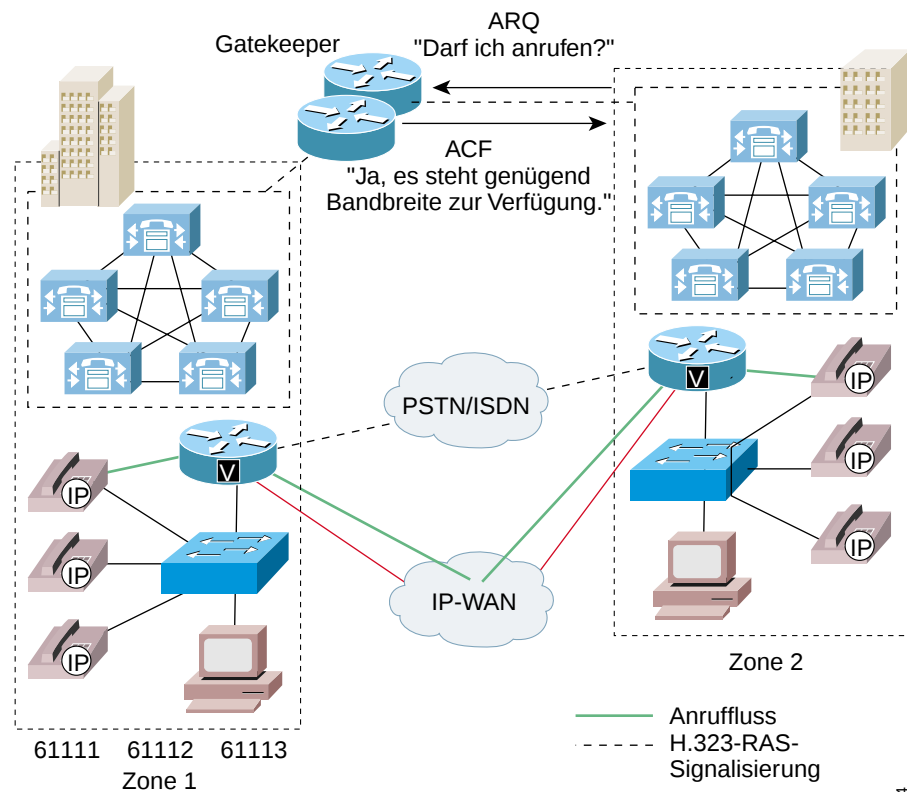
Für verteilte Anrufverarbeitungssysteme können Sie eine Anrufzugangskontrolle mit einem H.323-Gatekeeper implementieren. Bei diesem Entwurf wird Cisco CallManager beim Cisco IOS-Gatekeeper, der auch als Multimedia Conference Manager (MCM) bekannt ist, als ein Voice-over-IP (VoIP)-Gateway registriert und sendet jedes Mal eine Anfrage an ihn, wenn ein IP-WAN-Anruf erfolgen soll. Der Cisco IOS-Gatekeeper verbindet jeden Cisco CallManager mit einer Zone, die spezifische Bandbreitenbegrenzungen hat. So kann der Cisco IOS-Gatekeeper die Höchstgrenze der Bandbreitennutzung durch Sprachanrufe über das IP-WAN in eine Zone oder aus ihr heraus festsetzen.

Wenn Cisco CallManager einen IP-WAN-Anruf ausführen möchte, fordert er zunächst eine Berechtigung vom Gatekeeper an. Wenn der Gatekeeper die Berechtigung erteilt, wird der Anruf über das IP-WAN getätigt. Wenn der Gatekeeper diese Anfrage ablehnt, tätigt Cisco CallManager den Anruf über den sekundären Pfad, also über PSTN/ISDN.

Dies ist also eigentlich eine Anruf-Accounting-Methode, mit der eine Anrufzugangskontrolle gewährleistet wird, bei der über den Gatekeeper einfach verfolgt wird, wieviel Bandbreite die IP-WAN-Anrufe in Anspruch nehmen. Bei der maximalen Bandbreiteneinstellung für eine Zone sollte beachtet werden, dass Sprachanrufe nicht mehr als 75 % der WAN-Verbindung in Anspruch nehmen sollten. In Abbildung 6-3 wird der Vorgang dargestellt, der bei diesem Anrufzugangskontrollmechanismus verwendet wird.

**Hinweis**

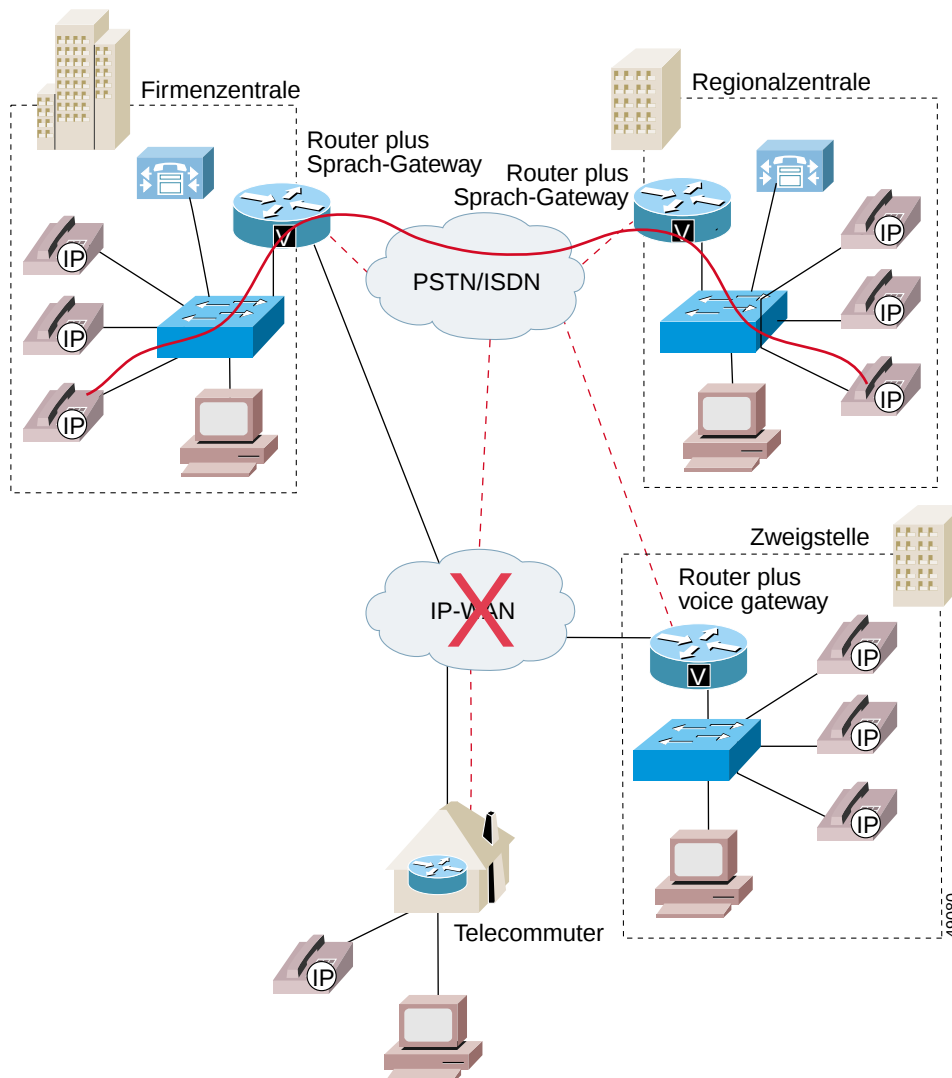
In diesem Schema sind IP-Telefone nicht mobil über mehrere Standorte einsetzbar. Sollte ein IP-Telefon sich über das WAN registrieren, könnte die Anrufzugangskontrolle nicht bestimmungsgemäß funktionieren.

Abbildung 6-3 Anrufzugangskontrolle mithilfe eines Gatekeepers


40804

In WAN-Nutzungsmodellen mit mehreren Standorten ist eine dynamische Anrufweiterleitung das Ziel, über die Sprachanrufe zwischen den Standorten das IP-WAN als primären Pfad und PSTN/ISDN als sekundären Pfad verwenden können, wenn das IP-WAN außer Betrieb ist oder nicht über genügend Ressourcen für die Abwicklung zusätzlicher Anrufe verfügt. In Abbildung 6-4 wird diese Art der dynamischen Anrufweiterleitung dargestellt.

Abbildung 6-4 Dynamische Weiterleitung von Anrufen von Standort zu Standort



In diesem Modell ist es wichtig, dass festgestellt werden kann, wenn das IP-WAN außer Betrieb ist oder nicht über genügend Ressourcen zur Abwicklung zusätzlicher Anrufe verfügt, damit die Anrufe nur bei Bedarf über PSTN/ISDN geleitet werden können. Dieser Typ der dynamischen Weiterleitung reduziert die Anrufrkosten, was der Vorteil der Anrufzugangskontrolle für diese Lösung ist. In diesem Fall ist der Wählplan eng mit dem Anrufzugangskontrollmechanismus über einen Gatekeeper verbunden, weil letztendlich über den Wählplan entschieden wird, wann ein Anruf über das IP-WAN getätigt wird und wie vorgegangen werden soll, wenn der Gatekeeper den Anruf abweist.

Wie bereits erwähnt, können Sie für die Anrufzugangskontrolle einen H.323-Gatekeeper zur Begrenzung der Anzahl von Anrufen verwenden, die in eine Zone oder aus einer Zone heraus zulässig sind. Dadurch wird die Bandbreitenverfügbarkeit pro Standort begrenzt, da jeder Standort mit

einer bestimmten Zone verknüpft werden kann. Dieses Modell verwendet Cisco CallManager mit einem Gatekeeper zur Durchführung der Anrufzugangskontrolle in Hub-and-Spoke-Topologien.

Zusätzlich zur Anrufzugangskontrolle ist die Adressauflösung eine zweite wichtige Funktion, die vom Gatekeeper übernommen wird. An jedem beliebigen Standort weiß der Cisco CallManager, welche Durchwahlen er kontrolliert, und kann daher Anrufe an diese Durchwahlen weiterleiten. Durchwahlen außerhalb dieses festgelegten Bereichs kann der Cisco CallManager an einen Gatekeeper weitergeben, der die IP-Adresse eines anderen Cisco CallManagers zurückgibt, an den der Anruf weitergeleitet werden sollte. Dies ist möglich, da sich jeder Cisco CallManager (bzw. jeweils ein Cisco CallManager aus einem Cluster) beim Gatekeeper registriert, der statisch mit dem Adressbereich konfiguriert ist, der von diesem Cluster verwaltet wird.

Zusammengefaßt verfügt der Cisco CallManager über folgende Fähigkeiten zur Anrufzugangskontrolle:

- Unterstützung für bis zu 100 Standorte in einer verteilten Anrufverarbeitungsumgebung mit mehreren Standorten.
- Gatekeeper-Fähigkeiten für die Adressauflösung bei Anrufen zwischen verschiedenen Clustern, was eine Vereinfachung des Wählplans zur Folge hat.
- Cisco CallManager benötigt eine Bandbreite 128 KBit/s. für G.711-Anrufe und von 20 KBit/s. für G.729-Anrufe.
- Das komprimierte Echtzeit-Transportprotokoll (cRTP) wird in die Bandbreitenberechnungen für die Anrufzulassungsanfrage (ARQ) nicht einbezogen.

Betriebsmodell

Die Gatekeeper-Methode der Anrufzugangskontrolle wird in zwei Teilen konfiguriert:

- Gatekeeper-Konfiguration. Hierbei konfiguriert der Netzwerkadministrator einen Cisco IOS Multimedia Conference Manager (MCM), der als Gatekeeper fungiert. Als Plattformen sind Cisco 2600-, 3600- oder 7200-Router mit Cisco IOS Version 12.1(3)T oder höher empfehlenswert.

Die Auswahl der Gatekeeper-Plattform ist abhängig von der Anzahl der Registrierungen sowie der Anzahl der Anrufe pro Sekunde. Als grobe Richtlinien können Sie sich an den Angaben zur Leistung der unterschiedlichen Plattformen in Tabelle 6-1 orientieren.

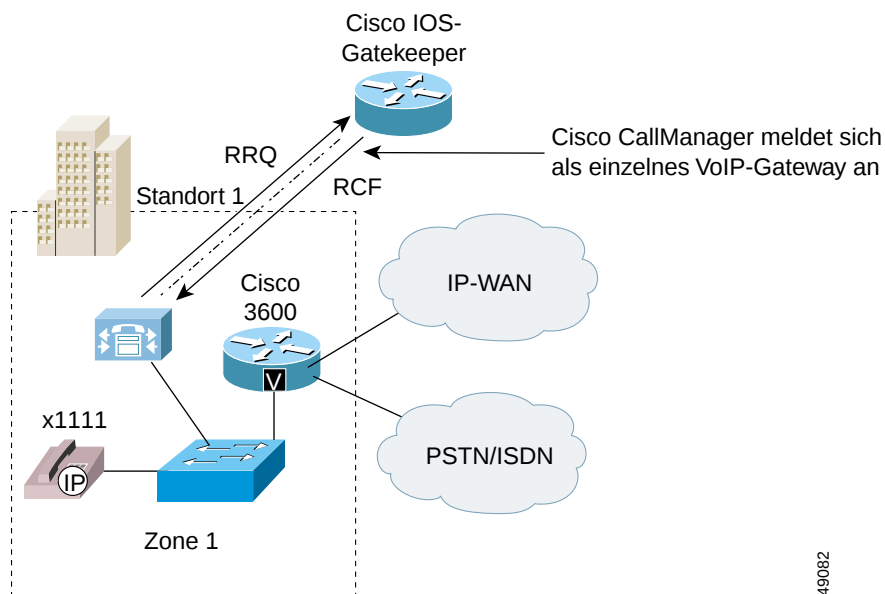
- Cisco CallManager-Konfiguration. Jeder Cisco CallManager bzw. jedes Cisco CallManager-Cluster muss sich bei dem Gatekeeper als einzelner VoIP-Gateway registrieren.

Tabelle 6-1 Angaben zur Leistung der Gatekeeper-Plattformen

Gateway-Plattform	Arbeitsspeicher	maximal Anrufe pro Sekunde für eine CPU-Auslastung von ca. 50 %
Cisco 2600	56 MB	7
Cisco 3620	56 MB	10
Cisco 3640	128 MB	24
Cisco 3660	256 MB	35
Cisco 7200/NPE300	256 MB	50

Interaktion zwischen Cisco CallManager und dem Gatekeeper

Cisco CallManager sendet eine Registrierungsanfrage (Registration Request = RRQ), um sich als einzelner VoIP-Gateway zu registrieren. Derzeit kann der Cisco IOS Multimedia Conference Manager (MCM) keine Rufnummernadressbereiche innerhalb einer RRQ annehmen. Sie können die Adressbereiche jedoch statisch auf dem Gatekeeper konfigurieren. In Abbildung 6-5 wird der Kommunikationsstrom zwischen Cisco CallManager und dem Gatekeeper dargestellt.

Abbildung 6-5 Cisco CallManager in Kommunikation mit einem Gatekeeper

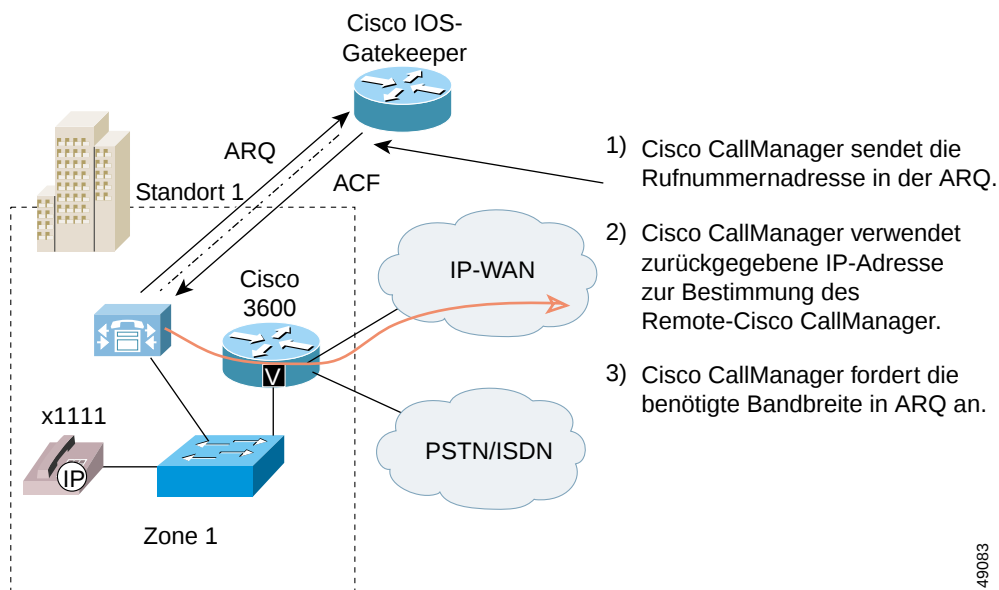
Als Ersatz bei Ausfällen und zur Sicherung kann sich mehr als ein Cisco CallManager eines Clusters beim Gatekeeper registrieren. Sie können dem Gatekeeper einer Cisco CallManager-Gruppe zuweisen, um festzulegen, welcher Cisco CallManager dieser Gruppe der primäre Manager ist und welche Manager der Sicherung dienen. Wenn der primäre

Cisco CallManager nicht mit dem Gatekeeper in Verbindung treten kann, entfernt der Gatekeeper seine Registrierung und baut eine Verbindung mit dem sekundären Cisco CallManager in der Gruppe auf

Wenn der Gatekeeper eine RRQ von einem Cisco CallManager erhält, stellt er eine Registrierungsbestätigung (Registration Confirm = RCF) aus und fügt diesen Cisco CallManager seiner Liste der registrierten Geräte hinzu. Der Gatekeeper weiß, welche Cisco CallManager bei ihm registriert sind. Mithilfe der Cisco IOS-Konfiguration kann der Gatekeeper außerdem ermitteln, welcher Cisco CallManager welcher Zone angehört und wieviel Bandbreite jeder Zone zugewiesen ist.

Wenn Cisco CallManager registriert ist, meldet er sich immer beim Gatekeeper, bevor er einen ausgehenden Anruf tätigt oder einen eingehenden Anruf annimmt. Cisco CallManager sendet hierfür eine Zulassungsanfrage (Admission Request = ARQ) an den Gatekeeper, wie in Abbildung 6-6 demonstriert ist. Als Teil der ARQ fordert Cisco CallManager außerdem je nach dem für den Anruf verwendeten Codec-Typ eine gewisse Bandbreite an. Er fordert 128 KBit/s. an, wenn der Anruf einen G.711-Codec verwendet, oder 20 KBit/s., wenn der Anruf einen G.729-Codec verwendet.

Abbildung 6-6 Anfrage zur Zulassung eines Anrufs

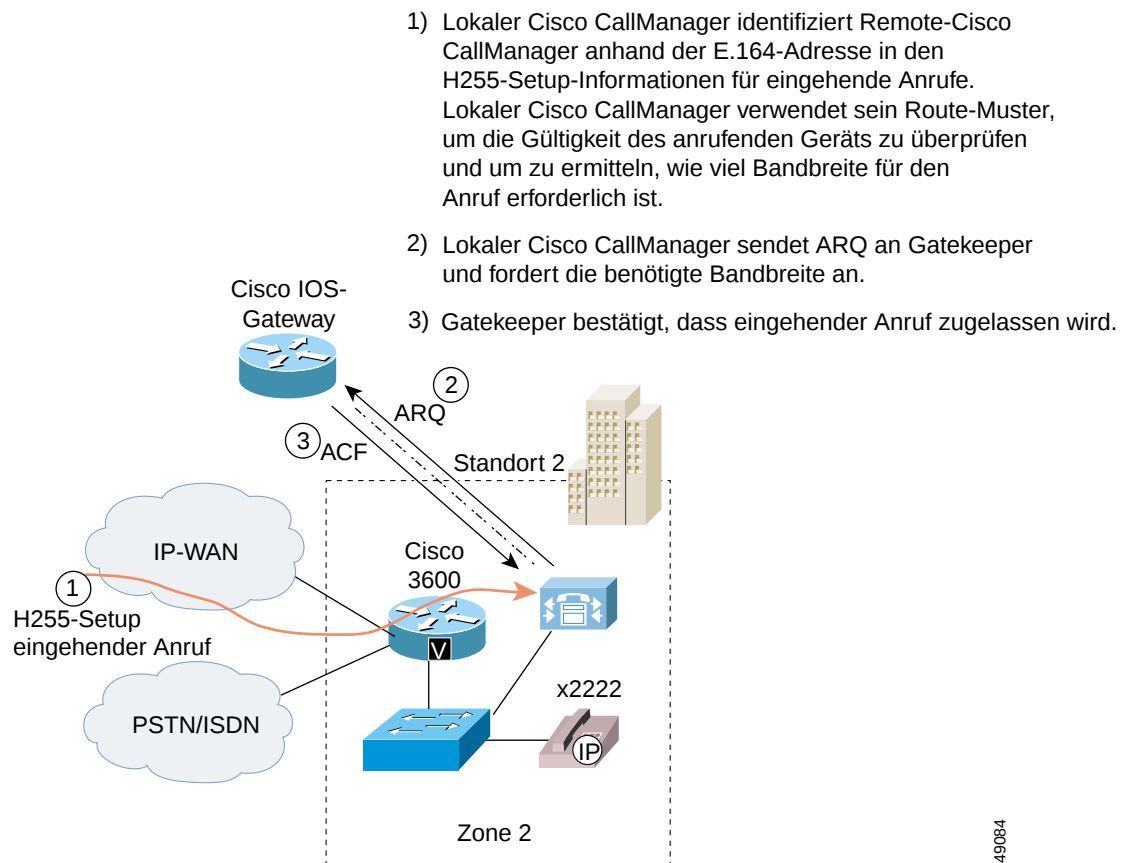


Daraufhin überprüft der Gatekeeper seine Konfiguration, um festzustellen, welche Bandbreite in der Zone verfügbar ist, der dieser Cisco CallManager zugeordnet ist. Außerdem überprüft er die Anzahl der Anrufe, die bereits in diese Zone bzw. aus dieser Zone heraus getätigt werden. Wenn Bandbreite verfügbar ist, sendet der Gateway eine Zulassungsbestätigung (Admission Confirm = ACF), mit der der Cisco CallManager den Anruf ausführen kann. Wenn keine Bandbreite verfügbar ist, sendet der Gatekeeper eine Zulassungsabweisung (Admission Reject = ARJ), die den Anruf verhindert und dem Anrufer ein Besetztzeichen ausgibt.

Wie in Abbildung 6-7 dargestellt, führt der lokale Cisco CallManager die folgenden Aktionen durch, wenn er einen eingehenden Anruf von einem entfernten Cisco CallManager über den Gatekeeper empfängt:

- Anhand der Telefonnummer der eingehenden H.225-Setupinformationen durchsucht er seine Weiterleitungsmuster nach einer Übereinstimmung. Wenn er ein passendes Weiterleitungsmuster findet, kann der lokale Cisco CallManager festlegen, ob der eingehende Anruf von einem gültigen Gerät abgeht und wieviel Bandbreite für den eingehenden Anruf benötigt wird.
- Er sendet eine Anrufzulassungsanfrage den Gatekeeper, um die benötigte Bandbreite anzufordern, bevor er den eingehenden Anruf annimmt.

Abbildung 6-7 Entgegennehmen eines Anrufs über den Gatekeeper



49084

Hinweise zur Verwendung eines Gatekeepers

Die folgenden Punkte sollten bei der Verwendung einer Anrufzugangskontrolle auf Grundlage eines Gatekeepers beachtet werden:

- Als Gatekeeper muss der Cisco IOS MCM verwendet werden. Als Plattformen sind Cisco 2600-, 3600- oder 7200-Router mit Cisco IOS Version 12.1(3)T oder höher empfehlenswert.
- Wenn zwei Gatekeeper redundant verwendet werden und der primäre Gatekeeper ausfällt, übernimmt der sekundäre Gatekeeper die Aufgaben des primären, ohne dass dieser bestehende Anrufe registriert hat. Dies kann zu Qualitätsverlusten führen, wenn der neue primäre Gatekeeper zu viele neue Anrufe zu den bereits bestehenden, nicht von ihm registrierten Anrufen zulässt. Diese Situation ist nur vorübergehend und wird aufgelöst, wenn die bestehenden Anrufe beendet werden.
- Der Standort der Geräte kann nicht geändert werden, ohne dem Gerät eine neue Nummer zuzuweisen. Somit wird sichergestellt, dass der lokalen Cisco CallManager zur Anrufverarbeitung verwendet wird.

Hinweise zu Wählplänen

Ein neues Leistungsmerkmal des Cisco CallManager Version 3.0(5) ist die Funktion, mit der der Gatekeeper den Wählplan zwischen den Cisco CallManager-Clustern auflösen kann. Für den Cisco CallManager Version 3.0(5) bestehen jetzt drei Nutzungsmodelle für die Auflösung der Ziele von Anrufen von Cluster zu Cluster:

- Cisco CallManager-Wählplanmodell
- Gatekeeper-Wählplanmodell
- Hybrides Wählplanmodell

Beim Cisco CallManager-Wählplanmodell muss jedes Cisco CallManager-Cluster über eine Trunkleitung und ein Weiterleitungsmuster zu jedem anderen Cluster verfügen. Der Verwaltungsaufwand nimmt mit steigender Anzahl der Cluster exponentiell zu. In diesem Modell bietet der Gatekeeper lediglich die Anrufzugangskontrolle, nicht aber die Wählplanauflösung. Dieses Modell hat große Ähnlichkeit mit dem Standardmodell, das heute in traditionellen PBX-Anlagen verwendet wird.

Das Gatekeeper-Wählplanmodell reduziert selbst in der hybriden Form den Konfigurations- und Verwaltungsaufwand ganz erheblich. In diesem Modell besteht nur eine Trunk-Leitung zwischen jedem Cisco CallManager und zu den anderen Clustern, die als "anonymes Gerät" bezeichnet wird. Dieses Gerät kann man sich als eine Trunk-Leitung von einem einzigen zu mehreren Punkten vorstellen, wodurch die vernetzten Punkt-zu-Punkt-Trunk-Leitungen des Cisco CallManager-Wählplanmodells unnötig werden. Das anonyme Gerät leitet Anrufe mithilfe des Gatekeepers an das richtige Cisco

CallManager-Cluster weiter. Wenn keine automatische Migration auf PSTN/ISDN bei Überlastung oder Ausfall erforderlich ist, kann der Wählplan in jedem Cluster in lediglich zwei Weiterleitungsmuster vereinfacht werden: eines für Anrufe von Cluster zu Cluster und eines für den Zugriff auf PSTN/ISDN. In diesem Modell konfigurieren Sie den Wählplan im Gatekeeper und stellen so einen zentralen Verwaltungspunkt zur Verfügung. Wenn neue Cluster hinzugefügt werden, müssen Sie statt jedes einzelnen Cisco CallManagers nur den Gatekeeper aktualisieren.

Zusammenfassend bieten die drei Wählplanmodelle die folgenden Funktionen und Fähigkeiten:

- Cisco CallManager-Wählplanmodell
 - Automatische Umleitung auf PSTN/ISDN bei Überlastung und Ausfall; der Gatekeeper wird nur zur Anrufzugangskontrolle eingesetzt.
 - Jede Kombination zweier Cisco CallManager-Cluster benötigt eine separate Trunk-Leitung.
 - Für jedes Cisco CallManager-Ziel müssen zwei Weiterleitungen vorgenommen werden, eine für das IP-WAN und eine für PSTN/ISDN.
 - Sie müssen jeden Cisco CallManager neu konfigurieren, wenn ein neues Cluster aufgenommen wird oder der Wählplan sich ändert.
- Hybrides Wählplanmodell
 - Automatische Umleitung auf PSTN/ISDN bei Überlastung und Ausfall; der Gatekeeper wird zur Anrufzugangskontrolle und für den Wählplan von Cluster zu Cluster eingesetzt.
 - In jedem Cisco CallManager-Cluster ist nur ein anonymes Gerät erforderlich.
 - Für jedes Cisco CallManager-Ziel müssen zwei Weiterleitungen vorgenommen werden, eine für das IP-WAN und eine für PSTN/ISDN.
 - Sie konfigurieren den Wählplan für Verbindungen von Cluster zu Cluster sowohl im Gatekeeper als auch im Cisco CallManager.
- Gatekeeper-Wählplanmodell
 - Manuelle Umleitung auf PSTN/ISDN bei Überlastung und Ausfall; der Gatekeeper wird zur Anrufzugangskontrolle und für den Wählplan von Cluster zu Cluster eingesetzt.
 - In jedem Cisco CallManager-Cluster ist nur ein anonymes Gerät erforderlich.
 - Es sind nur zwei Weiterleitungsmuster erforderlich, eines für Anrufe von Cluster zu Cluster für alle Standorte und eines für den Zugriff auf PSTN/ISDN.
 - Sie konfigurieren den Wählplan im Gatekeeper (nicht in jedem Cisco CallManager), um Anrufe von Cluster zu Cluster weiterzuleiten.

- Die Benutzer müssen die richtige Nummer für PSTN/ISDN wählen, um auf einen entfernten Standort zugreifen zu können, wenn das IP-WAN außer Betrieb oder überlastet ist.

Auswahl des Gatekeepers und Redundanz

Die Fehlertoleranz für den Gatekeeper ist im Cisco AVVID-Netzwerk von Bedeutung. Durch die Verwendung des Hot Standby Router Protocols (HSRP) können Sie Redundanz für die Gatekeeper erreichen. Wenn Sie zwei Gatekeeper mit HSRP konfigurieren, kann der aktive Gatekeeper Anfragen verarbeiten und der Standby-Gatekeeper diese Aufgabe übernehmen, wenn der primäre Gatekeeper ausfällt.

Nach einem Ausfall ist der aktuelle Anrufstatus verloren. Der Standby-Gatekeeper (der jetzt der aktive Gatekeeper ist) startet, ohne über Informationen über die bestehende Bandbreitenauslastung beziehungsweise der derzeit getätigten Anrufe zu verfügen. Wenn die Anrufe, die vom ausgefallenen Gatekeeper zugelassen wurden, beendet und neue Anrufe durch den neuen Gatekeeper zugelassen werden, werden neue Statusinformationen gewonnen.

Während der HSRP-Ausfallzeit gehen Gatekeeper-Funktionen verloren. Dieser Zeitraum kann mithilfe des `standby-Zeitgeber`-Befehls konfiguriert werden; das HELLO-Intervall ist standardmäßig auf 3 Sekunden, die Haltezeit auf 10 Sekunden eingestellt.

Der Einsatz von Verzeichnis-Gatekeepers in einem hierarchischen Nutzungsmodell kann Cisco CallManager mit sehr vielen Clustern unterstützen. Die Behandlung des Themas von Verzeichnis-Gatekeepers überschreitet jedoch die Grenzen dieses Dokuments.

Bandbreitenauslastung in Abhängigkeit von der gewählten Rufnummer

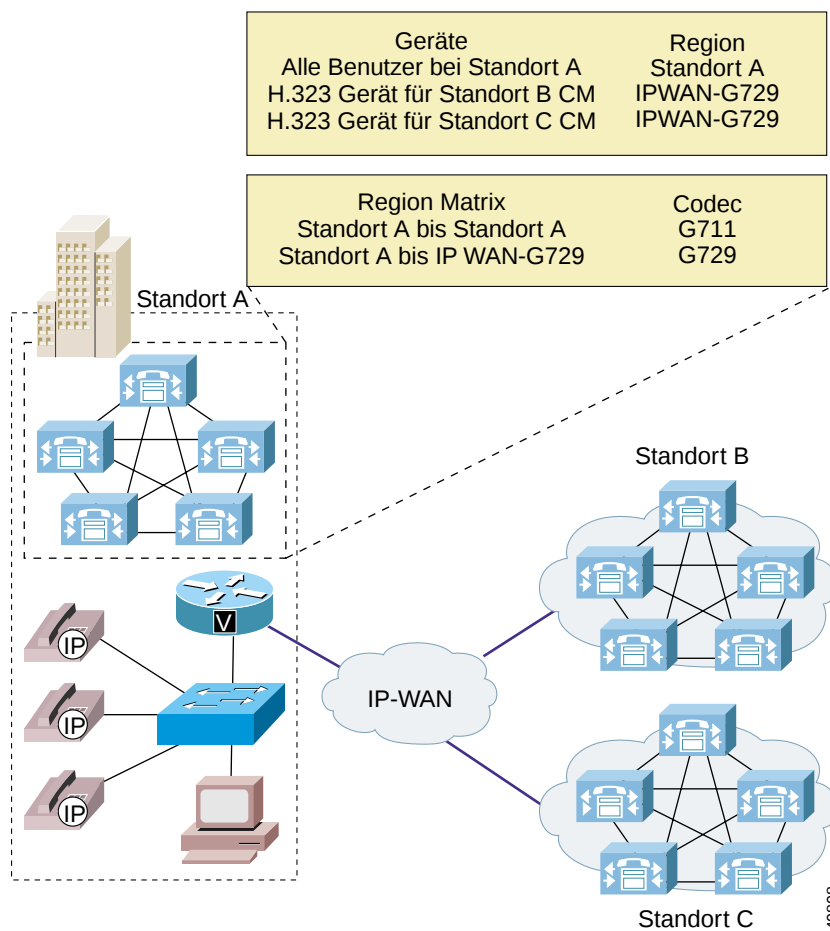
Die Bandbreite, die durch Anrufe zwischen Geräten (IP-Telefonen und Gateways) ausgelastet wird, kann über die Einrichtung von Regionen kontrolliert werden, die die Codec-Verwendung vorgeben. Die Geräte werden in eine Region gestellt, für die ein bestimmter Codec für alle Anrufe innerhalb der Region festgelegt wird und für die auch weitere Codecs für Anrufe in andere Regionen festgelegt werden können. Die Regionen werden den Geräten über einen Geräte-Pool zugewiesen. Die unterstützten Codecs, die in Regionen festgelegt werden können, sind G.711, G.729 und G.723.

In Abbildung 6-8 wird die Verwendung von Regionen für verteilte Anrufverarbeitungsumgebungen dargestellt, in denen oft nur zwei Regionen zugewiesen werden müssen.



Hinweis Wegen der Beschränkung auf nur einen Codec ist nur eine WAN-Region mit allen H.323-Geräten im gesamten IP-WAN verknüpft. In späteren Versionen des Cisco CallManagers werden eventuell mehrere WAN-Regionen unterstützt.

Abbildung 6-8 Die Verwendung von Regionen für die verteilte Anrufverarbeitung



Hinweise zu Cisco CallManager-Clustern

Die folgenden Hinweise treffen für Cisco CallManager-Cluster in einer verteilten Anrufverarbeitungsumgebung mit Cisco CallManager Version 3.0 zu:

- Jedes Cisco CallManager-Cluster kann bis zu 10.000 Benutzer unterstützen.
- Es können nicht mehr als 2.500 Benutzer bei einem gegebenen Cisco CallManager registriert sein, auch nicht unter Ausfallbedingungen.
- Nur ein einziger Cisco CallManager in einem Cluster registriert sich jeweils beim Cisco IOS-Gatekeeper.

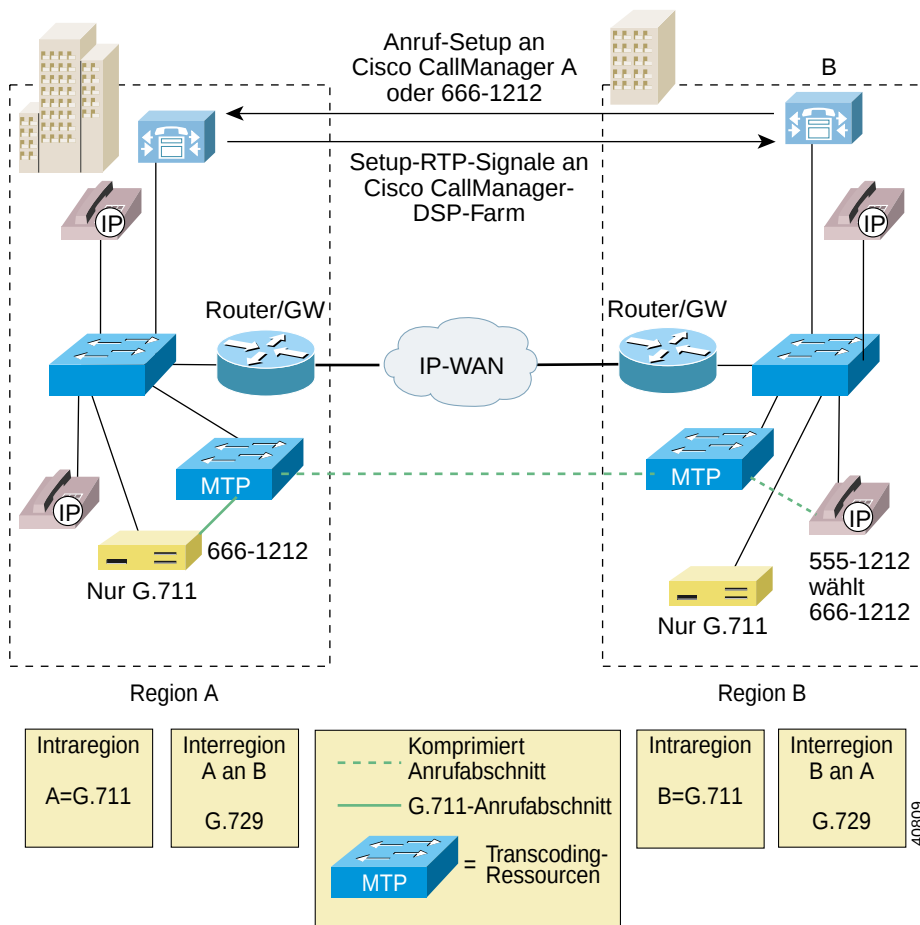
Bereitstellung von DSP-Ressourcen für das Transcoding und Conferencing

In diesem Abschnitt werden DSP-Ressourcen in verteilten Anrufverarbeitungsumgebungen kurz erläutert. In einem Multisite-WAN mit verteilter Anrufverarbeitung muss jeder Standort über DSP-Ressourcen für Conferencing und Transcoding über das IP-WAN verfügen. Die Dienste für Conferencing und Transcoding sind durch die Anwendung Media Termination Point (MTP) möglich.

Der Hauptgrund für Transcoding-DSP-Ressourcen ist die Umwandlung von einem Codec-Typ in einen anderen in einem Echtzeit-Transportprotokoll (RTP)-Datenstrom im Falle einer Nichtübereinstimmung der Codecs. Ein komprimierter G.729-Medien-RTP-Datenstrom über das IP-WAN muss beispielsweise eventuell an ein Gerät gesandt werden, das nur G.711 unterstützt. Die DSP-Transcoding-Ressource terminiert in diesem Fall den G.729-Medienstrom und wandelt ihn in G.711 um. Hierdurch kann der Medienstrom im gesamten WAN komprimiert bleiben. In Abbildung 6-9 wird die Funktion der DSP-Ressourcen im IP-WAN wie in den folgenden Schritten aufgeführt dargestellt:

-
- Schritt 1** Anrufer 555-1212 in Region B ruft per Voicemail in Region A an.
- Schritt 2** Cisco CallManager B erkennt, dass das Ziel Region A, LBR-Codec ist.
- Schritt 3** Cisco CallManager A erkennt einen eingehenden LBR-Anruf für ein G.711-Gerät.
- Schritt 4** Der Medienstrom wird an die terminierende DSP-Farm umgeleitet.
-

Abbildung 6-9 DSP-Ressourcen im WAN



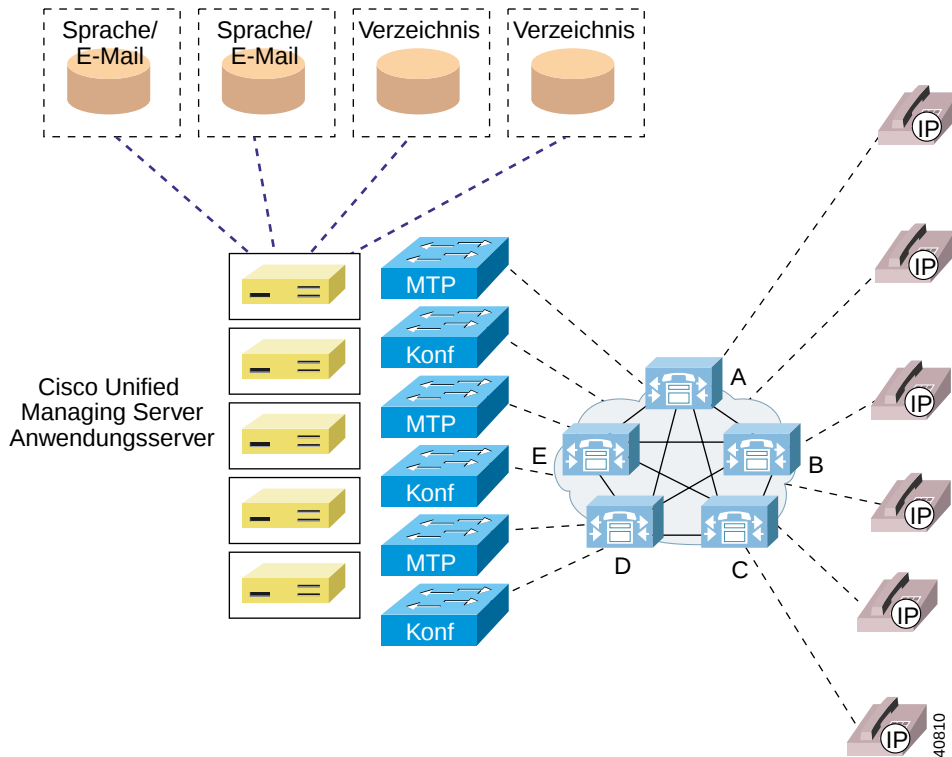
Die Anzahl der zugewiesenen Ressourcen hängt von den Anforderungen an das Transcoding in Voicemail sowie an Transcoding in G.711 für andere Anwendungen, wie z. B. Konferenzschaltungen, ab. Diese Zahlen werden auf der Grundlage des Verhältnisses zwischen Benutzern an Voicemail-Ports und dem Aufkommen der getätigten Konferenzanrufe berechnet.

In einer Umgebung, in der nicht alle Geräte alle Codec-Typen unterstützen können, sollten Sie das dedizierte Transcoding zwischen den Clustern konfigurieren. Wählen Sie für diese Konfiguration **Device (Gerät) > Gatekeeper** in der Cisco CallManager-Administration aus und aktivieren Sie das für den Media Termination Point benötigte Auswahlfeld. Wenn Sie diesen Konfigurationsschritt nicht durchführen, kann Cisco CallManager nicht automatisch den richtigen Transcoder auswählen, so dass der RTP-Datenstrom die Übertragung nicht abschließen kann, wenn die Codecs nicht übereinstimmen.

Hinweise zu Voice Messaging

In einem Multisite-IP-WAN mit verteilter Anrufverarbeitung muss jeder Standort über eigene Voice Messaging-Komponenten verfügen. Dies trifft bei der Verwendung des Cisco Unified Messaging Servers ebenso zu wie bei der Verwendung einer Schnittstelle mit einem anderen Voice Messaging System. Siehe Abbildung 6-10.

Abbildung 6-10 WAN-Cluster-Platzierung von Voicemail





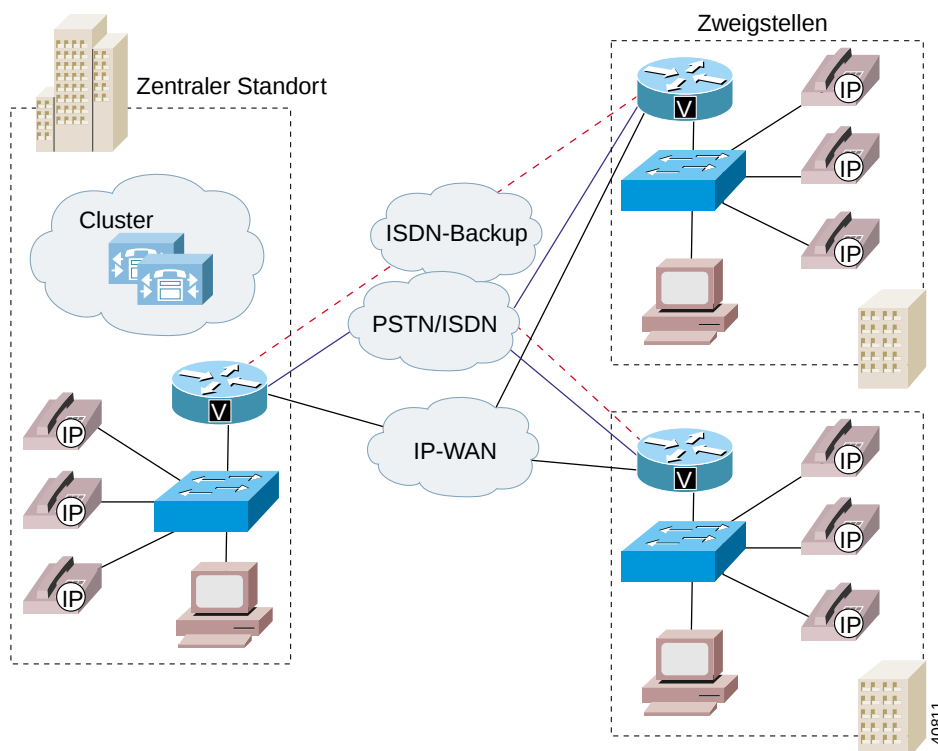
Multisite-WAN mit zentraler Anrufverarbeitung

In diesem Kapitel werden Designrichtlinien für Multisite-WAN-Systeme beschrieben, die für den Einsatz des Cisco CallManager Version 3.0(5) für die zentrale Anrufverarbeitung anzuwenden sind. Der Schwerpunkt liegt auf der zentralen Anrufverarbeitung. Sie finden außerdem Verweise auf entsprechendes Material in anderen Abschnitten dieses Handbuchs.

Zentrale Anrufverarbeitung

In einem System mit zentraler Anrufverarbeitung (siehe Abbildung 7-1) befinden sich die Cisco CallManager im Hub oder am zentralen Standort. In den Zweigstellen findet keine lokale Anrufverarbeitung statt.

Abbildung 7-1 Multisite-WAN mit zentraler Anrufverarbeitung



In Abbildung 7-1 befindet sich der Cisco CallManager-Cluster am zentralen Standort. Da alle IP-Telefone in diesem Cluster bei einem Cisco CallManager angemeldet werden müssen, ist diese Lösung auf 2500 Benutzer pro Cluster beschränkt. Um diese Lösung zu erweitern, können mehrere Cluster am zentralen Standort installiert und über H.323 miteinander verbunden werden.

Der größte Vorteil dieses Modells besteht darin, dass die Anrufverarbeitung zentral erfolgen kann. Dadurch werden in den Zweigstellen weniger Geräte benötigt. Früher wären mehrere PBX-systeme verwendet worden, was einen erheblichen Verwaltungsaufwand bedeutete, der nun ebenfalls wegfällt. Abbildung 7-1 zeigt, dass das IP-WAN durch eine ISDN (Integrated Services Digital Network)-Verbindung gesichert ist, die einen redundanten IP-WAN-Pfad für die Anrufverarbeitung bereitstellt. Dieses Schema bietet sich besonders für kleine Zweigstellen mit weniger als 20 Mitarbeitern und Telecommuter an. Life-Line-Dienste können von dedizierten POTS-Leitungen oder Mobiltelefonen bereitgestellt werden.

Anrufzugangskontrolle

Bei Verwendung der zentralen Anrufverarbeitung erfolgt die Anrufzugangskontrolle über das Standort-Prinzip. Dabei wird für die Standorte eine geografische Entsprechung angegeben, etwa der Name einer Zweigstelle. Sie können einen Standort, beispielsweise Zweigstelle 1, Büro am Messegelände, nennen. (Es kann auch eine Postleitzahl angegeben werden.) Der Standort sollte einem geografischen Ort entsprechen, der mit einem Wide Area Link verbunden ist. Anschließend wird für den Standort die maximale Bandbreite festgelegt, die für Sprachanrufe mit anderen Standorten verwendet werden kann. Die Geräte an diesem Standort werden dann diesem Standort zugewiesen. Siehe Abbildung 7-2.

Abbildung 7-2 Konfiguration des Cisco CallManager-Standorts



40812

Der zentrale Cisco CallManager überwacht, wieviel Bandbreite ein Standort für Sprachanrufe mit anderen Standorten benötigt. Wenn die konfigurierte Einstellung mit einem neuen Anruf über das IP-WAN überschritten werden würde, erhält der Anrufer ein Besetztzeichen und eine konfigurierbare Anzeige, beispielsweise "Alle Trunks belegt" (sofern das Gerät diese Funktionalität unterstützt). Wenn der Anrufer ein Besetztzeichen erhält, muss er auflegen und den Zugriffscode für das PSTN/ISDN-Gateway dieses Standorts wählen, um einen ausgehenden Anruf tätigen zu können.

Tabelle 7-1 bietet eine Übersicht über gebräuchliche Gateways und die Cisco IOS-Versionen, die mindestens erforderlich sind.

Tabelle 7-1 Mindestens erforderliche Cisco IOS-Version für IOS-Gateway-Plattform

Plattform	Mindestens erforderliche Cisco IOS-Version
Cisco 1750	12.1.(1)T
Cisco 2600	12.0.(7)T
Cisco 3600	12.0.(7)T
Cisco MC 3810 v3	12.0.(7)XK

Darüber hinaus muss die Bandbreite, die für einen bestimmten Standort konfiguriert ist, kleiner oder gleich der konfigurierten Queue für Sprache in den Wide Area Links sein. Die bevorzugte Queuing-Methode ist das Low-Latency-Queuing, das in Kapitel 8, "Quality of Service", näher beschrieben wird.

Einschränkungen bei der standortbasierten Anrufzugangskontrolle

Beachten Sie, dass bei der standortbasierten Anrufgangskontrolle folgende Einschränkungen bestehen:

- Geräte können nicht zwischen verschiedenen Standorten verschoben werden, da der Cisco CallManager die Bandbreite für den angegebenen Standort und nicht für den physischen Standort des Geräts überwacht.
- Cisco CallManager Version 3.0(5)-Installationen mit zentraler Anrufverarbeitung sind auf Hub-und-Spoke-Topologien beschränkt.
- Wenn mehr als eine Verbindung oder virtuelle Verbindung für einen Spoke-Standort vorhanden ist, sollte die Bandbreite an die dedizierten Ressourcen angepasst werden, die auf der kleineren Verbindung zugewiesen sind.
- Der Cisco IOS-Gatekeeper kann die Zugangskontrolle nur für Anrufe zwischen Cisco CallManagern bereitstellen. Zwischen einem Cisco CallManager und einem entfernten Cisco IOS-Gateway ist keine

Zugangskontrolle durch den Gatekeeper möglich. Ein Beispiel wäre, wenn ein Cisco CallManager an einem Standort bei einem anderen Standort anruft, bei dem ein Cisco IOS-Gateway mit einer PBX verbunden ist. Der Cisco CallManager verwendet keine Rufnummernadressen in der ARP-Anfrage, wenn eine Zulassungsanfrage (Admission Request, ARQ) beim Gatekeeper gestellt wird. Diese Einschränkung wird in zukünftigen Versionen des Cisco CallManagers möglicherweise wegfallen.

Informationen zu Cisco CallManager-Clustern

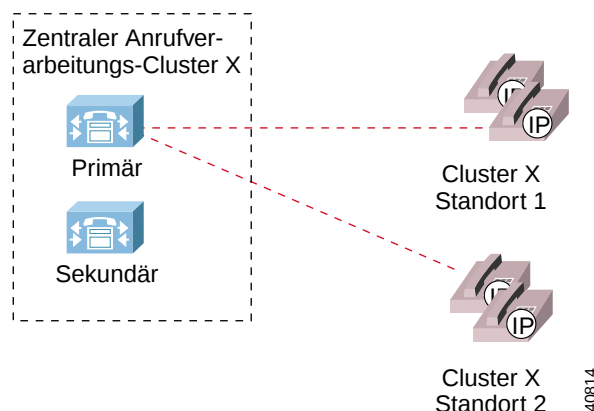
Folgende Designparameter gelten für Cisco CallManager-Cluster in einer Umgebung mit zentraler Anrufverarbeitung, in der der Cisco CallManager Version 3.0(5) verwendet wird.

- Ein primärer Cisco CallManager pro Cluster
- Maximal 2500 IP-Telefone pro Cluster
- Maximal drei Cisco CallManager pro Cisco CallManager-Cluster
- Nur Hub-und-Spoke-Topologien

Bei WAN-Cisco CallManager-Clustern müssen sich alle aktiven Geräte bei einem Cisco CallManager anmelden. Dadurch kann der Cisco CallManager den Anrufstatus für alle Anrufe erhalten und sicherstellen, dass die angegebene Bandbreite für einen Standort nicht überschritten wird.

Abbildung 7-3 zeigt Geräte, die bei einem Cisco CallManager angemeldet sind.

Abbildung 7-3 Anmeldung bei einem Cisco CallManager in einem Cluster



Falls mehr als 2500 entfernte Geräte benötigt werden, können mehrere WAN-Cluster konfiguriert und über H.323 verbunden werden. Weitere Informationen finden Sie in Kapitel 3, "Cisco CallManager-Cluster".

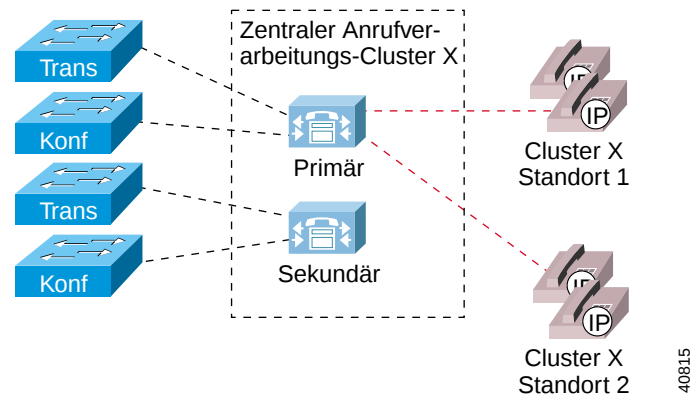
In diesem Modell sollte eine Cisco CallManager-Redundanzgruppe konfiguriert werden. Diese sollte als Standardredundanzgruppe für Cisco CallManager verwendet werden. Alle Geräte würden dann dieser Gruppe zugewiesen werden, um sicherzustellen, dass alle beim selben Cisco CallManager angemeldet sind.

DSP-Ressourcenzuweisung für Transcoding und Conferencing

Die zentrale Anrufverarbeitung wird in der Regel in Umgebungen eingesetzt, in denen die dedizierte Anrufverarbeitung an den einzelnen Standorten zu teuer oder aus verwaltungstechnischen Gründen nicht akzeptabel ist. Die Vorteile einer solchen Konfiguration liegen in der zentralen Verwaltung und den niedrigen Kosten, wenn es sich um sehr viele Standorte handelt. Digital Signal Processor (DSP)-Ressourcen sind für das Transcoding und Conferencing von Anrufen erforderlich. Diese Ressourcen werden jedem einzelnen Cisco CallManager zugeordnet und müssen sich am zentralen Standort befinden.

Abbildung 7-4 zeigt die Aufteilung der DSP-Ressourcen.

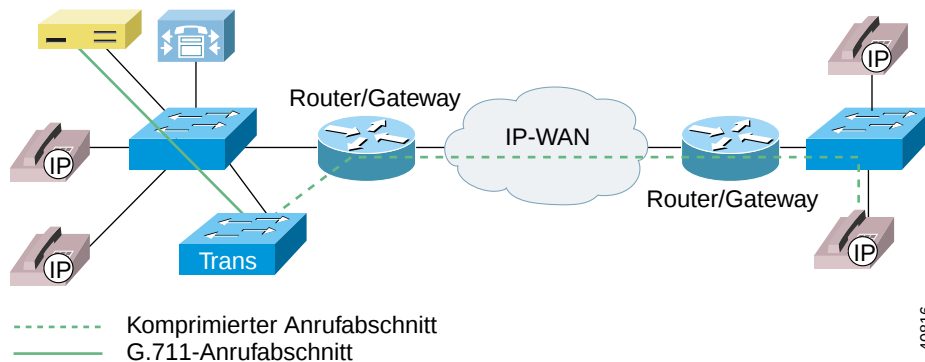
Abbildung 7-4 DSP-Ressourcenzuweisung



Die Anzahl der zugewiesenen Ressourcen hängt von den Anforderungen für das Transcoding in Voicemail und das Transcoding in G.711 bei anderen Anwendungen (z. B. Conferencing) ab. Diese Anzahl wird aus dem Verhältnis Benutzer/Voicemail-Anschlüsse und der Anzahl der durchgeführten Konferenzschaltungen errechnet. Wenn aus Kostengründen nicht jedem Cisco CallManager Ressourcen zugewiesen werden können, können die Ressourcen statisch innerhalb des WAN-Clusters verschoben werden, falls der primäre Cisco CallManager einmal ausfällt.

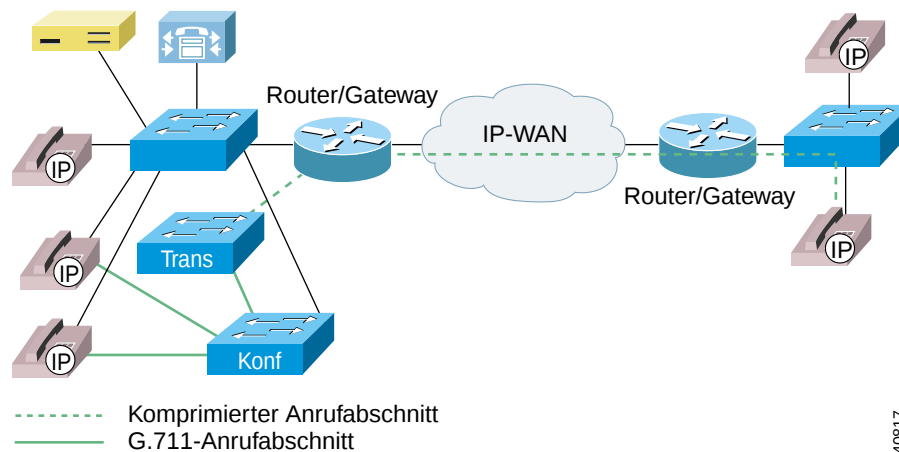
Abbildung 7-5 zeigt eine zentrale Transcoding-Ressource, die G.729a oder G.723.1 in G.711 umwandelt, wenn ein ursprünglicher G.729a- oder G.723.1-Anruf an die Voicemail geleitet wird, die eine G.711-Anwendung ist.

Abbildung 7-5 Anrufluss beim zentralen Transcoding eines Anrufs in Voicemail



Das Conferencing ist ein weiteres Beispiel für eine Anwendung, die nur G.711 verwendet. Wenn also der Teilnehmer, der eine Konferenzschaltung aufbauen möchte, das WAN nur mit einem Low-Bit-Rate-Codec durchlaufen kann, muss ein Transcoding des Anrufs in G.711 erfolgen, bevor die Konferenzschaltung aufgebaut werden kann. Siehe Abbildung 7-6.

Abbildung 7-6 Anrufluss beim zentralen Transcoding eines Anrufs für Conferencing



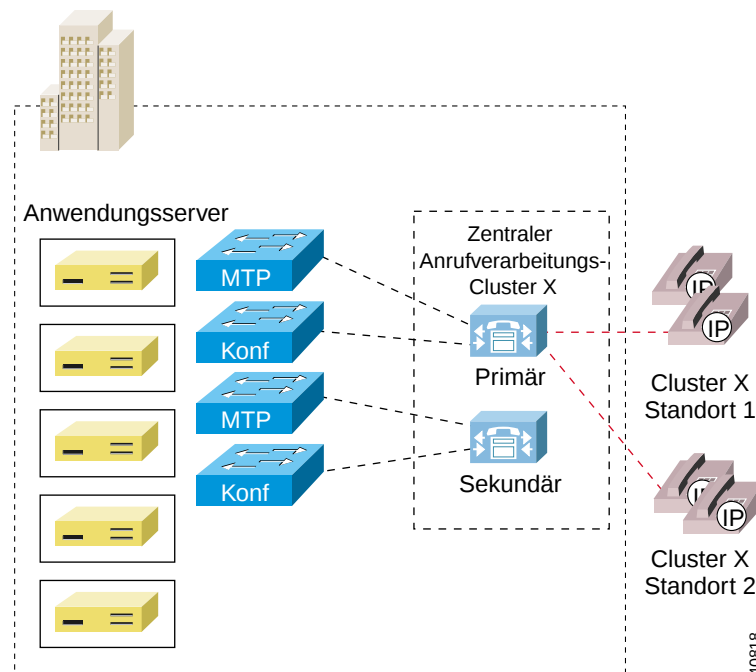
Bei dem in Abbildung 7-6 dargestellten Szenario durchläuft der aus der Zweigstelle kommende Anruf das WAN mit G.729a, muss jedoch in G.711 transcodiert werden, bevor er in die Konferenzschaltung aufgenommen werden kann.

Informationen zum Voice Messaging

Wie die Anrufverarbeitung sind auch Voicemails in Zweigstellen im Normalfall nicht kosteneffektiv. Ein zentrales Voicemail-System erleichtert die Verwaltung und die Bereitstellung von IP-Telefonie-Services.

Egal, ob eine Verbindung zu einem bestehenden System oder einem IP-basierten Voicemail-System aufgebaut wird, Sie müssen immer ausreichend Kapazitäten für parallel laufende Voicemail-Sitzungen planen und entsprechende Transcoding-Ressourcen bereitstellen, falls ein Low-Bit-Rate-Codec für das WAN erforderlich ist. Siehe Abbildung 7-7.

Abbildung 7-7 Anordnung der Voicemail-Cluster bei zentraler Anrufverarbeitung



In Abbildung 7-7 gibt es fünf Anwendungsserver am Standort des Hubs, die Voicemail für maximal 2500 entfernte Benutzer bereitstellen. Die DSP-Ressourcen werden für das Transcoding von G.729 in G.711 benötigt, falls ein Low-Bit-Rate-Codec zwischen Standorten verwendet wird und es sich bei der Anwendung um eine G.711-Anwendung handelt.



Quality of Service

In diesem Kapitel werden die Voraussetzungen für Quality of Service (QoS) von Implementierungen der IP-Telefonielösungen in einem gesamten Unternehmensnetzwerk angesprochen. Wenn Sie die erforderlichen Tools anwenden, können Sie unabhängig vom verwendeten Medium Sprach-, Bilder- und Datenübertragungen über eine IP-Infrastruktur mit exzellenter Qualität selbst bei niedrigen Datenübertragungsgeschwindigkeiten erreichen. Weitere detaillierte Informationen zum Entwerfen von Quality of Service-Netzwerken für die AVVID-Nutzung finden Sie im Cisco AVVID QoS Design Guide unter http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/index.htm

QoS-Standortmodell

Bis vor kurzem ging man davon aus, dass Quality of Service in Unternehmensnetzwerken niemals zu einem Problem werden könnte, da der Datenverkehr eher stoßweise erfolgt und Pufferüberlastungen und Paketverlusten standhalten kann. Als Anwendungen wie Sprach- und Bildübertragung überhand nahmen, die für Verluste und Verzögerungen anfällig sind, mussten die Netzwerkdesigner erkennen, dass in einem Netzwerk nicht die Bandbreite, sondern die Pufferkapazität die größte Herausforderung darstellt. Ein Pufferspeicher kann in kürzester Zeit ausgelastet sein. Wenn diese Situation auftritt, können Pakete verloren gehen. Bei Sprachanwendungen, die extrem Verlust-intolerant sind, führt dies zu einer Verminderung der Sprachqualität. QoS-Tools sind zur Verwaltung dieser Puffer notwendig, um Verluste, Verzögerungen und Verzögerungsunterschiede zu minimieren.

Die QoS in Unternehmensnetzwerken teilt sich in zwei Konfigurationsbereiche, die in den folgenden Abschnitten erörtert werden:

- Verkehrsklassifizierung
- Interface-Queueing

Verkehrsklassifizierung

Integraler Bestandteil der Cisco Netzwerkdesign-Architektur ist es, den Verkehr so nah wie möglich am Rand des Netzwerks zu klassifizieren bzw. zu markieren. Die Verkehrsklassifizierung ist ein Eingangskriterium für den

Zugriff auf die unterschiedlichen Queueingsschemata, die in den Switches und WAN-Schnittstellen des Unternehmensnetzwerkes verwendet werden. Wenn ein IP-Telefon mit einem einzigen Kabelmodell angeschlossen wird, wird dieses Telefon zum Rand des verwalteten Netzwerkes. Daher kann und muss das IP-Telefon Verkehrsflüsse klassifizieren. In Tabelle 8-1 werden die Richtlinien für die AVVID-Verkehrsklassifikationen aufgeführt.

Tabelle 8-1 Verkehrsklassifikationsrichtlinien für AVVID-Netzwerke

Verkehrstyp	Class of Service (CoS) in Schicht 2	IP-Präzedenz in Schicht 3	DSCP in Schicht 3
Voice RTP	5	5	EF
Voice Control	3	3	AF31
Video	4	4	AF41
Daten	0-2	0-2	0-AF23

Interface-Queueing

Um Sprachqualität garantieren zu können, muss bei einem Entwurf QoS innerhalb der Infrastuktur des Unternehmensnetzwerkes aktiviert werden. Wenn Sie QoS in Switches des Unternehmensnetzwerkes aktivieren, können Sie den gesamten Sprachverkehr so konfigurieren, dass er separate Warteschlangen verwendet, so dass Sie praktisch die Möglichkeit verlorener Datenpakete bei einer sofortigen Auslastung des Schnittstellenpuffers ausschließen.

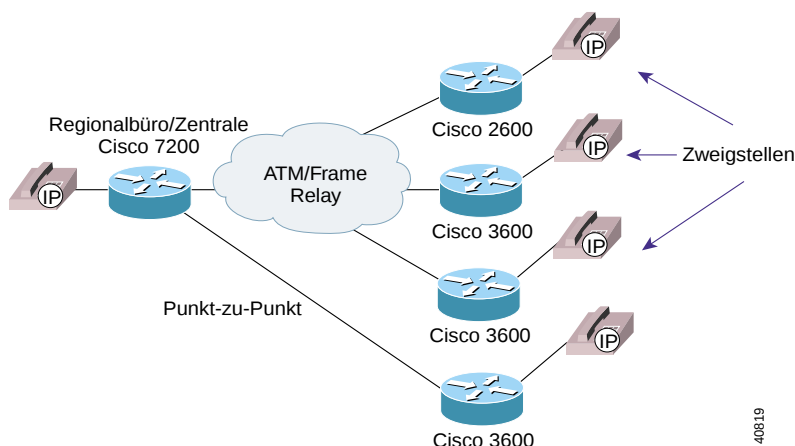
Wenn auch die Netzwerkmanagements-Tools u. U. keine Überlastung des Unternehmensnetzwerkes anzeigen, müssen QoS-Tools dennoch die Sprachqualität garantieren. Die heutigen Netzwerkmanagements-Tools zeigen nur die durchschnittliche Netzwerkauslastung für eine gewisse Beispielzeitspanne an. Dieser Mittelwert ist zwar nützlich, gibt jedoch nicht die Auslastungsspitzen an einer Schnittstelle des Unternehmensnetzwerkes an. Die Puffer an den Übertragungsschnittstellen eines Unternehmensnetzwerkes sind in kurzen, vorübergehenden Intervallen vollständig überlastet, da der Netzwerkverkehr stoßweise fließt. Bei einer solchen Überlastung gehen Pakete, die für diese Übertragungsschnittstelle vorgesehen sind, verloren. Der Verlust des Sprachverkehrs kann nur durch die Konfiguration mehrerer Warteschlangen an den Switches des Unternehmensnetzwerkes vermieden werden. In Tabelle 8-2 werden die Cisco Ethernet-Switches aufgeführt, die verbesserte Queueingsdienste unterstützen.

Tabelle 8-2 Von Cisco Switches unterstützte Queueingdienste

Campus Switching Element	Queueingsschema	Queueings-Zeitplaner	Warteschlangenzulassung
Catalyst 6000	2Q2T und 1P2Q2T	WRR und PQ/WRR	Konfigurierbar
Catalyst 8500	4Q1T	WRR	In CoS-Paaren konfigurierbar
Catalyst 4000	2Q1T	RR	In CoS-Paaren konfigurierbar
Catalyst 3500	2Q1T	PQ	Nicht konfigurierbar. CoS 0-3 = Warteschlange1 CoS 0-3 = Warteschlange2
Catalyst 2900 XL (8 MB DRAM)	2Q1T	PQ	Nicht konfigurierbar. CoS 0-3 = Warteschlange1 CoS 0-3 = Warteschlange2
IP-Telefon	1P3Q1T	RR mit einem PQ-Zeitgeber	Nicht konfigurierbar. CoS 5 = Warteschlange0 (PQ). Alle anderen CoS-Werte = Warteschlangen 1-3.

QoS-WAN-Modell

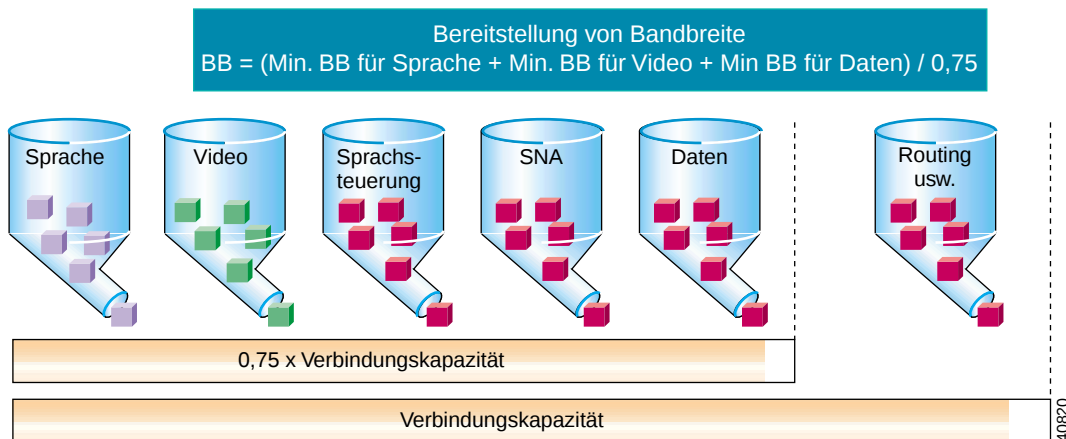
Das Unternehmens-WAN-Modell wird in Abbildung 8-1 dargestellt.

Abbildung 8-1 Typisches Unternehmens-WAN


WAN-Versorgung

Bevor Sprache und bewegte Bilder in einem Netzwerk platziert werden können, muss sichergestellt sein, dass genügend Bandbreite für alle erforderlichen Anwendungen verfügbar ist. Zunächst sollten die Mindestanforderungen in Bezug auf die Bandbreite für alle wichtigen Anwendungen (beispielsweise Sprachsignale, Bildsignale, Sprachkontrollprotokolle sowie sämtlicher Datenverkehr) zusammengefasst werden. Diese Summe steht für die Mindestanforderungen an die Bandbreite für jede gegebene Verbindung, die nicht mehr als 75 % der gesamten Bandbreite, die für diese Verbindung zur Verfügung steht, betragen sollte. Diese 75%-Regel geht davon aus, dass ein Teil der Bandbreite für zusätzlichen Verwaltungsdatenverkehr erforderlich ist, wie z. B. für das Umleiten sowie die Aufrechterhaltung der 2. Schicht, sowie für zusätzliche Anwendungen, wie z. B. E-Mail, HTTP-Verkehr sowie sonstigen, schwer messbaren Datenverkehr. Siehe Abbildung 8-2.

Abbildung 8-2 Versorgung eines konvergenten Netzwerks



WAN-QoS-Tools

In diesem Abschnitt werden die Tools erörtert, die zur Implementierung von QoS für IP-Telefonie-Anwendungen im gesamten Unternehmens-WAN verwendet werden. Diese Tools umfassen das Setzen von Prioritäten für den Verkehr, Verbindungsfragmentierung und -verschachtelung (Link Fragmentation and Interleaving = LFI) sowie die Verkehrssteuerung. Zum Abschluss dieses Abschnitts werden die idealen Vorgehensweisen für jedes dieser anwendbaren Routing-Protokolle zusammengefasst.

Setzen von Prioritäten für den Verkehr

Wenn aus den vielen verfügbaren Schemata zum Setzen von Prioritäten eine Auswahl getroffen werden soll, müssen viele Faktoren in Betracht gezogen werden, wie z. B. die Art des Verkehrs, der in das Netzwerk gestellt wird, sowie die Backbone-Netzwerke, die passiert werden. Für einen Verkehr über ein IP-WAN, der viele Dienste umfasst, empfiehlt Cisco eine Queueing mit niedrigen Latenzzeiten für Verbindungen mit niedriger Geschwindigkeit. So sind bis zu 64 Verkehrsklassen mit der Fähigkeit, beispielsweise das Verhalten der Prioritäten-Warteschlangen- steuerung für Sprache und interaktive bewegte Bilder festzulegen, eine maximale Bandbreite für die Zuführung von Systems Network Architecture (SNA)-Daten und Marktdaten sowie Weighted Fair Queueing für andere Verkehrstypen möglich.

In Abbildung 8-3 wird dieses Schema zum Setzen von Prioritäten folgendermaßen dargestellt:

- Sprache wird in eine Warteschlange mit der Fähigkeit der Prioritäten-Queueing gestellt; ihr wird eine Bandbreite von 48 KBit/s. zugewiesen. Das Eingangskriterium für diese Warteschlange sollte der Differentiated Services Code Point (DSCP)-Wert EF bzw. der IP-Präzedenzwert 5 sein. Verkehr von mehr als 48 KBit/s geht hierbei verloren, wenn die Schnittstelle überlastet wird. Daher muss ein Zugangskontrollmechanismus verwendet werden, um sicherzustellen, dass dieser Wert nicht überschritten wird.
- Video-Konferenzverkehr wird in eine Warteschlange mit der Fähigkeit der Prioritäten-Queueing gestellt, und ihr wird eine Bandbreite von 384 KBit/s. zugewiesen. Das Eingangskriterium für diese Warteschlange sollte ein DSCP-Wert von AF41 bzw. der IP-Präzedenzwert 4 sein. Verkehr von mehr als 384 KBit/s. geht hierbei verloren, wenn die Schnittstelle überlastet wird. Daher ist es ebenso wie bei Sprachverkehr überaus wichtig, dass ein Zugangskontrollmechanismus verwendet wird, um sicherzustellen, dass dieser Wert nicht überschritten wird.

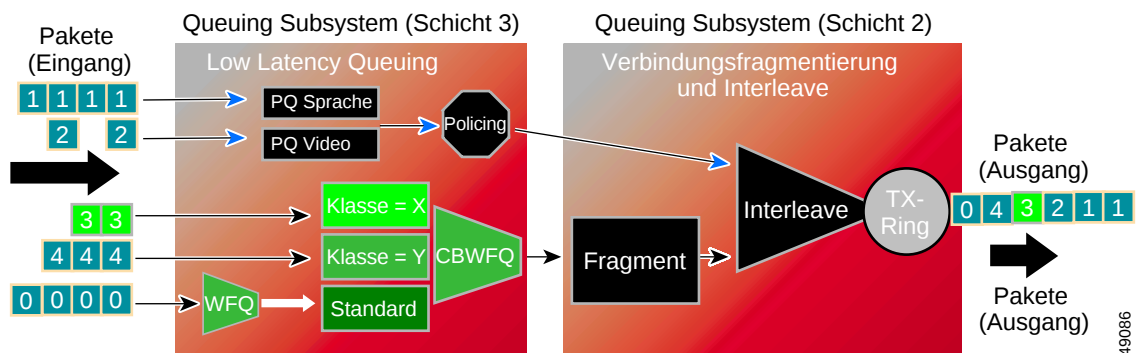


Hinweis Einseitiger Bilderverkehr, wie z. B. IP-TV, sollte ein Klassen-basiertes, gewichtetes, faires Queueingschema verwenden, da die Verzögerungstoleranzen viel höher liegen.

- Wenn die WAN-Leitungen überlastet werden, können die Sprachkontrollsignalisierungsprotokolle vollständig unterdrückt werden, so dass die Fähigkeit der IP-Telefone, Anrufe über das IP-WAN zu tätigen, ausgeschaltet wird. Sprachkontrollprotokollverkehr, wie z. B. H.323 und das Skinny Client Control Protocol, erfordert seine eigene Klassen-basierte, gewichtete, faire Warteschlange mit einer konfigurierbaren Mindestbandbreite, die dem einem DSCP-Wert von AF31 entspricht, der wiederum einem IP-Präzedenzwert von 3 entspricht.

- SNA-Verkehr wird in eine Warteschlange gestellt, die über eine festgelegte Bandbreite von 56 KBit/s verfügt. Der Queueingsbetrieb innerhalb dieser Klasse ist First-in-First-out (FIFO) mit einer zugewiesenen Mindestbandbreite von 56 KBit/s. Der Verkehr in dieser Klasse, der 56 KBit/s. überschreitet, wird in die Standardwarteschlange gestellt. Das Eingangskriterium für diese Warteschlange könnte TCP-Port-Nummern, die Schicht-3-Adresse, die IP-Präzedenz oder ein DSCP-Wert sein.
- Der gesamte übrige Verkehr kann in eine Standardwarteschlange gestellt werden. Wenn eine Bandbreite festgelegt ist, wäre der Queueingsbetrieb FIFO. Alternativ kann durch Angeben des Schlüsselwortes **fair** der Betrieb als gewichtete faire Queueing ablaufen.

Abbildung 8-3 Optimierte Queueing für VoIP über das WAN



Die folgenden Punkte müssen in Betracht gezogen werden, wenn eine Queueing mit niedrigen Latenzzeiten (Low Latency Queueing, LLQ) konfiguriert wird:

- Die Mindestanforderungen an die System-Software für Mietleitungen und den asynchronen Transfermodus (ATM) ist Cisco IOS Version 12.1(2)T.
- Die Mindestanforderung an die System-Software für Frame Relay ist Cisco IOS Version 12.1(2)T.

In Tabelle 8-3 werden die Mindestanforderungen an die Bandbreite für Sprach-, Video- und Datennetze mit Cisco CallManager Version 3.0(5) angegeben. Beachten Sie bitte, dass es sich bei hierbei um Mindestwerte handelt und jedes Netzwerk mit angemessener Kapazität entworfen werden sollte.

Tabelle 8-3 Mindestanforderungen an die Bandbreite mit Cisco CallManager 3.0(5)

Verkehrstyp	Mietleitungen	Frame Relay	ATM	ATM/Frame Relay
Sprache + Daten	64 KBit/s	64 KBit/s	128 KBit/s	128 KBit/s
Sprache, Video und Daten	768 KBit/s	768 KBit/s	768 KBit/s	768 KBit/s

Verbindungseffizienztechniken

Da die Bandbreite für Backbone-Netze häufig abschreckend kostenintensiv ist, sind u. U. nur Leitungen mit niedriger Geschwindigkeit verfügbar, wenn entfernte Standorte miteinander verbunden werden. In solchen Fällen ist es wichtig, dass durch die Übertragung möglichst vieler Sprachanrufe über die Verbindung mit niedriger Geschwindigkeit maximale Einsparungen erzielt werden. Viele Komprimierungsschemata, wie z. B. G.729, können einen 64-KBit/s-Anruf auf eine Nutzlast von nur 8 KBit/s komprimieren. Gateways und IP-Telefone von Cisco unterstützen eine Reihe von Codecs, die die Effizienz dieser Leitungen mit niedriger Geschwindigkeit verbessern können.

Die Verbindungseffizienz kann durch die Verwendung von komprimiertem RTP (cRTP) weiterhin verbessert werden, wodurch ein IP + UDP + RTP-Header von 40 Byte auf ca. zwei bis vier Byte komprimiert werden kann. Außerdem nutzt die Sprachaktivitätserkennung (Voice Activity Detection = VAD) die Tatsache, dass in den meisten Gesprächen meist jeweils nur ein Teilnehmer redet. Die VAD nutzt diese ungenutzte Zeit dadurch aus, dass sie die Nutzung der Bandbreite durch Daten zulässt.

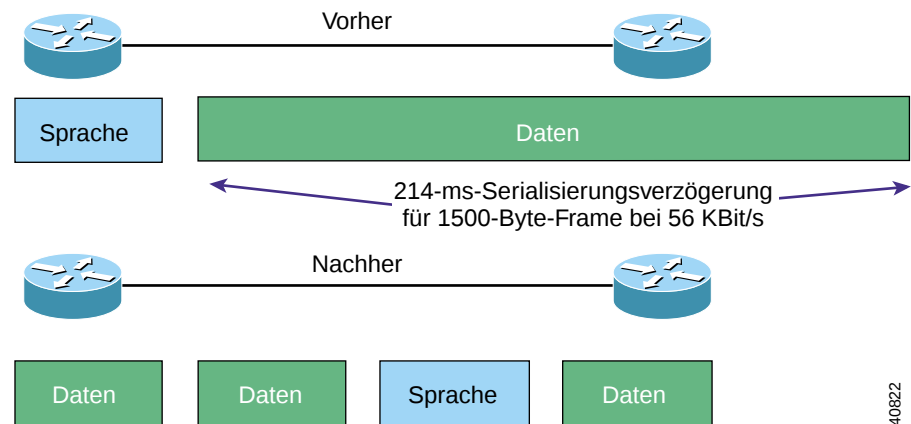


Hinweis

cRTP wird derzeit nur für Mietleitungen und Frame Relay-Medien unterstützt. Cisco IOS Version 12.1(2)T, das die Leistung stark verbessert, ist die empfohlene System-Software für cRTP.

Für Verbindungen mit niedriger Geschwindigkeit (weniger als 768 KBit/s.) müssen Techniken verwendet werden, die Verbindungsfragmentierung und -verschachtelung (Link Fragmentation and Interleaving = LFI) bieten. Hierdurch wird Jitter beschränkt, indem der Sprachverkehr daran gehindert wird, sich hinter großen Daten-Frames zu verzögern. Die drei Techniken, die für diesen Zweck verfügbar sind, sind Multilink-PPP (MLP) für serielle Punkt-zu-Punkt-Verbindungen, FRF.12 für Frame Relay sowie MLP über ATM für ATM-Verbindungen (verfügbar in Cisco IOS Version 12.1(5)T. In Abbildung 8-4 wird der allgemeine Betrieb von LFI dargestellt.

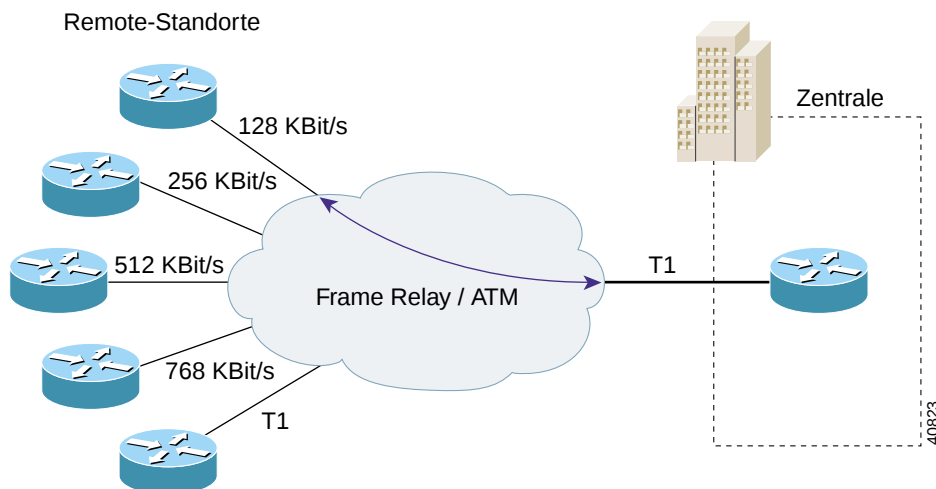
Abbildung 8-4 Verbindungsfragmentierungs- und -verschachtelungs (LFI)-Betrieb



Verkehrssteuerung

Verkehrssteuerung ist für Multiple Access, Non-Broadcast Netze wie z. B. ATM und Frame Relay erforderlich, bei denen die physische Zugriffsgeschwindigkeit zwischen zwei Endpunkten variiert. Die Verkehrssteuerungstechnologie lässt unterschiedliche Zugriffsgeschwindigkeiten zu. Im Fall von Frame Relay mit FRF.12 lässt die Verkehrssteuerung außerdem eine angemessene Begrenzung der Variation der Verzögerungen, auch Jitter genannt, zu. Für ATM ist aufgrund der Datenraten Fragmentierung in der Regel nicht erforderlich. In Abbildung 8-5 wird die Verkehrssteuerung mit Frame Relay und ATM dargestellt.

Abbildung 8-5 Verkehrssteuerung mit Frame Relay und ATM



Ideale Vorgehensweisen

In Tabelle 8-4 werden die empfohlenen Software-Mindestversionen für unternehmensweit implementierten Sprachverkehr über das WAN einschließlich der empfohlenen Parameter für QoS-Tools aufgeführt. Die derzeit empfohlenen Cisco IOS-Versionen ändern sich mit der Verfügbarkeit neuerer Versionen.

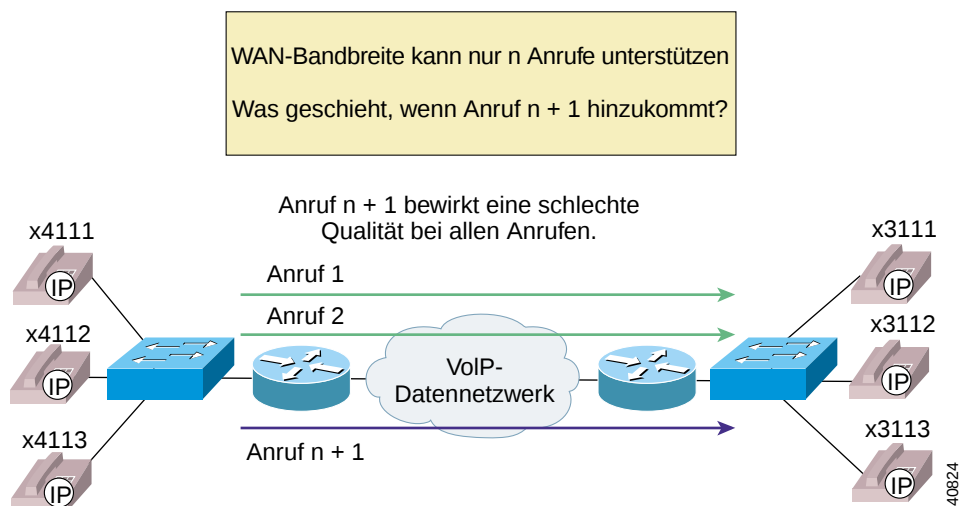
Tabelle 8-4 Empfohlene Cisco IOS-Versionen und QoS-Tools

Datenleitungstyp	Mindestens Cisco IOS Version	Klassifikation	Setzen von Prioritäten	LFI	Verkehrssteuerung
Serielle Leitungen	12.0(7)T	DSCP = EF für Sprache; DSCP = AF41 für Video; DSCP = AF31 für Sprachkontrollverkehr; andere Verkehrsklassen haben eine eindeutige Klassifizierung.	LLQ mit CBWFQ	MLP	Nicht verfügbar
Frame Relay	12.1(2)T	DSCP = EF für Sprache; DSCP = AF41 für Video; DSCP = AF31 für Sprachkontrollverkehr; andere Verkehrsklassen haben eine eindeutige Klassifizierung.	LLQ mit CBWFQ	FRF.12	Verkehr auf Committed Information Rate (CIR) steuern.
ATM	12.1(5)T	DSCP = EF für Sprache; DSCP = AF41 für Video; DSCP = AF31 für Sprachkontrollverkehr; andere Verkehrsklassen haben eine eindeutige Klassifizierung.	LLQ mit CBWFQ	MLP über ATM	Verkehr auf garantierten Anteil der Bandbreite steuern.
ATM und Frame Relay	12.1(5)T	DSCP = EF für Sprache; DSCP = AF41 für Video; DSCP = AF31 für Sprachkontrollverkehr; andere Verkehrsklassen haben eine eindeutige Klassifizierung.	LLQ mit CBWFQ	MLP über ATM und Frame Relay	Verkehr auf garantierten Anteil der Bandbreite auf der langsamsten Verbindung steuern.

Anrufzugangskontrolle

Anhand der Anrufzugangskontrolle muss sichergestellt werden, dass die Netzwerkressourcen nicht überlastet werden. Anrufe, die die festgelegte Bandbreite überschreiten, werden entweder auf eine andere Route umgeleitet, wie z. B. auf PSTN/ISDN, oder der Anrufer erhält das Besetztzeichen. In Abbildung 8-6 wird verdeutlicht, dass die Anrufzugangskontrolle unabhängig davon benötigt wird, ob es sich bei dem Implementierungsmodell zum Arbeitsbereich um Toll Bypass oder IP-Telefonie handelt.

Abbildung 8-6 Zum Schutz der WAN-Bandbreite erforderliche Anrufzugangskontrolle



Es gibt zwei Schemata, anhand derer Sprachanrufe über das WAN Anrufzugangskontrolle gewährleistet werden kann.

- Anrufzugangskontrolle per Gatekeeper – siehe "Anrufzugangskontrolle" auf Seite 6-3
- Standort-Anrufzugangs – siehe "Anrufzugangskontrolle" auf Seite 7-2



Catalyst DSP-Ressourcen

In diesem Kapitel werden Catalyst Digital Signal Processor (DSP)-Ressourcen beschrieben, wobei der Schwerpunkt auf zwei neuen Sprachmodulen für den Catalyst 4000 und den Catalyst 6000 liegt. Sie erfahren außerdem, wie diese Ressourcen bereitgestellt werden. Bei den neuen Modulen handelt es sich um das WS-X4604-GWY für den Catalyst 4000 und das WS-X6608-E1 für den Catalyst 6000. Sie können mit dem Cisco CallManager Version 3.0(5) verwendet werden. Sie stellen Conferencing- und Media Termination Point (MTP)-Transcoding-Services zur Verfügung und fungieren darüber hinaus als PSTN/ISDN-Gateway.

Erläuterungen zu Catalyst DSP-Ressourcen

Die DSP-Ressourcen der neuen Catalyst 4000- und Catalyst 6000-Gateway-Module bieten in erster Linie Hardwareunterstützung für die IP-Telefoniefunktionen des Cisco CallManagers. Diese Funktionen umfassen hardwarebasiertes Sprach-Conferencing, hardwarebasierte MTP-Unterstützung für zusätzliche Dienste und Transcoding-Services.

Bei Verwendung von Catalyst für das Conferencing werden Sprachkonferenzen über die Hardware unterstützt. Mithilfe von DSPs werden Voice-over-IP (VoIP)-Sitzungen in Time Division Multiplexing (TDM)-Signale konvertiert, die anschließend in Konferenzschaltungen mit mehreren Teilnehmern integriert werden können.

Der Catalyst MTP-Dienst kann entweder wie die Originalsoftware-MTP-Ressource oder als Transcoding-MTP-Ressource agieren. Ein MTP-Dienst bezeichnet die Möglichkeit, zusätzliche Dienste zur Verfügung zu stellen, wie beispielsweise Halten, Makeln und Konferenzen, wenn Gateways und Clients verwendet werden, die die H.323v2-Funktionen des OpenLogicalChannel und CloseLogicalChannel mit EmptyCapabilitiesSet nicht unterstützen. MTP ist als Softwarefunktion erhältlich, die mit dem Cisco CallManager oder auf einem eigenständigen Windows NT-Server ausgeführt werden kann. Wenn Sie MTP mit dem Cisco CallManager ausführen, werden 24 MTP-Sitzungen unterstützt. Wenn MTP auf einem eigenständigen Windows NT-Server ausgeführt wird, werden bis zu 48 MTP-Sitzungen unterstützt. Die neuen Catalyst Gateway-Module unterstützen dieselbe Funktionalität, sie stellen die Dienste jedoch über die Hardware zur Verfügung.

Transcoding ist nichts anderes als ein IP-to-IP-Voice-Gateway-Dienst. Ein Transcoding-Knoten kann G.711-Sprachsignale in Low-Bit-Rate (LBR)-komprimierte Sprachsignale wie G.729a konvertieren. Dies ist wichtig, um Anwendungen wie Integrated Voice Response (IVR), Voice Messaging und Konferenzschaltungen über langsame IP-WANs aktivieren zu können. MTP-Transcoding wird derzeit nur von Catalyst Sprach-Gateways unterstützt.

Tabelle 9-1 zeigt DSP-Ressourcen, die über die Catalyst Sprachdienstmodule konfiguriert werden können.

Tabelle 9-1 Catalyst DSP-Ressourcenmatrix

Catalyst Sprachmodule	PSTN/ISDN-Gateway-Sitzungen	Conferencing-Sitzungen	MTP-Transcoding-Sitzungen
Catalyst 4000 WS-X4604-GWY	Nur G.711 • 96 Anrufe	Nur G.711 • 24 Konferenzteilnehmer • Maximal 4 Konferenzen mit jeweils 6 Teilnehmern	In G.711 • 16 MTP-Transcoding-Sitzungen
Catalyst 6000 WS-6608-T1 oder WS-6608-E1	WS-6608-T1 • 24 Anrufe pro physikalischen DS1-Anschluss • 192 Anrufe pro Modul WS-6608-E1 • 30 Anrufe pro physikalischen DS1-Anschluss • 240 Anrufe pro Modul	G.711 oder G.723 • 32 Konferenzteilnehmer pro physikalischen Anschluss • Maximal 6 Teilnehmer pro Konferenz • 256 Konferenzteilnehmer pro Modul G.729 • 24 Konferenzteilnehmer pro physikalischen Anschluss • Maximal 6 Teilnehmer pro Konferenz • 192 Konferenzteilnehmer pro Modul	Folgende Kapazitäten gelten auch für gleichzeitiges Transcoding und Conferencing: G.723 in G.711 • 31 MTP-Transcoding-Sitzungen pro physikalischen Anschluss G.729 in G.711 • 248 Sitzungen pro Modul • 24 MTP-Transcoding-Sitzungen pro physikalischen Anschluss • 192 Sitzungen pro Modul

Catalyst Conferencing

Um IP-Telefoniesysteme in großen Unternehmensumgebungen zu skalieren, muss das hardwarebasierte Conferencing eingesetzt werden. Die neue Hardware für die Familie der Catalyst 4000- und Catalyst 6000-Switches wurde speziell für diesen Zweck entwickelt. Mit diesen neuen Catalyst Sprachmodulen ist Conferencing über Ihre Hardware möglich. Sie benötigen dazu keine Conferencing-Software auf einem Windows NT-Server im IP-Telefonienetzwerk.

Details zum Conferencing-Design

In den folgenden Punkten werden die Designmerkmale und die Anforderungen der neuen Catalyst Sprachmodule zusammengefasst:

- Unterstützung von maximal sechs Teilnehmern pro Konferenzschaltung.
- Das Catalyst 4000 WS-X4604-GWY-Modul unterstützt 24 Konferenzteilnehmer pro Modul.
- Das Catalyst 4000 WS-X4604-GWY-Modul unterstützt Conferencing ausschließlich für G.711-Sprachsignale. Mithilfe von Transcoding können G.729a- oder G.723.1-Signale für Konferenzschaltungen in G.711-Signale konvertiert werden.
- Die Catalyst 6000 WS-X6608-T1- oder WS-X6608-E1-Module unterstützen 32 G.711- oder G.723-Konferenzteilnehmer pro physikalischen Anschluss (256 pro Modul) oder 24 G.729-Konferenzteilnehmer pro physikalischen Anschluss (192 pro Modul).
- Die Catalyst 6000 WS-X6608-T1- oder WS-X6608-E1-Module können sowohl komprimierte als auch nicht komprimierte VoIP-Konferenzschaltungen unterstützen.
- Jeder Cisco CallManager benötigt eigene Konferenz- und MTP-Transcoding-Ressourcen, da die DSP-Ressourcen sich immer nur bei einem Cisco CallManager anmelden können. Cisco CallManager können DSP-Ressourcen nicht gemeinsam nutzen.

Das Catalyst 4000-Modul WS-X4604-GWY unterstützt bis zu vier Konferenzschaltungen gleichzeitig mit jeweils sechs Teilnehmern. Das Catalyst 6000-T1- oder E1-PSTN/ISDN-Gateway-Modul WS-X6608 unterstützt ebenfalls Konferenzschaltungen. Wenn Sie das WS-X6608-Modul einem Cisco T1- oder E1-AVVID-Gateway hinzugefügt haben, kann es für das Conferencing für jeden Anschluss einzeln konfiguriert werden. Das Catalyst 6000-Conferencing-Modul unterstützt maximal sechs Konferenzteilnehmer pro Konferenz. Pro konfigurierten logischen Anschluss sind maximal 32 G.711- oder G.723-Konferenzteilnehmer gleichzeitig zulässig. Das ergibt maximal 256 Konferenzteilnehmer pro Modul bei G.711- oder G.723-Anrufen.

In Tabelle 9-1 finden Sie eine Übersicht über die Anzahl der Konferenzschaltungen, die für jedes Modul zulässig sind.

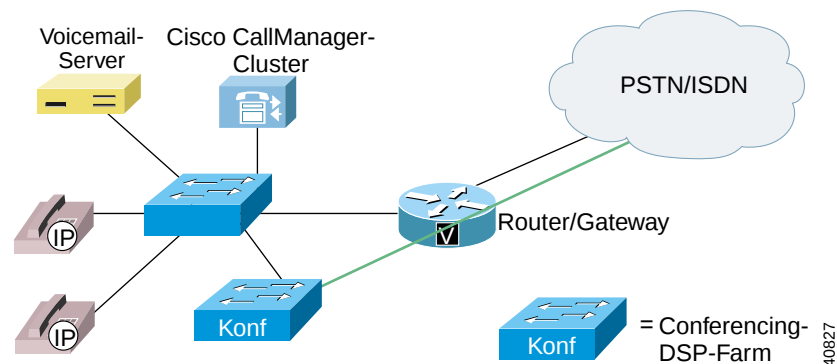
Sowohl das WS-X4604-GWY- als auch das WS-X6608-T1-Modul (bzw. WS-X6608-E1) verwenden für das Conferencing oder für Transcoding-Services das Skinny Station Protocol zur Kommunikation mit dem Cisco CallManager. Die Catalyst 6000-Conferencing-Lösung unterstützt sowohl komprimierte als auch nicht komprimierte Konferenzteilnehmer.

Mit dem Catalyst 4000 können nur G.711-Anrufe, d. h. nicht komprimierte Anrufe, zu einer Konferenzschaltung zusammengeführt werden. Wenn der Conferencing-Dienst sich mit dem Skinny Station Protocol beim Cisco CallManager anmeldet, gibt er an, dass nur G.711-Sprachanrufe verbunden werden können. Falls komprimierte Anrufe an einer Konferenz teilnehmen sollen, erstellt der Cisco CallManager zunächst eine Verbindung zu einem Transcoding-Port. Dadurch wird der komprimierte Sprachanruf in einen G.711-Sprachanruf konvertiert. Sobald die G.711-Verbindungen einer bestimmten Conferencing-Sitzung zugewiesen sind (maximal sechs Teilnehmer pro Konferenzschaltung), wird der Anruf in TDM-Signale konvertiert und an die Summenlogik weitergeleitet, die die einzelnen Signale kombiniert. Im Gegensatz zum WS-X6608-x1-Modul, das eine Konferenzschaltung zwischen allen Konferenzteilnehmern zulässt, nehmen beim Catalyst 4000 WS-X4604-GWY-Modul nur die drei Hauptredner an der Konferenzschaltung teil. Das WS-X4604-GWY-Modul überprüft laufend, wer die Hauptredner sind und passt die Konferenzschaltung entsprechend an. Dabei ist die Sprachlautstärke entscheidend, Hintergrundgeräusche werden nicht berücksichtigt.

Beachten Sie beim Konfigurieren von Conferencing-Diensten auch Folgendes:

- Wenn Sie ein Unternehmen mit Konferenzanschlüssen ausstatten, ermitteln Sie zunächst die Anzahl der Anrufer, die in Zukunft versuchen werden, von einer komprimierten Cisco CallManager-Region aus an einer Konferenzschaltung teilzunehmen. Wenn Sie die Anzahl der komprimierten Anrufer ermittelt haben, können Sie genau bestimmen, wieviele MTP-Transcoding-Ressourcen Sie benötigen.
- Konferenz-Bridges können sich immer nur bei einem Cisco CallManager anmelden, und Cisco CallManager können DSP-Ressourcen nicht gemeinsam nutzen. Deshalb müssen Sie separate Conferencing-Module für jeden Cisco CallManager im Cluster konfigurieren.

Abbildung 9-1 zeigt die Komponenten, die beim Catalyst Conferencing verwendet werden.

Abbildung 9-1 Catalyst Conferencing

Conferencing-Einschränkungen

Folgende Einschränkungen bestehen für das Catalyst Conferencing:

- Beim Conferencing mit dem Catalyst 4000-Modul werden ausschließlich G.711-Verbindungen unterstützt, sofern kein MTP-Transcoding verwendet wird.
- Beim Conferencing mit dem Catalyst 6000-Modul können Port-Grenzen nicht überschritten werden.
- Für jeden Cisco CallManager muss eine eigene Conferencing-Ressource konfiguriert werden.

Konferenzschaltungen in einem IP-WAN werden im nächsten Abschnitt, "Catalyst MTP-Transcoding" beschrieben.

Catalyst MTP-Transcoding

Wenn ein WAN Teil einer IP-Telefonieimplementierung ist, ist eine Sprachkomprimierung erforderlich. In den vorherigen Beispielen in diesem Dokument waren alle Campus-orientierten Sprachsignale nicht komprimiert (G.711). Dadurch wurde die bestmögliche Qualität erzielt, und gleichzeitig traten die wenigsten Komplikationen auf. Sobald ein WAN-Netzwerk implementiert wird, empfiehlt sich die Sprachkomprimierung. Hierbei stellt sich die Frage, wie WAN-Benutzer das Conferencing oder IP-basierte Anwendungen einsetzen, die nur G.711-Sprachverbindungen unterstützen. Die Lösung ist die hardwarebasierte MTP-Transcoding, mit der komprimierte Sprachsignale in G.711-Signale konvertiert werden.

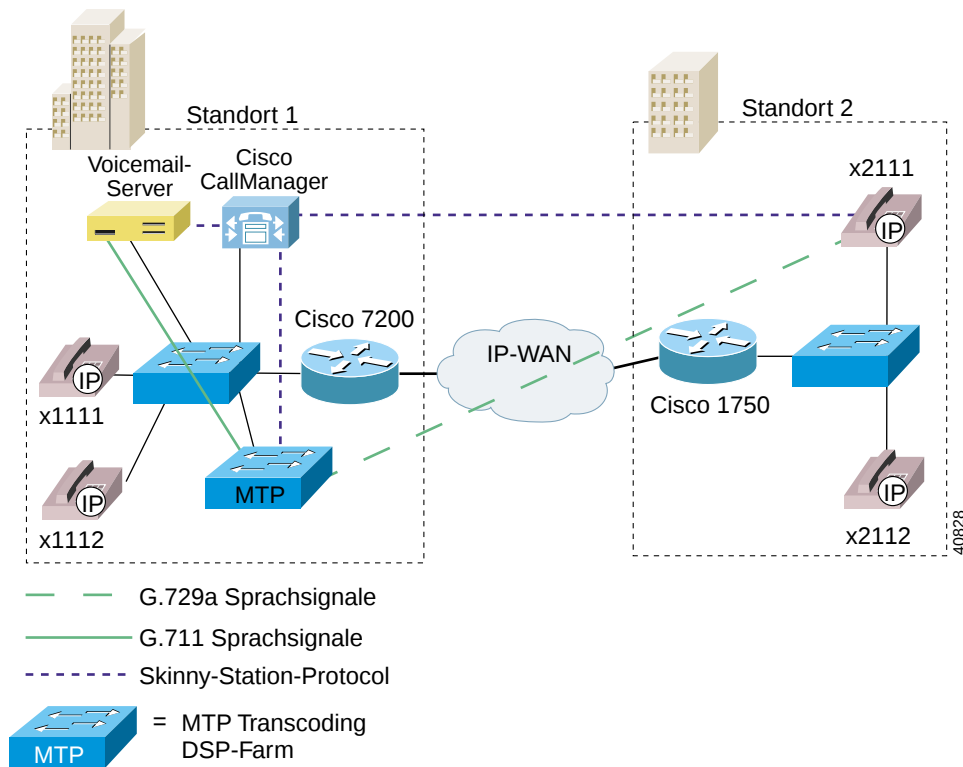
Details zum MTP-Transcoding-Design

In den folgenden Punkten werden die Designmerkmale und die Anforderungen des MTP-Transcoding zusammengefasst:

- Stellen Sie für die Anzahl der IP-WAN-Anrufer bei G.711-Endpunkten eine ausreichende Anzahl an MTP-Transcoding-Ressourcen zur Verfügung.
- Das Catalyst 4000 WS-X4604-GWY-Modul unterstützt 16 Transcoding-Sitzungen pro Modul.
- Die Catalyst 6000 WS-X6608-T1- oder WS-X6608-E1-Module unterstützen 31 G.723- oder G.711-Transcoding-Sitzungen pro physikalischen Anschluss (248 pro Modul) oder 24 G.729-in-G.711-Transcoding-Sitzungen pro physikalischen Anschluss (192 pro Modul).
- Transcoding wird nur in Low-Bit-Rate-to-High-Bit-Rate-Konfigurationen (G.729a oder G.723.1 in G.711) oder umgekehrt unterstützt.
- Jeder Cisco CallManager benötigt eigene MTP-Transcoding-Ressourcen.
- Jeder Transcode besitzt einen eigenen Jitter-Puffer von 20-40 ms.

IP-to-IP-Packet-Transcoding und -Sprachkomprimierung

Die Sprachkomprimierung zwischen IP-Telefonen kann problemlos mithilfe von Regionen und Standorten im Cisco CallManager konfiguriert werden. Catalyst Conferencing und manche Anwendungen unterstützen derzeit jedoch nur G.711-Verbindungen, also nicht komprimierte Verbindungen. Aus diesem Grund wurde MTP-Transcoding oder die Packet-to-Packet-Gateway-Funktionalität in zwei der neuen Module für den Catalyst 4000 und Catalyst 6000 integriert. Ein Packet-to-Packet-Gateway ist ein Gerät mit DSPs, das für Transcoding von Sprachsignalen mithilfe von verschiedenen Komprimierungsalgorithmen verantwortlich ist. Beispiel: Wenn ein Benutzer mit einem IP-Telefon an einem Remote-Standort einen Benutzer in der Zentrale anruft, weist der Cisco CallManager das Remote-IP-Telefon an, nur für den WAN-Anruf komprimierte Sprachsignale (G.729a) zu verwenden. Wenn der angerufene Teilnehmer in der Zentrale nicht verfügbar ist, wird der Anruf unter Umständen an eine Anwendung weitergeleitet, die nur G.711 unterstützt. In diesem Fall transcodiert ein Packet-to-Packet-Gateway die G.729a-Sprachsignale in G.711-Sprachsignale, damit eine Nachricht beim Voice Messaging Server hinterlassen werden kann. Siehe Abbildung 9-2.

Abbildung 9-2 IP-to-IP-Packet-Gateway-Transcoding für WAN mit zentraler Anrufverarbeitung


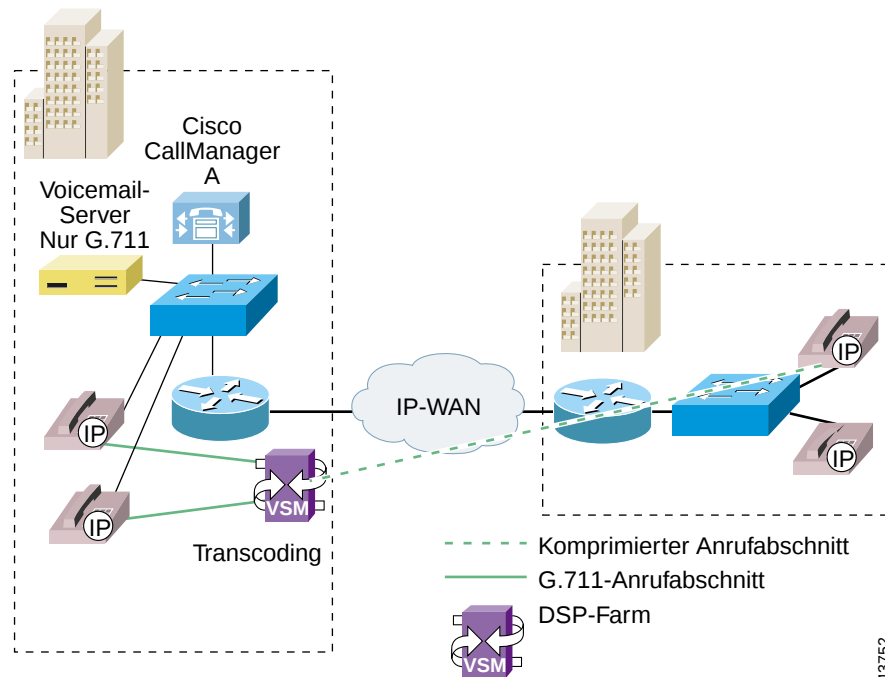
Sprachkomprimierung, IP-to-IP-Packet-Transcoding und Conferencing

Das Verbinden von Standorten über ein IP-WAN mit dem Zweck, eine Konferenzschaltung herzustellen, ist ein komplexes Szenario. In diesem Szenario sind die Catalyst Module sowohl für das Conferencing als auch für die IP-to-IP-Transcoding zum Dekomprimieren der WAN-IP-Sprachverbindung verantwortlich. In Abbildung 9-3 nimmt ein Remote-Benutzer an einer Konferenzschaltung teil, die über die Zentrale erfolgt. Für diese Konferenzschaltung mit drei Teilnehmern werden sieben DSP-Kanäle des Catalyst 4000-Moduls und drei DSP-Kanäle des Catalyst 6000-Moduls verwendet. In folgender Auflistung wird beschrieben, wie die Kanäle im Einzelnen genutzt werden:

- Catalyst 4000
 - Ein DSP-Kanal zur Konvertierung des IP-WAN-G.729a-Sprachanrufs in einen G.711-Sprachanruf.
 - Drei Conferencing-DSP-Kanäle zur Konvertierung der G.711-Signale in TDM für den Summierungs-DSP.
 - Drei Kanäle vom Summierungs-DSP, um die drei Anrufer miteinander zu verbinden.

- Catalyst 6000
 - Es werden drei Conferencing-DSP-Kanäle verwendet. Mit dem Catalyst 6000 werden alle Sprachsignale an einen logischen Conferencing-Anschluss gesendet, über den das gesamte Transcoding und die gesamte Summierung erfolgt.

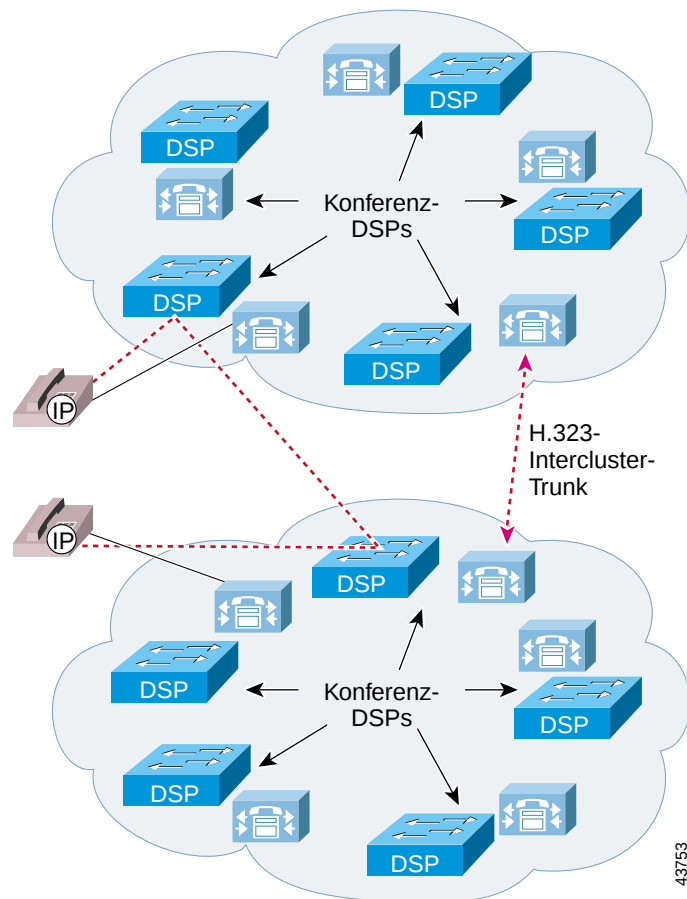
Abbildung 9-3 Zentrales MTP-Transcoding und Conferencing für WAN mit mehreren Standorten



43752

IP-to-IP-Packet-Transcoding über Intercluster-Trunks

H.323v2-Intercluster-Trunks werden zur Verbindung von Cisco CallManager-Clustern verwendet. Wenn das Transcoding zwischen Clustern erforderlich ist, werden die Intercluster-Trunks mit MTP konfiguriert. In diesem Fall werden alle Anrufe zwischen Clustern über das MTP/Transcoding-Gerät in jedem Cluster geleitet. Beim Catalyst 6000-Modul wird immer der MTP-Dienst verwendet, unabhängig davon, ob für den jeweiligen Intercluster-Anruf das Transcoding erforderlich ist. Im Gegensatz zu früheren Versionen unterstützt der Cisco CallManager Version 3.0 (und höher) Verbindungen mit komprimierten Sprachanrufen über den MTP-Dienst, wenn ein Hardware-MTP verwendet wird. Abbildung 9-4 zeigt einen Intercluster-Anruffluss.

Abbildung 9-4 Intercluster-Anruffluss mit Transcoding

Die folgende Auflistung enthält Details zu Intercluster-MTP/Transcoding:

- Wenn das Transcoding zwischen Cisco CallManager-Clustern erforderlich ist, muss der H.323-Intercluster-Trunk mit einer MTP-Ressource konfiguriert werden.
- Alle Anrufe zwischen Cisco CallManager-Clustern werden über MTPs geleitet.
- Ausgehende Intercluster-Anrufe verwenden eine MTP/Transcoding-Ressource des Cisco CallManagers, von dem der Anruf stammt.
- Eingehende Intercluster-Anrufe verwenden die MTP/Transcoding-Ressource des Cisco CallManagers, der den Eingangs-Intercluster-Trunk abschließt.
- Weitere DSP-MTP/Transcoding-Ressourcen sollten Cisco CallManagern zugewiesen werden, die H.323-Intercluster-Trunks abschließen.

Einschränkungen der MTP-Transcoding

Folgende Einschränkungen bestehen für die Catalyst MTP-Transcoding:

- Das Catalyst MTP-Transcoding unterstützt nur die LBR-codec-to-G.711-Konvertierung und umgekehrt. LBR-to-LBR-codec-Konvertierungen werden nicht unterstützt.
- Beim Transcoding mit dem Catalyst 6000-Modul können Anschlussgrenzen nicht überschritten werden.
- Für jeden Cisco CallManager muss eine eigene MTP-Transcoding-Ressource konfiguriert werden.
- Wenn das Transcoding zwischen Cisco CallManager-Clustern erforderlich ist, muss der H.323-Intercluster-Trunk mit einer MTP-Ressource konfiguriert werden. Alle Anrufe zwischen Cisco CallManager-Clustern werden über MTPs geleitet.
- Wenn alle n MTP-Transcoding-Sitzungen genutzt werden und versucht wird, eine Verbindung n + 1 herzustellen, wird der nächste Anruf ohne MTP-Transcoding-Ressource abgeschlossen. Wenn für diesen Anruf die MTP-Softwarefunktion verwendet werden soll, mit der zusätzliche Dienste bereitgestellt werden, wird die Verbindung zwar aufgebaut, der Versuch, zusätzliche Dienste zu nutzen, schlägt jedoch fehl, und der Anruf wird unter Umständen unterbrochen. Wenn für den Anruf die Transcoding-Funktionen verwendet werden, wird eine Verbindung zwar direkt hergestellt, es sind jedoch keine Töne hörbar.

In Tabelle 9-1 finden Sie eine Übersicht über die Transcoding-Funktionen jedes einzelnen Moduls.

Catalyst 4000-Sprachdienste

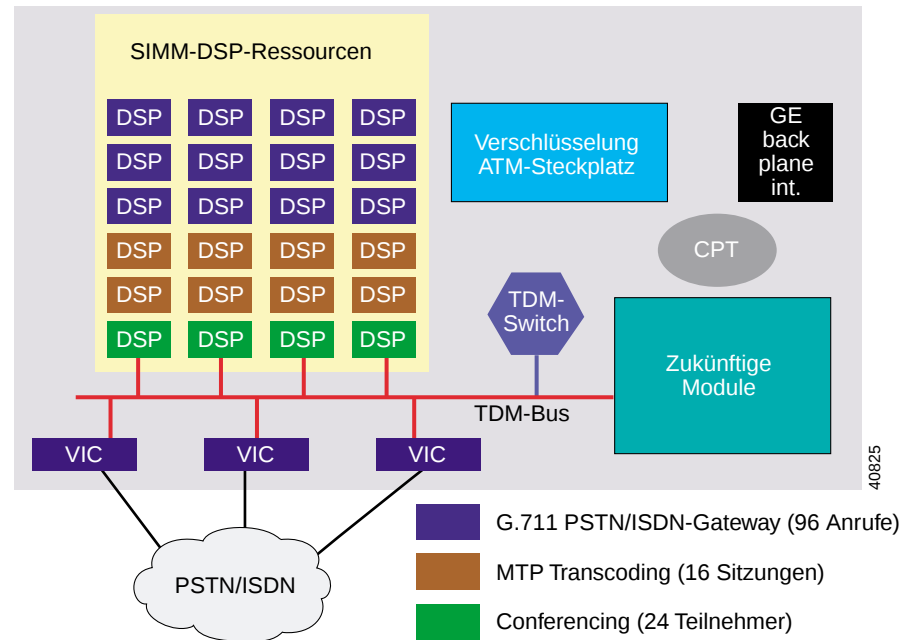
Das PSTN/ISDN-Gateway- und Sprachdienstmodul für die Catalyst 4003- und 4006-Switches unterstützt drei analoge Voice Interface Cards (VICs) mit jeweils zwei Anschlüssen oder eine T1/E1-Karte mit zwei Anschlüssen und zwei analoge VICs. Die VIC-Schnittstellen können beliebig kombiniert werden aus Foreign Exchange Office (FXO), Foreign Exchange Station (FXS) und Ear & Mouth (E&M). Dieses Modul unterstützt darüber hinaus Conferencing- und Transcoding-Services, sofern es über die Command Line Interface (CLI) als IP-Telefonie-Gateway konfiguriert wird.

Das Catalyst 4000-Sprach-Gateway-Modul kann entweder im Toll Bypass- oder im Gateway-Modus konfiguriert werden. Die Conferencing- und Transcoding-Ressourcen können jedoch nur im Gateway-Modus konfiguriert werden. Sobald der Gateway-Modus aktiviert ist, werden die 24 DSPs (4 SIMMs mit jeweils 6 DSPs) des Moduls automatisch aufgeteilt:

- PSTN/ISDN-Gateway: 96 Kanäle G.711-Sprachsignale und
- Conferencing: 24 Kanäle G.711-Conferencing und
- MTP-Transcoding: 16 Kanäle LBR-G.711-Transcoding

Abbildung 9-5 zeigt eine physikalische Darstellung des Catalyst 4000-Sprach-Gateway-Moduls im Gateway-Modus.

Abbildung 9-5 Catalyst-Sprach-Gateway-Modul im Gateway-Modus



Der Gateway-Modus ist die Standardkonfiguration. In zukünftigen Versionen des Catalyst 4000-Moduls können Sie die Conferencing-Transcoding-Verhältnisse über das CLI ändern.

Folgende Konfigurationshinweise beziehen sich auf das Catalyst 4000-Modul:

- Das WS-X4604-GWY verwendet eine Cisco IOS-Schnittstelle für die erste Gerätekonfiguration. Alle folgenden Konfigurationen für die Sprachfunktionen erfolgen im Cisco CallManager. Das Catalyst 4000-Modul verwendet für alle PSTN/ISDN-Gateway-Funktionen H.323v2 und ist wie ein Cisco IOS-Gateway konfiguriert. Fügen Sie das Catalyst 4000-Gateway einfach im Cisco CallManager-Konfigurationsbildschirm als H.323-Gateway hinzu.
- Das WS-X4604-GWY kann als PSTN/ISDN-Gateway (Toll Bypass-Modus) sowie als hardwarebasierter Transcoder oder als Konferenz-Bridge (Gateway-Modus) fungieren. Geben Sie einen oder beide der folgenden CLI-Befehle ein:

```
Voicecard Conference
Voicecard Transcode
```

- Das WS-X4604-GWY benötigt zusätzlich zur IP-Adresse des Cisco CallManagers eine eigene lokale IP-Adresse. Es empfiehlt sich außerdem, eine Loopback-IP-Adresse für das lokale Signaling Connection Control Part (SCCP) anzugeben.
- Sowohl für den Conferencing- als auch für den MTP-Transcoding-Service kann ein primärer, sekundärer und tertiärer Cisco CallManager definiert werden.

Catalyst 6000-Sprachdienste

Das WS-6608-E1 entspricht dem Modul, das E1-PSTN/ISDN-Gateway-Unterstützung für den Catalyst 6000 bietet. Dieses Modul verfügt über acht Channel Associated Signaling (CAS)- oder PRI-Schnittstellen, jede mit eigener CPU und eigenen DSPs. Wenn die Karte über den Cisco CallManager als Sprach-Gateway hinzugefügt wurde, kann sie als Conferencing- oder als MTP-Transcoding-Knoten konfiguriert werden. Jeder Anschluss ist von den anderen Anschlüssen des Moduls unabhängig. Jeder Anschluss kann entweder nur als PSTN/ISDN-Gateway-Schnittstelle, als Conferencing-Knoten oder als MTP-Transcoding-Knoten konfiguriert werden. In den meisten Konfigurationen wird für jeden Conferencing-Knoten ein Transcoding-Knoten konfiguriert.



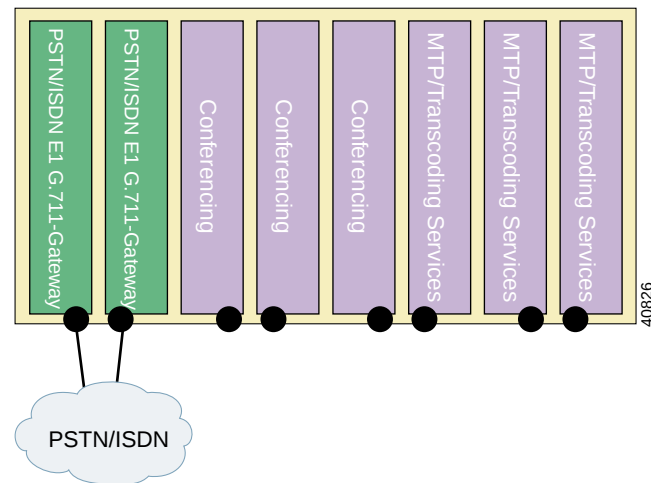
Hinweis Conferencing- und MTP-Transcoding-Service können Anschlussgrenzen nicht überschreiten.

Um als PSTN/ISDN-Gateway, als Conferencing-Ressource oder als MTP-Transcoding-Ressource fungieren zu können, benötigt jeder Anschluss des Moduls eine eigene IP-Adresse. Es kann entweder eine statische IP-Adresse für den Anschluss konfiguriert oder eine IP-Adresse vom DHCP bereitgestellt werden. Wenn eine statische IP-Adresse eingegeben wird, muss auch eine TFTP-Serveradresse angegeben werden, denn die Anschlüsse erhalten alle Konfigurationsinformationen aus der heruntergeladenen TFTP-Konfigurationsdatei. Wenn die einzelnen Anschlüsse einmal über die Cisco CallManager-Schnittstelle konfiguriert wurden, kann jeder eine der folgenden Konfigurationen unterstützen:

- PSTN/ISDN-Gateway-Modus: 24 Sitzungen über das WS-6608-E1-Modul; 30 Sitzungen über das WS-6608-E1-Modul
- Conferencing-Modus: 32 Conferencing-Sitzungen für G.711 oder G.723; 24 Conferencing-Sitzungen für G.729
- MTP-Modus: 31 MTP-Transcoding-Sitzungen für G.723 in G.711; 24 MTP-Transcoding-Sitzungen für G.729 in G.711

Abbildung 9-6 zeigt eine mögliche Konfiguration des Catalyst 6000-Sprach-Gateway-Moduls. Bei dem Modul im Diagramm sind zwei der acht Anschlüsse im PSTN/ISDN-Gateway-Modus konfiguriert, drei Anschlüsse im Conferencing-Modus und drei Anschlüsse im MTP-Transcoding-Modus.

Abbildung 9-6 Catalyst 6000-Sprach-Gateway-Modul





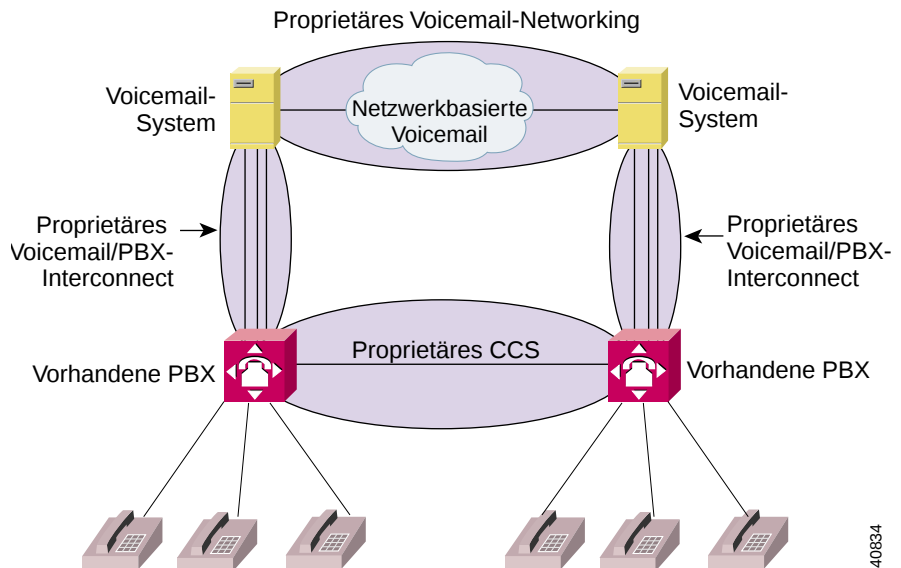
Migration auf ein IP-Telefonie-Netzwerk

In diesem Kapitel wird erläutert, wie ein Unternehmen seine konventionelle Nebenstellenanlage (PBX) mit zugehörigen Systemen (hauptsächlich Voice Messaging (Sprachmitteilungen)) auf ein IP-Telefonie-Netzwerk umstellen kann. Es werden vier Umstellungsmodelle vorgestellt, die unterschiedliche Funktionssätze umfassen, und die Schritte für jedes dieser Modelle werden erläutert.

Netzwerkmodelle

Konventionelle Sprachnetze, die in IP-Netzwerke umgewandelt werden sollen, enthalten mindestens eine PBX-Anlage, häufig jedoch mehrere PBX-Anlagen, die sich an unterschiedlichen Standorten befinden. Ein Netzwerk aus PBX-Anlagen kann ein spezialisiertes, firmeneigenes Netzwerkprotokoll verwenden, anhand dessen die Funktionen allen PBX-Anlagen verfügbar gemacht werden.

Wenn Voice Messaging einen Teil des Sprachnetzes darstellt, sind die Voice Messaging-Systeme mit der PBX-Anlage über ein Protokoll und eine Hardware-Schnittstelle verbunden. Wenn es in einem Netzwerk mehrere Voice Messaging-Systeme gibt, können sie so miteinander vernetzt sein, dass sie dem Benutzer wie ein einziges Voice Messaging-System erscheinen. In der Regel werden die Voice Messaging-Systeme über firmeneigene Protokolle miteinander verbunden und vernetzt. Siehe Abbildung 10-1.

Abbildung 10-1 Geschlossene im Vergleich zu offenen Protokollen in einem Sprachnetz

40834

PBX- und Voice Messaging-Schnittstellen und -Protokolle

Wenn ein IP-Netzwerk in eine solche Umgebung eingeführt wird, können die Benutzer des IP-Netzwerks in der Regel IP-Funktionen nutzen, wenn sie andere Benutzer des IP-Netzwerks anrufen. Ebenso können die PBX-Benutzer die Funktionen der PBX nutzen, wenn sie andere PBX-Benutzer anrufen. Anrufe zwischen Benutzern des IP-Netzwerks und der PBX können jedoch nur einen Teilsatz der Funktionen, die von jedem System geboten werden, nutzen; dieser Teilsatz wird durch die Komplexitätsstufe der Voice Interface des IP-Netzwerks und der PBX bestimmt. Ebenso können Benutzer des IP-Netzwerks zwar auf das Voice Messaging-System hinter der PBX-Anlage zugreifen, in der Regel jedoch nur beschränkte Funktionen nutzen. Wenn IP-Mitteilungen verwendet werden, können Sie eventuell zu einem gewissen Grad mit dem konventionellen Voice Messaging-System vernetzt werden. Welche dieser Funktionen in welchem Maße unterstützt werden, hängt von den Protokollen und Schnittstellen ab, über die das IP-Netzwerk eine Verbindung zum herkömmlichen Voice Messaging-System herstellen kann.

In Tabelle 10-1 werden einige der häufiger verwendeten Schnittstellen und Protokolle für die Vernetzung der PBX und Voicemail-System-Netzwerken zusammengefasst.

Tabelle 10-1 Schnittstellen und Protokolle für die Vernetzung der PBX und Voicemail System-Netzwerke

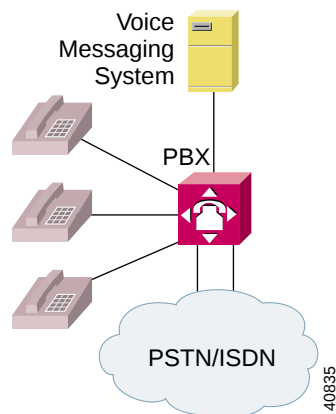
Hersteller	PBX-to-PBX-Protokolle	PBX-to-Voicemail-Schnittstellen	Voicemail-to-Voicemail-Netzwerk
Cisco	PRI, QSIG, CAS	SMDI, analog	AMIS-A ¹
Avaya	PRI, DCS, QSIG	Digitalsatzemulation Proprietär, X.25/C-LAN	Octelnet AUDIX Digital Networking AMIS-A
Nortel	PRI, MCDN, DPNSS, QSIG	Proprietär (IVMS)	Meridian Mail Networking VPIM AMIS-A
Siemens	PRI, CorNet, DPNSS, QSIG	BRI mit proprietären Erweiterungen	PhoneMail Fernstreckenvernetzung (Long Distance Networking = LDN) AMIS-A
Alcatel	PRI, DCS, QSIG	Unbekannt	Unbekannt
NEC	PRI, CCIS, QSIG	Proprietäre Meldungszentrumsschnittstelle (Message Center Interface = MCI)	Unbekannt

1. Cisco unterstützt AMIS-A auf Cisco uOne ab Version 5.0E.

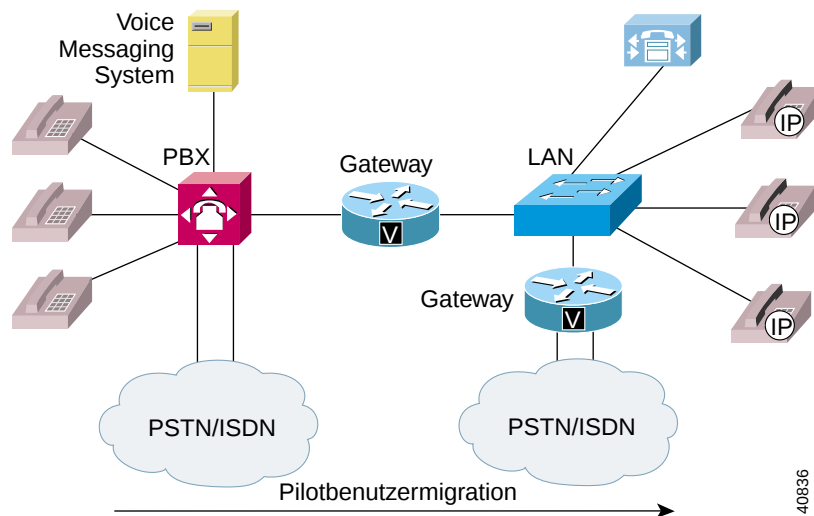
Während konventionelle Sprachnetze intern proprietäre, geschlossene Protokolle verwenden, können sie nur über offene Protokolle an IP-Netzwerke angeschlossen werden. Dasselbe gilt, wenn Geräte unterschiedlicher Hersteller miteinander vernetzt werden sollen. PRI (oder QSIG) zwischen PBX-Anlagen, das analoge Simplified Message Desk Interface (SMDI) zwischen PBX-Anlagen und Voicemail-Systemen und Audio Messaging Interchange Specification (AMIS) zwischen Sprachsystemen sind die leistungstärksten verfügbaren Schnittstellen.

Einfache Umstellungssequenz auf ein IP-Netzwerk

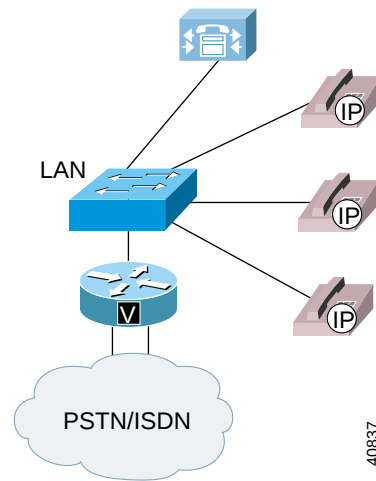
In den folgenden drei Abbildungen werden die Phasen der Migration von einem konventionellen Sprachnetzwerk auf ein Nur-IP-Netzwerk verdeutlicht. In Abbildung 10-2 wird das ursprüngliche konventionelle Sprachnetzwerk gezeigt.

Abbildung 10-2 Ursprüngliches konventionelles Sprachnetzwerk


In Abbildung 10-3 wird die Umstellungsphase dargestellt, bei der Benutzer in Blöcken der PBX auf das IP-Netzwerk übergehen.

Abbildung 10-3 Umstellungsphase


In Abbildung 10-4 wird das Netzwerk nach Abschluss der Migration und Außerbetriebnahme der PBX gezeigt.

Abbildung 10-4 Migration abgeschlossen

In der Regel erfolgt die Migration von einem konventionellen Sprachnetzwerk auf ein IP-Netzwerk in mehreren Stufen wie Folgt:

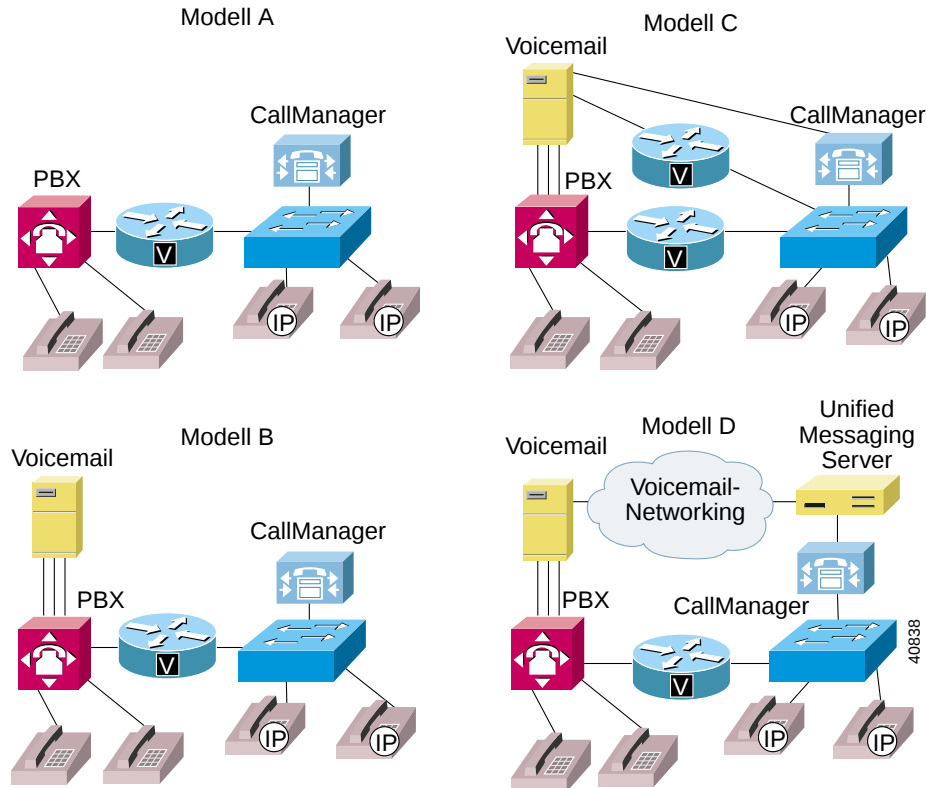
-
- Schritt 1** Pilotphase – Das IP-Netzwerk wird eingeführt, eine sehr begrenzte Anzahl von Benutzern erhält IP-Dienste. In dieser Erstphase der Nutzung, die häufig auch die Telekommunikations- oder IT-Gruppe umfasst, behalten die Benutzer manchmal ihre konventionellen Telefone neben den IP-Telefonen. In der Regel stellen sie jedoch gleich auf das neue System um. Wenn der Pilotversuch einige Wochen stabil und zufriedenstellend gelaufen ist, kann er ausgeweitet werden.
- Schritt 2** Migration eines Benutzerblocks – Ein Benutzerblock wird (in der Regel über das Wochenende) vom konventionellen Sprachnetzwerk auf das IP-Netzwerk umgestellt. Der Block kann als geographische Gruppe, als eine Gruppe, die sich einen Block von Directory Numbers (DNs) oder als Interessengemeinschaft, beispielsweise die Einkaufsabteilung, ausgewählt werden.
- Schritt 3** Migration weiterer Benutzerblöcke – Die Anzahl der Benutzer, die in einem Block umgestellt werden, hängt davon ab, wieviele Benutzer das Telekommunikationspersonal an einem Wochenende maximal umstellen kann sowie davon, wieviele Wochenenden die Telekommunikationsabteilung zu arbeiten bereit ist. In der Regel sollte die Migration so schnell wie möglich abgeschlossen werden.
-

Natürlich müssen bei der Planung einer Migration auch eine Reihe weiterer Überlegungen in Betracht gezogen werden, wie z. B. die Frage, ob die Benutzer ihre VNs behalten oder neue zugewiesen bekommen sollen, Benutzerschulungen, Rechnungssysteme, Sonderfunktionen, Bereitschaftspläne etc.

Referenzmodelle für Umstellungskonfigurationen

In diesem Abschnitt werden die vier grundlegenden Umstellungskonfigurationen behandelt. Diese Modelle sind in Abbildung 10-5 dargestellt.

Abbildung 10-5 Umstellungsmodelle



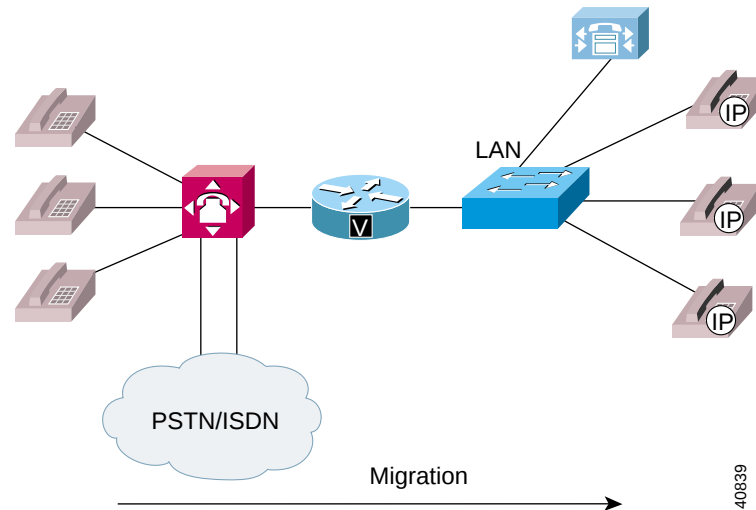
Die in Abbildung 10-5 gezeigten Modelle haben die folgenden Charakteristika:

- Modell A beschreibt die einfachste Situation; es betrifft nur die PBX-Dienste und schließt Voice Messaging aus.
- Modell B umfasst ein Voice Messaging-System hinter der PBX und geht davon aus, dass das Voicemail-System keine offene Schnittstelle für die Verbindung über ein IP-Netzwerk bietet. Daher muss der gesamte Voicemail-Verkehr vom IP-Netzwerk durch die PBX-Anlage geleitet werden.
- Modell C umfasst ein Voice Messaging-System, das eine Verbindung über ein IP-Netzwerk herstellen kann, sodass den IP-Benutzern eine stärkere Funktionalität zur Verfügung steht.
- Modell D führt einheitliche IP-Mitteilungen gleichzeitig wie die IP-Telefonie ein und ersetzt so die konventionelle Kombination aus PBX und Voice Messaging-System.

Detaillierte Beschreibung von Modell A

In Abbildung 10-6 wird die Topologie für Modell A dargestellt, die ein PBX, jedoch kein Voice Messaging umfasst.

Abbildung 10-6 Umstellungsmodell A – nur PBX



Modell A wirft zwei wichtige Fragen auf:

- Sollen die Trunk-Leitungen der PBX bis zum Abschluss der Migration erhalten bleiben, oder sollen die Trunk-Leitungen zusammen mit den Benutzern auf das IP-Netzwerk umgestellt werden?
- Welche Art der Verbindung soll zwischen der PBX und dem IP-Netzwerk verwendet werden?

In Tabelle 10-2 wird der Funktionssatz aufgeführt, der von den verschiedenen Verbindungsarten unterstützt wird.

Tabelle 10-2 Verbindungsarten und unterstützte Funktionssätze

Verbindungsart	Anrufer-nummer	Angerufene Nummer	Anrufer-name	Umleitungs-grund	MWI ¹ Ein/Aus	Beidseitige Einleitung	Relative Kosten
FXO/FXS	Nein	Ja	Nein	Nein	Nein	Nein	Sehr klein
E&M/R2	Nein	Ja	Nein	Nein	Nein	Ja	Klein
BRI/PRI	Ja	Ja	Ja	Nein	Nein	Ja	Mittel bis groß
QSIG	Ja	Ja	Ja	Ja	Ja	Ja	Groß
Digitalatsatzemulation	Ja	Ja	Ja	Ja	Nein	Ja	Mittel
PBX-WAN-Protokoll	Ja	Ja	Ja	Ja	Ja	Ja	Groß

1. MWI = Message Waiting Indicator

Die folgenden Punkte erläutern kurz die Wichtigkeit der Funktionen in Tabelle 10-2:

- Die Anrufernummer kann nicht nur am angerufenen Telefon angezeigt werden, sondern auch zur Rechnungsstellung und für Voicemail-Zwecke verwendet werden.
- Die angerufene Nummer ist wichtig, wenn der empfangende Switch den Anruf direkt an ein Telefon leitet, anstatt ihn erst bei einem Bearbeiter zu terminieren. Die angerufene Nummer wird außerdem für Voicemail verwendet.
- Der Name des Anrufers wird am angerufenen Telefon angezeigt.
- Umleitungsgrund (besetzt, keine Antwort auf Klingeln) kann von Voicemail-Systemen zum Abspielen unterschiedlicher Texte verwendet werden.
- MWI Ein/Aus kann den empfangenden Switch anweisen, den Mitteilungswarteindikator an einem Telefon zu erleuchten, wenn der Benutzer eine neue Mitteilung hat. Ohne diese Fähigkeit in der Leitung kann MWI auf dem Switch getrennt von dem Voice Messaging-System zur Verfügung stehen.
- Beidseitige Einleitung bezieht sich auf die Fähigkeit, einen Anruf auf ein und derselben Leitung zu tätigen und entgegenzunehmen. In der Regel ist dies für Verkehrszwecke wünschenswert, um den Bedarf nach noch mehr Trunk-Leitungsverbindungen zu vermeiden.



Hinweis QSIG ist in Cisco CallManager Version 3.0(5) nicht verfügbar. PRI bietet derzeit den besten verfügbaren Funktionssatz.

In Tabelle 10-2 wird aufgeführt, welche Elemente normalerweise über die Trunk-Leitungsschnittstelle geleitet werden. Unterschiedliche PBX-Anlagen verwenden allerdings u. U. nicht alle Informationen zur Implementierung aller verfügbaren Funktionen für einen gegebenen Trunk-Leitungstyp. In Tabelle 10-3 werden ungefähre Richtlinien zur Funktionsverfügbarkeit bei Verwendung von PRI aufgeführt.

Tabelle 10-3 Funktionsverfügbarkeit mit PRI

Funktion	PBX-PBX	IP-IP	IP-PBX
Übertragung	Ja	Ja	Ja (in Ursprungssystem)
Konferenz	Ja	Ja	Ja (in Ursprungssystem)
Anzeige der Nummer des Anrufers	Ja	Ja	Ja (kann von der PBX-Konfiguration abhängen)
Anzeige des Anrufernams	Ja	Ja	Ja
Anzeige des Namens des Angerufenen	Ja	Ja	Nein

Tabelle 10-3 Funktionsverfügbarkeit mit PRI (Fortsetzung)

Funktion	PBX-PBX	IP-IP	IP-PBX
Anrufentgegennahme-Gruppen	Ja	Ja	Nein
Musik beim Halten der Verbindung	Ja	Nein	Nein (keine Musik, wenn Cisco AVVID den Anruf in Haltestellung nimmt)
Wartefunktionen	Ja	Nein	Nein
Vermittlerdienste	Ja	Nein	Nein (wenn kein separater Cisco AVVID-Bearbeiter konfiguriert ist)

Wenn der Anruf von einem System getätigt, zu einem anderen weitergeleitet und dann zurück umgeleitet wird, werden zwei Kanäle auf der PRI verwendet und bleiben in Nutzung, bis der Anruf heruntergenommen oder freigesetzt wird. Für die Verkehrsplanung in einer E1-Umgebung bedeutet dies, dass nur 11 solcher Anrufe die gesamte PRI-Verbindung nutzen können.

Wenn die Trunk-Leitungen an der PBX-Anlage bleiben, damit die Rechnungsstellung an einem Punkt getätigt werden kann, kann die Identifizierung von Anrufen aus dem IP-Netzwerk nach Rufnummer schwierig sein.

In der folgenden Liste sind die Kosten des Systems vom Typ A zusammengefasst:

Hardware

- PRI-Gateway für IP-Netzwerk
- PRI-Karte auf PBX

Software

- Keine Extras zusätzlich zum Cisco CallManager
- PRI-Software auf PBX

In der folgenden Liste sind die Vor- und Nachteile des Systems vom Typ A zusammengefasst:

Vorteile

- Einfache und kostengünstige Implementierung
- Es ist nur eine minimale Neukonfiguration der PBX-Anlage erforderlich.

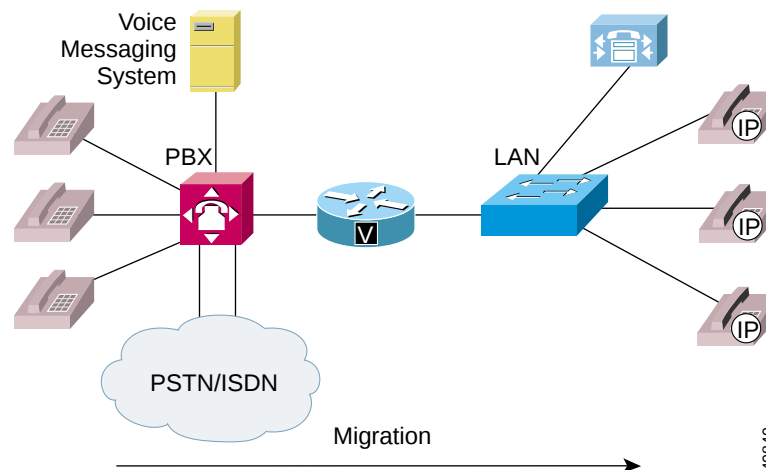
Nachteile

- Ohne QSIG werden vor allem Benutzer einer Anzeige fehlende Funktionsunterstützung bei Anrufen vom IP-Netzwerk zur PBX-Anlage bemerken.
- Die Rechnungsstellung für zwei Systeme ist nur schwer zu verwalten.

Detaillierte Beschreibung von Modell B

In Abbildung 10-7 wird die Topologie für Modell B dargestellt, die sowohl PBX als auch Voice Messaging umfasst.

Abbildung 10-7 Umstellungsmodell B – PBX mit Voice Messaging



Für Modell B müssen dieselben Überlegungen bezüglich der Telefoniefunktionen wie bei Modell A angestrengt werden, wobei die Einführung von Voice Messaging noch einige zusätzliche Überlegungen nach sich zieht. Im Allgemeinen bieten Voice Messaging-Systeme Anrufbeantwortungs- und Mitteilungsabrufdienste. Außerdem weisen sie die PBX-Anlage an, Mitteilungswarteindikatoren ein- oder auszuschalten, und bieten Dienste für abgehende Gespräche, durch die Benutzer sich aus einer Sprach-Mailbox zu einem anderen Telefon übertragen können. (Dieses Leistungsmerkmal ist auch eine Funktion für automatisierte Vermittlerfunktionen, die häufig in Voice Messaging-Systeme integriert sind.)

Es gibt drei wichtige Voraussetzungen für IP-Telefonie-Anwendungen in Netzwerken nach Modell B:

- Wenn ein Teilnehmer ein IP-Telefon anruft und der Anruf zu Voicemail weitergeleitet wird, muss der Anrufer die Begrüßung des IP-Benutzers für die Anrufentgegennahme hören können. Dies kann ein Problem darstellen, da die PBX-Anlage eventuell die ursprüngliche angerufene Nummer des Anrufs nicht beibehält, wenn sie den Anruf vom IP-Netzwerk als Trunk-Leitungsanruf ansieht. In diesem Fall hört der Anrufer nur eine allgemeine Begrüßung (z. B. "Willkommen bei Cisco").
- Wenn IP-Benutzer ihre Mitteilungstaste betätigen, sollten sie nach ihrem Kennwort gefragt werden. Das Voice Messaging-System sollte also die Informationen erhalten, die den Anruf mit der Rufnummer eines Benutzers verbinden, damit es die richtige Mailbox identifizieren kann.
- Der MWI am IP-Telefon sollte je nach dem Status der Sprach-Mailbox des Benutzers ein- und ausgeschaltet werden.

Im Allgemeinen kann keine dieser drei Funktionen in einem einfachen System des Typs B erreicht werden, bei dem die Verbindung zwischen dem IP-Netzwerk und der PBX-Anlage PRI ist und die Konfigurationssequenz für ein System des Typs A verwendet wird. Durch die Verwendung einer komplexeren Konfigurationsänderung an der PBX-Anlage können jedoch die ersten beiden Funktionen erreicht werden.

Diese Implementierung nach Modell B erfordert das Konfigurieren eines Phantom-Telefonbenutzers an der PBX-Anlage. Zur Vereinfachung der Wartung ist es praktisch, einen Block von VNs (Verzeichnis-Nummern) zu wählen, die in Beziehung zu der VN des IP-Benutzers stehen. Für die IP-VNs 32XX erstellen Sie beispielsweise äquivalente Phantombenutzer der PBX-Anlage 52XX. Das Phantomtelefon wird dauerhaft zu Voice Messaging weitergeleitet. Im IP-Netzwerk wird das Telefon so konfiguriert, dass es für Voice Messaging an die Phantom-VN weiterleitet, und am Telefon wird eine Kurzwahltaste zum Wählen der Phantom-VN eingerichtet. Diese Taste kann für Voice Messaging etikettiert werden (außer beim Cisco IP-Telefon 7960). Nun werden sowohl Anrufe zur Anrufbeantwortung als auch zur Mitteilungsabrufung direkt an die Sprach-Mailbox des Benutzers umgeleitet.

Diese Lösung hat auch ihre Nachteile. Sie macht zusätzlichen Verwaltungsaufwand und Benutzeraktionen notwendig, und die Sprach-Mailbox des IP-Benutzers muss eine andere Nummer haben als die VN des Telefons. Außerdem ist es bei manchen PBX-Anlagen notwendig, echte Verbindungskarten für die Phantomtelefone zu konfigurieren. Vielleicht wäre die Verwaltung einfacher, wenn die PBX-VN des Benutzers an der PBX-Anlage während der Migration als die Phantom-VN beibehalten würde und dem Benutzer im IP-Netzwerk eine neue VN zugewiesen werden könnte. Die ursprüngliche DID (DDI) könnte beibehalten werden, wenn die Trunk-Leitungen zum IP-Netzwerk umgeschaltet werden und eine Übersetzung für eingehende Ziffern verwendet würde. In einer solchen Situation würden jedoch die VN, die DID (DDI), und die Nummer der Sprach-Mailbox des Benutzers nicht mehr miteinander übereinstimmen.

Es ist für das Voice Messaging-System nicht möglich, für IP-Benutzer die richtige Begrüßung ("besetzt", "keine Antwort" oder "alle Anrufe") zu wählen, da diese Informationen nicht über die PRI an die PBX-Anlage gesendet werden.

Außerdem können MWI-Informationen nicht die PRI von der PBX-Anlage zum IP-Netzwerk überschreiten. Die Mitteilungsindikationsfunktion wäre daher also nicht für IP-Benutzer in einem System des Typs B verfügbar.

In der folgenden Liste sind die Kosten des Systems vom Typ B zusammengefasst:

Hardware

- PRI-Gateway für IP-Netzwerk
- PRI-Karte auf PBX

Software

- Keine Extras zusätzlich zum Cisco CallManager
- PRI-Software auf PBX

In der folgenden Liste sind die Vor- und Nachteile des Systems vom Typ B zusammengefasst:

Vorteile

- IP-Benutzer erhalten bei der Migration von PBX Zugriff auf Voice Messaging.
- Relativ kostengünstige Implementierung

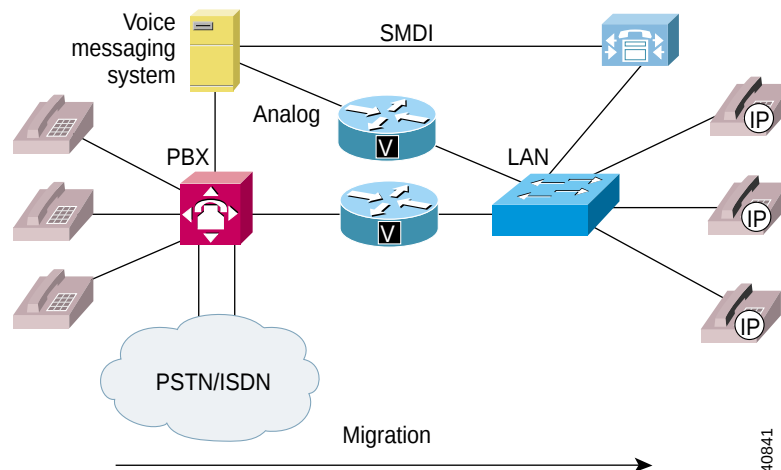
Nachteile

- Dieselben Sprachfunktionsnachteile wie beim System des Typs A
- Keine MWI-Unterstützung für IP-Benutzer
- Die Lösung zieht eine komplexe Verwaltung und möglicherweise auch PBX-Hardware nach sich.

Detaillierte Beschreibung von Modell C

In Abbildung 10-8 wird die Topologie für Modell C dargestellt, die PBX und Voice Messaging mit zusätzlicher SMDI und analogen Verbindungen vom Voice Messaging-System direkt zum IP-Netzwerk umfasst.

Abbildung 10-8 Modell C – PBX und Voice Messaging-System mit separaten Verbindungen zum IP-Netzwerk



Die Hinweise für Telefoniefunktionen für Modell C entsprechen denen von Modell A.

Für Voice Messaging bietet Modell C eine Lösung der Probleme von Modell B. Da das Voice Messaging-System die PBX-Anlage und das IP-Netzwerk als separate Systeme behandelt, können Anrufe, die das IP-Netzwerk erreichen, direkt an die Sprach-Mailbox weitergeleitet werden, ohne über die PBX zurückgeleitet werden zu müssen. Hierdurch sollten alle normalen Anrufbeantwortungs- und Mitteilungsabruffunktionen möglich sein. Da das Voice Messaging-System direkt über SMDI mit dem

IP-Netzwerk verbunden ist, kann das Voice Messaging-System außerdem MWI Ein- oder Aus-Meldungen an das IP-Netzwerk senden, so dass die Indikatoren am IP-Telefon richtig gesteuert werden können.

Damit dieses Modell funktioniert, muss das Voice Messaging-System zwei Qualifikationen erfüllen. Erstens muss es in der Lage sein, zwei PBX-Anlagen gleichzeitig in seiner Datenbank zu unterstützen und jede Mailbox mit der richtigen PBX-Anlage zu verbinden, damit es MWI-Informationen an die richtige Verbindung senden kann. Zweitens muss das IP-Netzwerk physisch mit dem Voice Messaging-System verbunden werden können, während die bestehende Verbindung zu der PBX-Anlage beibehalten werden muss. Nicht alle Voice Messaging-Systeme können diese Art der Integration unterstützen, und daher sollten Kunden den Hersteller ihres Voice Messaging-Systems zu Rate ziehen, bevor sie mit dieser Art Szenario fortschreiten.

In der folgenden Liste sind die Kosten des Systems vom Typ C zusammengefasst:

Hardware

- PRI-Gateway für IP-Netzwerk
- PRI-Karte auf PBX
- Analoge Gateways für das IP-Netzwerk und Voice Messaging
- Analoge Karten im Voice Messaging-System
- SMDI-Schnittstelle im Voice Messaging-System

Software

- Keine Extras zusätzlich zum Cisco CallManager
- PRI-Software auf PBX

In der folgenden Liste sind die Vor- und Nachteile des Systems vom Typ C zusammengefasst:

Vorteile

- IP-Benutzer können bei der Migration von PBX ihren Zugriff auf Voice Messaging beibehalten.
- Relativ kostengünstige Implementierung

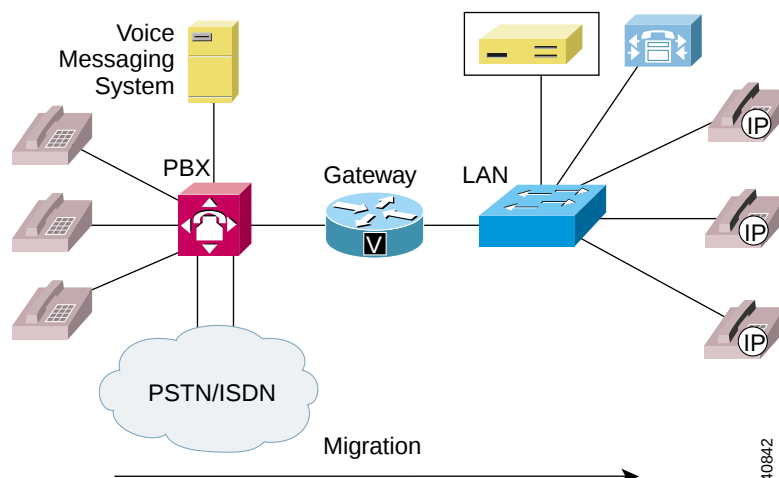
Nachteile

- Dieselben Sprachfunktionsnachteile wie beim System des Typs A
- Komplexere Verwaltung des Voice Messaging-Systems als beim System des Typs B, jedoch eine einfachere Verwaltung der PBX-Anlage
- Im Idealfall können DID (DDI)-Trunk-Leitungen von der PBX-Anlage in das IP-Netzwerk übernommen werden und so den Benutzern folgen. Andernfalls können einige Funktionen verloren gehen.

Detaillierte Beschreibung von Modell D

In Abbildung 10-9 wird die Topologie für Modell D dargestellt, die eine PBX mit Voice Messaging-System umfasst, das mit den einheitlichen Mitteilungsdiensten von Cisco Unified Messaging Server in das IP-Netzwerk übernommen wird. Bei der Erörterung dieses Modells wird nur die Voice Messaging-Komponente von Cisco Unified Messaging Server in Betracht gezogen.

Abbildung 10-9 Modell D – PBX mit Voice Messaging und Migration auf Cisco Unified Messaging Server-Mitteilungen



Die Überlegungen für Telefoniefunktionen für Modell D sind dieselben wie bei Modell A.

Für Voice Messaging sind die IP-Benutzer im Cisco uOne-System, während die PBX-Benutzer im Voice Messaging-System verbleiben. Wenn ein PBX-Benutzer in das IP-Netzwerk übernommen wird, wird seine Voicemail-Box aus dem Voice Messaging-System gelöscht, und in Cisco uOne wird eine neue hinzugefügt.

Da es keine Verknüpfung zwischen Cisco uOne und dem Voice Messaging-System gibt, sind die beiden Benutzergruppen separat und können mit Voice Messaging nicht miteinander interagieren. Wenn beispielsweise ein Voice Messaging-Benutzer eine Verteilerliste hat, können keine IP-Benutzer in sie aufgenommen werden. Außerdem funktioniert die Funktion "Absender antworten" zwischen diesen beiden Gruppen nicht, ebenso wie eine Reihe weiterer Funktionen. Wenn das Voice Messaging-System durch Cisco uOne ersetzt werden soll, ist diese Situation jedoch nur vorübergehender Natur.

Die Vernetzung nach der Spezifikation für den Austausch von Audionachrichten analog (AMIS-A) von Voice Messaging-Systemen ist für eine zukünftige Version von Cisco uOne geplant. Wenn dies verfügbar ist, können grundlegende Sprach-Mailbox-Funktionen in beiden Systemen zur Verfügung gestellt werden, wenn sowohl Cisco uOne und das Voice Messaging-System für die Vernetzung konfiguriert sind und das Voice Messaging-System AMIS-A unterstützt.

In der folgenden Liste sind die Kosten des Systems vom Typ D zusammengefasst:

Hardware

- PRI-Gateway für IP-Netzwerk
- PRI-Karte auf PBX

Software

- Keine Extras zusätzlich zum Cisco CallManager
- PRI-Software auf PBX

In der folgenden Liste sind die Vor- und Nachteile des Systems vom Typ D zusammengefasst:

Vorteile

- IP-Benutzer erhalten bei der Migration über PBX Zugriff auf Voice Messaging.
- Relativ kostengünstige Implementierung

Nachteile

- Dieselben Sprachfunktionsnachteile wie beim System des Typs A
- Keine Voicemail-Interaktion zwischen dem Voice Messaging-System und Cisco uOne
- Im Idealfall können DID (DDI)-Trunk-Leitungen von der PBX-Anlage in das IP-Netzwerk übernommen werden und so den Benutzern folgen. Andernfalls können einige Funktionen verloren gehen.



Netzwerkmanagement

Remote-Bedienbarkeit für Cisco CallManager

Netzwerkmanagements-Tools können bei richtigem Einsatz dem Netzwerkadministrator eine Gesamtübersicht über jedes beliebige Unternehmensnetzwerk bieten. Mit der Einführung konvergenter Netzwerke müssen Netzwerkmanagementsysteme mindestens über die folgenden Fähigkeiten verfügen:

- Netzwerkerkennungs- und -topologieübersicht
- Inventarkontroll- und Konfigurationsverwaltung der Netzwerkknoten
- Reporting, Systemprotokollierung und Analyse der so erhaltenen Daten

Cisco CallManager Remote-Bedienbarkeit und CiscoWorks2000 bieten diese Fähigkeiten sowie weitere Mechanismen, anhand derer die Funktionalität und Verfügbarkeit des Cisco AVVID-Netzwerks überprüft werden können. Es wurden zahlreiche Verwaltungsfunktionen hinzugefügt, angefangen mit Cisco CallManager Version 3.0, die einem Cisco AVVID-Netzwerk Einsicht in die Betriebs- und Berichterstellungsfähigkeiten gewährt. In Tabelle 11-1 werden die Leistungsmerkmale aufgeführt, die für Netzwerkmanagementsanwendungen zum Exportieren von Daten sowie besonders im Fall von CiscoWorks2000 zur Unterstützung von Reporting, proaktiver Verwaltung, Fehlerbeseitigung und anderen Fähigkeiten zur Verfügung gestellt wurden.

Tabelle 11-1 Remote-Bedienungsfunktionen für Cisco CallManager

Funktion	Beschreibung
Simple Network Management Protocol (SNMP)-Instrumentierung	Cisco CallManager wurden zwei Management Information Bases (MIBs) hinzugefügt, mit deren Hilfe ein Netzwerkmanagementsystem die gewünschten Informationen abrufen kann.
Anruferdetaildatensatz (Call Detail Record = CDR)-Protokollierung	Der Anruferdetaildatensatz wird für die Buchhaltung, Fehlerbeseitigung und Pfadanalyse verwendet.

Tabelle 11-1 Remote-Bedienungsfunktionen für Cisco CallManager

Funktion	Beschreibung
Cisco Discovery Protocol (CDP)-Unterstützung (CDP-MIB)	Cisco Discovery Protocol-Unterstützung für Cisco CallManager-Server-Ankündigung und -Erkennung über ein Netzwerkmanagementsystem wie z. B. CiscoWorks2000. Dies ist die "Tell" (Aussage)-Seite von CDP über SNMP-Aktivierung.
Systemprotokollierungskomponenten	Cisco Syslog Collector für die Filterung, Sammlung und Lagerung von Mitteilungen auf einem Syslog-Server.

In den folgenden Abschnitten werden einige dieser Leistungsmerkmale detaillierter beschrieben.

SNMP-Instrumentierung auf dem Cisco CallManager-Server

Simple Network Management Protocol (SNMP)-Funktionen für Cisco CallManager ermöglichen den Netzwerkmanagementsanwendungen das Abrufen von Daten vom Cisco CallManager-Server auf die standardmäßige Weise. Der SNMP-Agent auf dem Cisco CallManager-Server ist ein Teilagent (Erweiterungsagent) des Microsoft Windows 2000-Systemagenten. Daher müssen Sie den SNMP-Dienst auf dem Windows 2000-System aktivieren, damit die SNMP-Instrumentierung auf dem Cisco CallManager-Server funktioniert.

Zwei Management Information Bases (MIBs) wurden in Cisco CallManager Version 3.0 eingeführt, um das Exportieren von Daten sowie Unterstützung für Server-Ankündigung und -Erkennung zu bieten. Beide MIBs sind voneinander unabhängige Erweiterungsagenten, die zukünftige Anwendungen und Funktionen erleichtern:

- CISCO-CCM-MIB

Diese MIB exportiert Daten aus der Cisco CallManager-Datenbank und anderen Datenquellen. Beispiele für die exportierten Daten umfassen Cisco CallManager-Gruppentabellen, Regionentabellen, Zeitzonengruppentabellen, Geräte-Pool-Tabellen, Gateway-Informationstabellen und Status-Traps, CDR-Host-Protokollierungstabelle, Leistungszähler usw.

- CISCO-CDP-MIB

Diese MIB verwendet Cisco Discovery Protocol (CDP), um CiscoWorks2000 zu aktivieren und den Cisco CallManager-Server auffindig zu machen, sowie um Informationen von Variablen wie z. B. der Schnittstellentabelle, der Geräte-ID usw. abzurufen. Dies ist eine

begrenzte Implementierung der MIB und eigentlich nur ein Teilsatz der CDP-MIB in Zusammenhang mit Ankündigungen (also der "Tell"-Seite der MIB).

Weitere detaillierte Informationen über die CDP-MIB erhalten Sie bei der Cisco Connection Online (CCO) unter

<http://www.cisco.com/univercd/cc/td/doc/product/fhubs/fh300mib/mibcdp.htm>

Systemprotokollierungskomponenten

Das Hauptziel von Systemprotokollierungskomponenten ist die Unterstützung einer funktionierenden Lösung für eine zentrale Ereignisprotokollierung und eines Fehlerbeseitigungsschemas in der verteilten Cisco AVVID-Umgebung mit mehreren Plattformen. In einem offenen, verteilten System können Sie mehrere Anwendungen auf mehreren Systemen ausführen. Zur Vereinfachung der Verwaltung sollten Sie ein gemeinsames Ereignisprotokoll und ein gemeinsames Verfolgungsprotokoll unterhalten, in dem Cisco CallManager Ereignisse melden kann.

Die Schnittstelle, an der Ereignisse protokolliert werden, muss für die meisten üblichen Programmiersprachen verwendet werden können. Bei einer gemeinsamen Protokollierschnittstelle muss außerdem das Format der Protokollmeldungen im gesamten System einheitlich sein, damit es leicht gelesen werden kann. Schließlich sollte das System außerdem über eine gemeinsame Verwaltungsschnittstelle verfügen, an der alle verfolgten Ereignisse angezeigt und kontrolliert werden können. Cisco CallManager und CiscoWorks2000 bieten diese Funktionen für die einheitliche Meldungsprotokollierung, -anzeige und -verwaltung. Die folgenden beiden Komponenten bilden den Kern des Systemprotokollierungsmechanismus:

- Syslog Collector, ein Bestandteil des Cisco CallManagers
- Syslog Receiver (Der CiscoWorks2000-Server kann auch als Empfänger fungieren, wie unter "Syslog-Verwaltungsschnittstelle" auf Seite 11-4 beschrieben.)

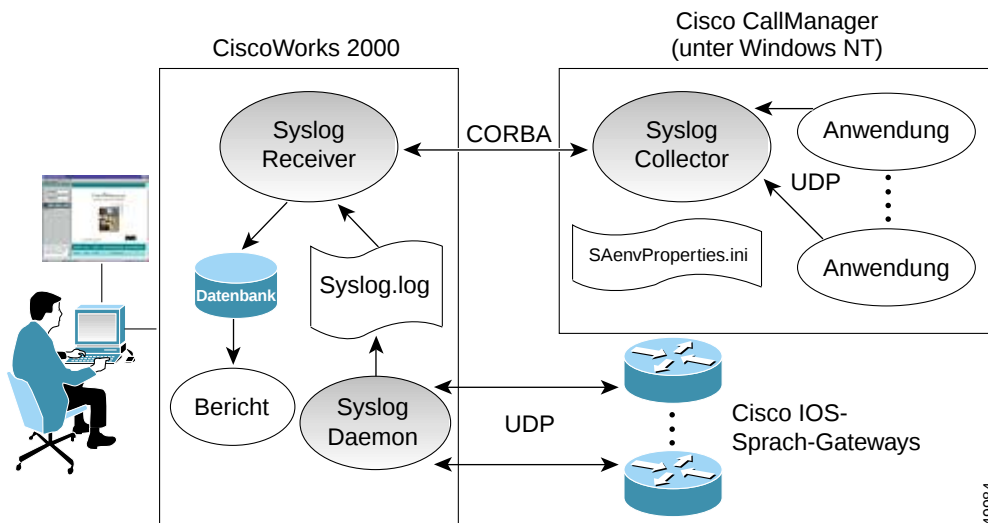
Syslog Collector

Ein Syslog Analyzer Collector (SAC)-Programm wird als ein Windows NT-Dienst auf dem Cisco CallManager-Server oder einem anderen Verarbeitungsknoten im Netzwerk ausgeführt. Das SAC-Programm stellt anhand einer Konfigurationsdatei (.ini-Datei) die Umgebungsvariablen wie beispielsweise den CiscoWorks2000-Hostnamen und andere Parameter ein. Diese Konfigurationsdatei, SAenvProperties.ini, und ihr Verzeichnispfad sind in der Windows NT-Registrierung angegeben, und das Cisco CallManager-Installationsprogramm stellt ihre Werte ein. Während des Systemstarts versucht der SAC, sich beim CiscoWorks2000-Server anzumelden, um mithilfe eines Common Object Request Broker Architecture (CORBA)-Methodenaufrufs einige Konfigurations- und MeldungsfILTERinformationen abzurufen. Daraufhin sendet er eine

Initialisierungsmeldung, die aus dem SAC-Hostnamen, dem Namen der syslog-Datei und weiteren Informationen besteht, damit CiscoWorks2000 ihn weiter verfolgen kann.

Während einer normalen Sitzung liest SAC Meldungen vom User Datagram Protocol (UDP)-Port 514. Wenn er neue Meldungen erhält, verarbeitet SAC die Meldungen (beispielsweise durch Ausführen von Filterung und Zeitzonenumwandlungen) und sendet sie dann zur Speicherung und Analyse an den CiscoWorks2000-Server. Außerdem sendet SAC in regelmäßigen Abständen eine Status- oder Statistik-Meldung an den CiscoWorks2000-Server. In Abbildung 11-1 ist die Interoperabilität von CiscoWorks2000 und Cisco CallManager dargestellt.

Abbildung 11-1 Syslog-Architektur für die Interoperabilität von Cisco CallManager und CiscoWorks2000



Syslog-Verwaltungsschnittstelle

Die Verwaltungsschnittstelle Syslog ist eine Web-basierte Schnittstelle, die einen Bestandteil der Verwaltung von Cisco CallManager darstellt und unter **Service> Trace** zu finden ist. Auf einer neuen Seite werden der Status jeder Verfolgungsmarkierung und die Optionen für die Verfolgungsausgabe jedes Dienstes für jeden Server in einem Cisco CallManager-Cluster angezeigt, wie in Abbildung 11-2 dargestellt. Sie können die Verfolgungsmarkierungen über die Verwaltungsschnittstelle aktivieren oder deaktivieren und so die Verfolgungskonfiguration in der Datenbankschicht aktualisieren.

Abbildung 11-2 Benutzerschnittstelle zur Verwaltung für Syslog-Verfolgungsfunktionen

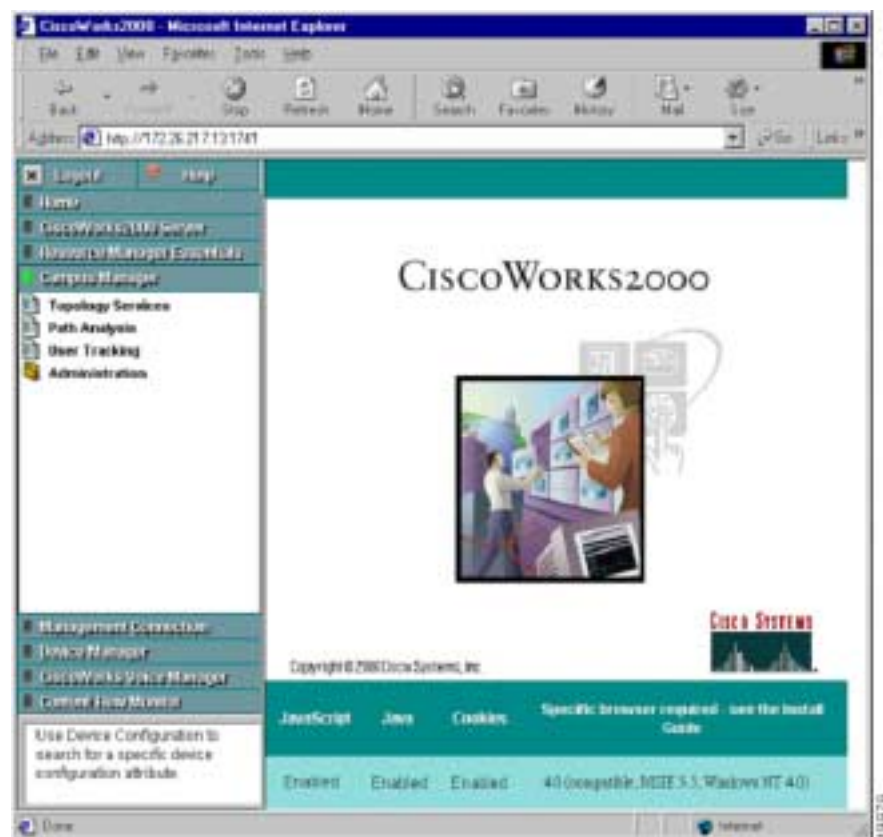


Es gibt auch Optionen, mit denen Meldungen zur Fehlerbehebungsverfolgung aktiviert und der Syslog-Servername konfiguriert werden können. Sie sollten die Option zur Fehlerbehebungsverfolgung nur aktivieren, wenn es in dem System wenig Aktivitäten gibt. Dadurch vermeiden Sie, dass das Netzwerk mit übermäßigem Verkehr gefüttert und Ihr System überlastet wird. Sie können die Fehlerbehebungsverfolgungsmeldungen an das Windows 2000-Ereignisprotokoll, an eine lokale Datei, an den Syslog-Server oder an alle Drei senden. Geben Sie den Syslog-Servernamen nur ein, wenn Sie einen anderen Syslog-Dämon als den CiscoWorks2000-SAC als Syslog-Server verwenden. Andernfalls lassen Sie das Feld für den Syslog-Servernamen leer; der Name des lokalen Hosts wird dann standardmäßig übernommen.

CiscoWorks2000 Sprachverwaltungsfunktionen

CiscoWorks2000 ist eine Produkt-Suite zur Netzwerkmanagement, Inventarkontrolle, Analyse und Fehlerbehebung. Das Common Management Framework (CMF) in CiscoWorks2000 ist eine Web-basierte Anwendung mit einer Reihe von Plug-in-Anwendungs-Suiten, die gewisse Verwaltungsfunktionssätze bieten. In Abbildung 11-3 ist die Benutzeroberfläche von CMF dargestellt.

Abbildung 11-3 Common Management Framework und Benutzeroberfläche für CiscoWorks2000



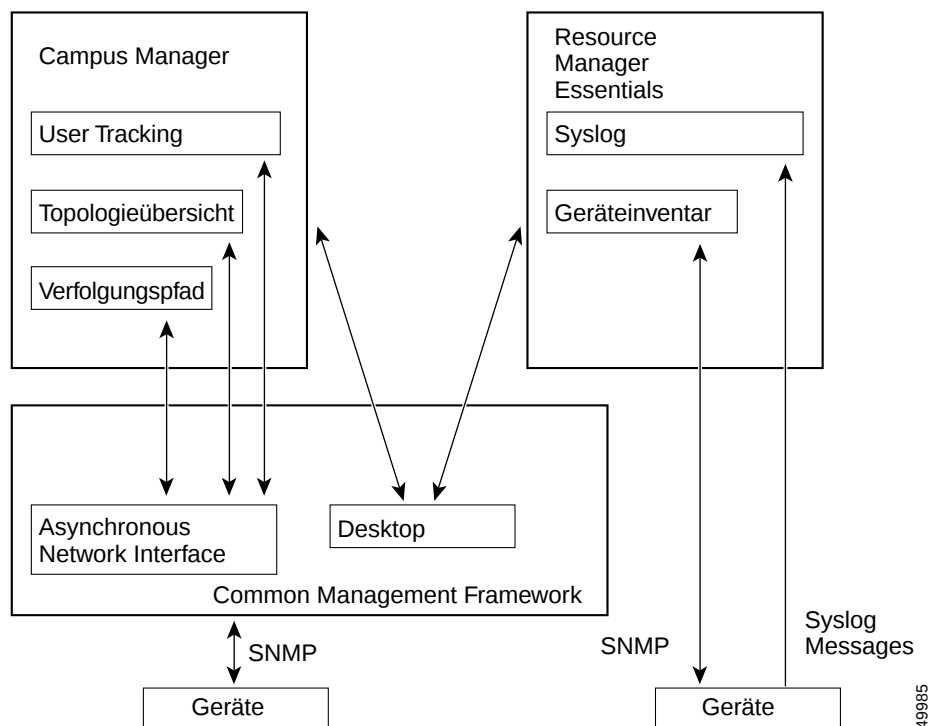
Jede Anwendungs-Suite auf der gemeinsamen Web-basierten Oberfläche nutzt eine gemeinsame Datenbank. CiscoWorks2000 kann entweder auf einer Windows NT- oder einer Sun Solaris-Plattform ausgeführt werden. In Tabelle 11-2 werden die jeweiligen Komponenten beschrieben, die zur Vervollständigung der Produkt-Suite für die Cisco AVVID-Netzwerkmanagement benötigt werden.

Tabelle 11-2 Komponenten der CiscoWorks2000-Produkt-Suite

CiscoWorks2000-Komponenten	Beschreibung und Funktion
Common Management Framework Version 1.1.1 (CD-ROM Eins, Ausgabe 3)	Dient als eine grundlegende Web-Anwendung für alle Komponenten, als einzelner Manager mit grafischer Benutzeroberfläche für andere CiscoWorks2000-Komponenten und als zentrale Datenbank. Diese Komponente ist Bestandteil des LAN-Verwaltungslösungs (LAN Management Solution = LMS)-Pakets.
Campus Manager Version 3.0.1 P1 (im Lieferumfang des Voice-Updates enthalten)	Bietet verschiedene Funktionen, wie z. B. die Erkennungs- und Topologieübersicht, den zentralen Punkt für die Host-Verwaltung (Konsole), User Tracking und Pfadanalyse.
Resource Manager Essentials Version 3.2 (im Lieferumfang des Voice-Updates enthalten)	Wartet das verwaltete Geräteinventar, die Konfigurationsverwaltung und das Systemprotokollierungslager sowie die Systemprotokollierungsanalyse.

Wie bereits erläutert besteht die CiscoWorks2000-Architektur aus einem einheitlichen Verwaltungsrahmen (dem Common Management Framework = CMF) mit einem Web-basierten Desktop als einziger Verwaltungspunkt. Als zusätzliche Komponente bietet die asynchrone Netzwerkschnittstelle (Asynchronous Network Interface = ANI) Dienste zum Sammeln von Daten mithilfe des Simple Network Management Protocols (SNMP), Cisco Discovery Protocol und den Tabellen des Interim Local Management Interface (ILMI). In Abbildung 11-4 ist diese Architektur dargestellt.

Abbildung 11-4 CiscoWorks2000-Architektur



Die Erkennung des Netzwerks setzt ein, wenn Sie ein Seed-Gerät, vorzugsweise einen Router oder einen Switch, zur Verfügung stellen, über den die ANI das Netzwerk durch Lesen der CDP-Cache-Tabellen und SNMP-Variablen seiner Nachbarn lesen und eine entsprechende Netzwerktopologieübersicht erstellen kann. Der CMF bietet außerdem eine grobe Sicherheit, Prozesskontrolle und Geräteinformationsabruf über SMTP. Er verwendet die Verwaltungsinformationsdatenbanken von CDP und dem Cisco CallManager dazu, die Cisco CallManager im Netzwerk zu erkennen und ihre entsprechenden Datentabellen abzurufen und zu speichern.

Campus Manager

Der ANI-Erkennungsprozess hat dem Cisco AVVID-Netzwerk in der Common Management Framework (CMF) Version 1.1.1 Unterstützung für Sprachkomponenten hinzugefügt. Diese CMF-Version unterstützt die folgenden Sprachgeräte und -funktionen:

- Cisco CallManager

Cisco CallManager Version 3.0 (und später) umfasst den CDP-Treiber und unterstützt teilweise CDP-MIB und SNMP. Dies ist die "Tell" (Aussage)-Seite von CDP, sodass es sich hierbei immer um ein Randgerät handelt, und es wird in der Topologieübersicht als ein Cisco CallManager-Symbol angezeigt.

- Cisco IOS-Voice-Gateways
Die Voice-Gateways werden genau so erkannt, wie herkömmliche Router.
- Cisco IP-Telefone (Modelle 7960, 7940 und 7910)
Cisco IP-Telefone enthalten die "Tell"-Seite" des CDP-Treibers, unterstützen jedoch kein SNMP.
- VLAN-Verwaltung
Dieses Leistungsmerkmal bietet Tools für die grafische VLAN-Konfiguration und logische Topologieübersicht.
- Mobilität und Verfolgung der End-Geräte
Dieses Leistungsmerkmal bietet Tools für die Verfolgung und Konfiguration mobiler Benutzer und des VLANs.
- Verfolgungspfadanalyse
Dieses Leistungsmerkmal verfolgt Pfade aus Schicht 2 und Schicht 3 zwischen zwei Geräten oder Endstationen anhand der IP-Adresse oder der Directory Number.

Da in der Regel viele Cisco IP-Telefone in einem Netzwerk installiert sind, muss die ANI die Erkennung der Cisco IP-Telefone separat abwickeln, um eine Überlastung der Netzwerktopologieübersicht zu vermeiden. Aus diesem Grund ignoriert CMF Version 1.1.1 die CDP-Cache-Einträge der Cisco IP-Telefone in den benachbarten Switches und erstellt keine Geräteobjekte für sie; daher werden verkettete IP-Telefone nicht erkannt. Die Cisco IP-Telefone werden als Endbenutzergeräte behandelt und über User Tracking erkannt, wie im nächsten Abschnitt beschrieben.

User Tracking

User Tracking (UT, Benutzerverfolgung), ein Dienstmodul des Campus Managers und der ANI, erkennt speziell Endbenutzerknoten wie z. B. Systeme, Cisco CallManager-Hosts, Cisco IP-Telefone und Nicht-CDP-Systeme. User Tracking führt eine anfängliche Erkennung aller Hosts in der Topologieübersicht und eine darauf folgende Erkennung zur Wartung der User Tracking-Tabelle durch. Sie können eine zeitliche Begrenzung für diese folgende Erkennung festlegen; der Standardwert beträgt eine Stunde.

Die anfängliche UT-Erkennung erstellt eine Telefontabelle, indem folgende Schritte ausgeführt werden:

1. UT liest den Content Addressable Memory (CAM) und die Address Resolution Protocol (ARP)-Tabelle der Switches und Router, die bereits von ANI erkannt und in der Topologieübersicht aufgezeichnet wurden.
2. Aufgrund der Informationen von CAM- und ARP-Abfragen erzeugt UT eine Endbenutzertabelle mit Geräte- und Port-Informationen. Wenn es sich bei dem Endbenutzer um ein Cisco IP-Telefon handelt, führt UT die folgenden Schritte aus:

- Es wird der Telefoneintrag von den CCM-Hosts mithilfe der Verwaltungsinformationsdatenbank CISCO-CCM-MIB gelesen.
- Es wird eine Telefontabelle erzeugt, die mit den in Abbildung 11-5 gezeigten Werten übereinstimmt.
- Für ältere Modelle von Cisco IP-Telefonen (Cisco IP-Telefonmodell 12 SP+ und 30 VIP), fragt UT anhand der CCM-MIB den Cisco CallManager ab und erstellt die Telefontabelle auf der Grundlage der Geräte- und Port-Informationen, die bei der ersten Erkennung gesammelt wurden.



Hinweis Bei Nicht-Cisco IP-Telefonen wird eine Anfrage an den Cisco CallManager über SNMP getätigt, und die zurückgegebenen Informationen werden mit Querverweisen zu den Informationen versehen, die durch Standardabfragen an Switches zur Abrufung von MAC-Adressen und Switch-Anschlüssen (Abfrage der CAM-Tabelle) und durch Abfragen an Router zur Zuweisung von IP-Adressen und MAC-Adressen (Abfrage der ARP-Tabelle) zusammengetragen wurden.

Abbildung 11-5 User Tracking-Telefontabelle

Phone Number	MAC Address	IP Address	CCM Address	Status	Phone Type	Phone Class	Device Name	Device	Port	Port Name	Location
2439 2050	0018-eb-00-2a-40	192.168.76.157	192.168.76.75	active	12SP+	Main Phone	deno-5000	192.168.76.40	3/12		2008/06/11 14:00:00
2440 2051	0018-eb-00-2a-40	192.168.76.171	192.168.76.75	active	12SP+	Line Phone	deno-5000	192.168.76.40	3/18		2008/06/11 14:00:00
24407 2000	0018-eb-00-5b-e3	192.168.76.212	192.168.76.75	active	30/0P	Field Device	field-c5000a	192.168.76.196	3/5		2008/06/11 14:00:00
24406 2001	0018-eb-00-2a-68	192.168.76.211	192.168.76.75	active	12SP+	Field Device 2	field-c5000a	192.168.76.196	3/6		2008/06/11 14:00:00
24500 2053	0018-eb-00-2a-75	192.168.76.103	192.168.76.75	active	12SP+	Caterpillar Phone	deno-5000	192.168.76.40	3/20		2008/06/11 14:00:00
25476 2002	0018-eb-00-2a-ac	192.168.76.212	192.168.76.75	active	12SP+	Field phone in Lab	deno-4000	192.168.76.234	2/5		2008/06/11 14:00:00
24408 2054	0018-eb-00-2a-ab	192.168.76.103	192.168.76.75	active	12SP+	Device Phone	deno-5000	192.168.76.40	3/21		2008/06/11 14:00:00

Verfolgungspfadanalyse

Das Pfadanalyse-Tool, ein Bestandteil des Campus Managers, verfolgt die IP-Konnektivität zwischen verwalteten Geräten im Netzwerk. Bei den Endpunkten der Verfolgung muss es sich um ein verwaltetes Gerät oder einen Endbenutzerknoten im UT handeln, da die Verfolgung nur durchgeführt werden kann, wenn die Daten absolut verlässlich sind. Die Verfolgung zeigt Pfade von einem Ende zum anderen auf Schicht 3 (IP) sowie in manchen Fällen Schicht-2-Geräte im Schicht-3-Pfad an. Das Pfadanalyse-Tool bietet zwei Arten der Verfolgung, Daten und Sprache. In diesem Kapitel wird nur die Sprachverfolgung behandelt.

Eine Sprachverfolgung wird anhand der Anruferdetaildatensätze (Call Details Records = CDRs) durchgeführt und zeigt auch den IP-Pfad der Verfolgung für den Fall an, dass der Status des Netzwerks zwischen zwei

Telefonen oder zwischen einem Telefon und dem Cisco CallManager festgestellt werden muss. Die Datenpfadübersicht kann auch einen Rückwärtspfad anzeigen, der verwendet wird, falls eine Kongruenz in den IP-Routing-Pfaden von Schicht 3 vorliegt. Die Nicht-CDR-Sprachverfolgung führt außerdem eine Quellen-geroutete Verfolgung mit demselben IP-Präzedenzwert wie ein Sprachanruf durch (nur RTP). Diese Verfolgung wird verwendet, wenn die Sprache einem anderen Pfad folgt als Daten und wenn sie QoS, die für Sprache zur Verfügung gestellt wurde, nutzen oder Probleme mit ihr erkennen kann.

Die CDR-basierte Sprachverfolgung kann drei Werte für eine Verfolgung annehmen: Zeitraum zur Abgleichung des Anrufs, Nummer des Anrufers und angerufene Nummer. Eine Abgleichung der Daten tritt auf, wenn die Ziffern ganz rechts eingegeben werden. Die Pfadanalyse-Tools durchsuchen die CDRs aller verwalteten Cisco CallManager-Hosts in der Datenbank, und die übereinstimmenden Datensätze werden zurückgegeben. Die Tools können die Datensätze anzeigen und untersuchen sowie Vorschläge für die möglichen Ursachen eines Problems und Korrekturmaßnahmen nach bestem Wissen machen.

In Abbildung 11-6 wird ein Beispiel für eine Verfolgungspfadanalyse dargestellt, in der Geräte der Schicht 2 und Schicht 3 angezeigt werden.

Abbildung 11-6 Beispiel für eine Verfolgungspfadanalyse

Zurückgegebene CDR-Details für übereinstimmende Kriterien.

Angabe der anrufenden oder angerufenen Nummer bzw. Zeitraum für Sprachverfolgung. CDRs und alle Cisco CallManager werden durchsucht.



Resource Manager Essentials

Die CiscoWorks2000 LAN-Verwaltungslösung wird im Paket mit den Resource Manager Essentials (RME) geliefert, die vornehmlich für die Inventarkontrolle, das Systemkonfigurationslager und die Konfigurationsverwaltung, den Syslog-Server und die Syslog-Analyse sowie andere Berichterstellungsfunktionen verantwortlich sind. RME Version 3.1 ist die erforderliche Mindestversion, die detaillierte Berichterstellungsfähigkeiten und Verwaltbarkeit für importierte Cisco CallManager-Hosts unterstützt.

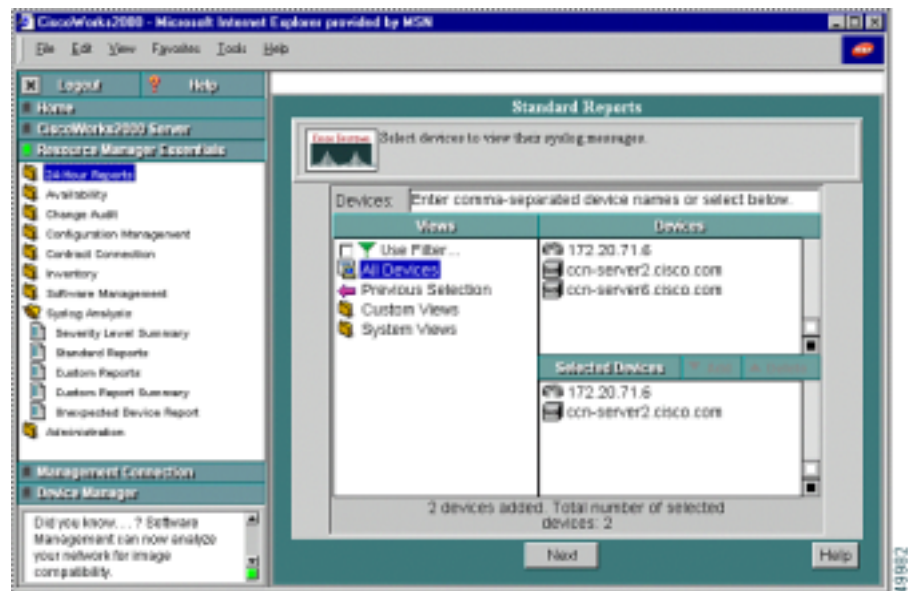
Die Systemprotokollierungsfähigkeiten von Cisco CallManager, die unter "Systemprotokollierungskomponenten" auf Seite 11-3 näher beschrieben sind, sind in CiscoWorks2000 integriert. RME dient als einziger Verwaltungspunkt für die Meldungsfilterkonfiguration von Syslog Collector sowie die Gerätedetailberichterstellung für Cisco CallManager und andere Cisco-verwaltete Geräte.

Inventarkontrolle und Reporting

Cisco CallManager wird in RME auf dieselbe Weise unterstützt wie jedes Cisco-Gerät. Auf die von Cisco CallManager unterstützten MIBs kann über einen Standard-SNMP-Agenten zugegriffen werden. RME identifiziert den Cisco CallManager über die Compaq sysObjectID, so dass das Exportieren eines ähnlichen Systems, das Cisco CallManager nicht ausführt, unbedingt vermieden werden muss; andernfalls vergeudet RME Ressourcen auf das regelmäßige Sammeln von Konfigurationsinformationen vom Nicht-CallManager-System.

RME erstellt außerdem eine separate Gruppe in der Geräteauswahl (einer neuen Systemansicht mit der Bezeichnung "Cisco CallManagers"), wenn es erkennt, dass Cisco CallManager-Hosts für die Inventar- und Berichterstellungsverwaltung importiert wurden. Berichte, die in der Geräteauswahl angezeigt werden, sollen Daten über die Konfiguration und den Status von Cisco CallManager selbst liefern; sie liefern keine Berichte über Informationen bezüglich der Einzelkomponenten, die im Cisco CallManager konfiguriert wurden. In Abbildung 11-7 sehen Sie ein Beispiel für einen Gerätebericht von RME.

Abbildung 11-8 Standard Report in CiscoWorks2000



Sie können über die Verwaltungsschnittstelle von CiscoWorks2000 auch benutzerdefinierte Berichte wie z. B. Filter für Benutzer-URLs, automatisierte Aktionen und Meldungen festlegen (siehe Abbildung 11-9). Diese Funktionen des Syslog Analyzers und der Verwaltungsschnittstelle wurden in RME Version 3.1 aktualisiert, um Unterstützung für Cisco CallManager und seine Suite von Sprachanwendungen zu bieten.

Syslog Message Filtering

Zusätzlich zur System Diagnostic Interface (SDI)-Filterung bestehen es im Syslog Analyzer zwei weitere Positionen für das Durchführen der Meldungsfiltrierung:

- Im Syslog Analyzer Collector (SAC)-Prozess, bevor die Meldung an das Netzwerk gesandt wird
- Im CiscoWorks2000-Server, wo der Administrator einen benutzerdefinierten Bericht festlegen kann

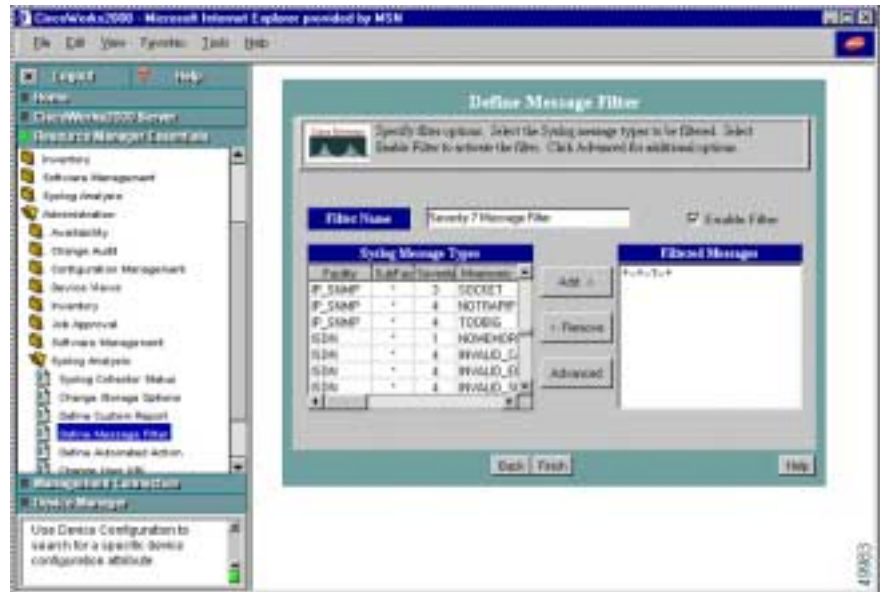


Hinweis Wenn Sie die Syslog-Filter auf dem CiscoWorks2000-Server einstellen, werden alle definierten Syslog-Meldungen an den Server gesandt, wodurch fehlerhafter Netzwerkverkehr entsteht. Cisco empfiehlt Ihnen daher, mithilfe des SAC Filter zu erstellen, bevor Sie sie an den Syslog-Server senden.

Im Filterungsmechanismus können Sie Filter auf der Grundlage der Quelle, des Vorrichtungscodes, des Teilvorrichtungscodes, des Schweregrads, des mnemonischen Codes oder der Muster in der Meldung

definieren. In Abbildung 11-9 ist ein Beispiel für das Definieren eines Meldungsfilters an der Verwaltungsschnittstelle von CiscoWorks2000 dargestellt.

Abbildung 11-9 Für einen Remote SAC definierter Meldungsfilter



Warnungen

Der Syslog Analyzer in CiscoWorks2000 verfügt über eine Web-basierte Verwaltungsschnittstelle zum Definieren einer automatischen Aktion für einen Ereignissatz oder für Syslog-Meldungen von bestimmten Geräten. In zukünftigen Versionen von CiscoWorks2000 wird dieses Leistungsmerkmal noch weiter verbessert, sodass Warnungen oder Traps erzeugt werden können. Derzeit kann der Syslog Analyzer zur Benachrichtigung über Ereignisse entweder durch Schreiben einer Protokolldatei oder durch Erzeugen einer E-Mail-Nachricht verwendet werden. Cisco empfiehlt, das gewünschte E-Mail-Ziel als E-Mail-Empfänger, der eine Seite erzeugen kann, oder E-Mail-Alias für eine Network Operation Center (NOC)-Warnmeldung zu konfigurieren. Einen deutlichen Vorteil für einen reibungslosen Betrieb könnte man erzielen, wenn E-Mail-Nachrichten zur Benachrichtigung über Ereignisse an einen E-Mail-fähigen Pager oder ein Mobiltelefon gesendet werden können.



Konventionen

In diesem Dokument werden folgende Konventionen angewendet:

Konvention	Beschreibung
Fettdruck	Befehle und Schlüsselwörter sind in Fettdruck geschrieben.
Kursivdruck	Argumente, für die Sie Werte vorgeben müssen, sind in Kursivdruck geschrieben.
[]	Elemente in eckigen Klammern sind optional.
{ x y z }	Alternative Schlüsselwörter stehen in geschweiften Klammern und werden durch vertikale Striche getrennt.
[x y z]	Optionale alternative Schlüsselwörter stehen in eckigen Klammern und werden durch vertikale Striche getrennt.
Zeichenfolge	Eine Gruppe von Zeichen ohne Anführungszeichen. Sie dürfen die Zeichenfolge nicht in Anführungszeichen setzen, da die Anführungszeichen sonst als Teil der Zeichenfolge interpretiert werden.
Bildschirmtext	Terminal-Sitzungen und Informationen, die das System anzeigt, erscheinen als Bildschirmtext.
Bildschirmtext in Fettdruck	Informationen, die Sie eingeben müssen, werden als Bildschirmtext in Fettdruck dargestellt.
Bildschirmtext in Kursivdruck	Argumente, für die Sie Werte eingeben müssen, werden als Bildschirmtext in Kursivdruck dargestellt.
→	Der Zeiger dient zur Hervorhebung einer wichtigen Textzeile in einem Beispiel.
^	Das Symbol ^ entspricht der Strg-Taste. Die Tastenkombination ^D in einer Bildschirmanzeige bedeutet, dass Sie die Strg-Taste und die Taste D gleichzeitig gedrückt halten müssen.
< >	Zeichen, die nicht angezeigt werden (z. B. Passwörter), werden in spitzen Klammern dargestellt.

Für Hinweise gelten folgende Konventionen:



Hinweis Auf diese Weise werden Hinweise für den Leser gekennzeichnet. Hinweise enthalten hilfreiche Vorschläge oder Verweise auf Material, das nicht in dieser Publikation enthalten ist.

Für Aktionen, mit denen Sie Zeit sparen können, gelten folgende Konventionen:



Schnellverfahren Aktionen, mit denen Sie Zeit sparen können, werden auf diese Weise dargestellt. Mit der im Abschnitt beschriebenen Aktion können Sie Zeit sparen.

Für Tipps gelten folgende Konventionen:



Tipps Auf diese Weise werden Informationen mit hilfreichen Tipps gekennzeichnet.

Für Hinweise zum vorsichtigen Vorgehen gelten folgende Konventionen:



Vorsicht Auf diese Weise wird der Leser aufgefordert, vorsichtig zu sein. In dieser Situation könnten bestimmte Vorgehensweisen zur Beschädigung von Geräten oder zu Datenverlust führen.

Für Warnungen gelten folgende Konventionen:



Warnung Das Warnsymbol weist auf Gefahren hin. In dieser Situation könnten Sie sich Verletzungen zuführen. Bevor Sie an einem Gerät arbeiten, müssen Sie sich über die Gefahren bewusst sein, die beim Umgang mit elektrischen Schaltkreisen bestehen. Darüber hinaus müssen Sie wissen, welche Standardmaßnahmen zur Vermeidung von Unfällen zu ergreifen sind.

Zusätzliche Informationen

Dieser Abschnitt enthält Verweise auf Dokumente, die zusätzliche Informationen zu den in diesem Handbuch behandelten Themen enthalten.

- Hohe Verfügbarkeit:
 - http://www.cisco.com/warp/partner/synchronicd/cc/sol/mkt/ent/ndsgn/highd_wp.htm
 - <http://www.zdnet.com/zdtag/whitepaper/campuslan.pdf>
- Schutz vor Stromausfall:
 - <http://www.apcc.com/go/machine/cisco/3a.cfm>
- Simple Mail Transfer Protocol (SMTP):
 - <http://www.cisco.com/univercd/cc/td/doc/product/software/ioss390/ios390ug/ugsmtp.htm>
- Internet Message Access Protocol (IMAP):
 - <http://www.imap.org/whatisIMAP.html>

- Lightweight Directory Access Protocol Version 3 (LDAPv3):
 - <http://www.critical-angle.com/ldapworld/ldapv3.html>
- Glossar mit Begriffen und Akronymen
 - <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm>
 - <http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm>

Bezug der Dokumentation

Im folgenden Abschnitt erfahren Sie, wo Sie die Dokumentation von Cisco Systems beziehen können.

World Wide Web

Sie können den Großteil der aktuellen Cisco Dokumentation im World Wide Web auf folgenden Sites abrufen:

- <http://www.cisco.com>
- <http://www.cisco.de>
- <http://www-europe.cisco.com>

Dokumentation auf CD-ROM

Die Cisco Dokumentation und weitere hilfreiche Literatur finden Sie im CD-ROM-Paket, das Sie zusammen mit Ihrem Produkt erhalten. Die Dokumentations-CD-ROM wird monatlich aktualisiert und ist unter Umständen aktueller als die gedruckte Dokumentation. Das CD-ROM-Paket ist einzeln oder im Jahresabo erhältlich.



A – B

ACF	Zugangsbestätigung (Admission Confirm)
ACL	Zugriffskontrollliste (Access Control List)
ADPCM	Adaptive Differential Pulse Code Modulation
AMIS-A	Spezifikation für den Austausch von Audionachrichten analog (Audio Messaging Interchange Specification Analog)
ANI	Automatische Nummernidentifizierung
ARQ	Zulassungsanfrage (Admission Request)
ASIC	Anwendungsspezifischer integrierte Schaltkreis (Application-specific Integrated Circuit)
AVVID	Siehe Cisco AVVID.
BRI	Basic Rate Interface. Siehe auch PRI.

C

CAC	Anrufzugangskontrolle (Call Admission Control)
CAS	Channel Associated Signaling
CBWFQ	Weighted Fair Queueing (Class Based Weighted Fair Queuing, Klassen-basierte)
CDP	Cisco Discovery Protocol
CIR	Committed Information Rate
Cisco AVVID	Cisco-Architektur für Sprache, Bilder und integrierte Daten (Voice, Video, Integrated Data)
CLID	Rufnummernanzeige (Calling Line ID)
CO	Fernsprechvermittlungsstelle (Central Office)
Codec	Codierer-Decodierer
CoS	Class of Service

CPE	Ausrüstung der Kundenbüros (Customer Premised Equipment)
cRTP	Komprimiertes Echtzeit-Transportprotokoll (Compressed Real-Time Transport Protocol)

D

DDI	Direkte Einwahl (Direct Dial Inward)
DHCP	Dynamic Host Configuration Protocol
DID	Direkte Einwahl (Direct Inward Dial)
DN	Verzeichnisnummer (Directory number)
DNIS	Dienst zur Identifizierung der gewählten Nummer (Dialed Number Identification Service)
DSCP	Differenzierter Servicepunkt (Differentiated Services Code Point)
DSP	Digitaler Signalprozessor
DTMF	Mehrfrequenzwahlverfahren (Dual Tone Multifrequency)

E – F

E1	Digitales großflächiges Übertragungsschema. E1 ist das europäische Äquivalent einer T1-Leitung.
E&M	Empfangen und Übermitteln (oder Ear and Mouth)
EIGRP	Enhanced Interior Gateway Routing Protocol
FB	Im Sendebetrieb (Forward-Busy)
FIFO	First-in, First-out
FNA	Senden-keine-Antwort (Forward-No-Answer)
FXO	Foreign Exchange Office
FXS	Foreign Exchange Station

G – H

GK	Gatekeeper
-----------	------------

GW	Gateway
H.323 RAS	Registrierung, Zulassung (Admission) und Status
HSRP	Hot Standby Routing Protocol

I – L

IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
ISDN	Integrated Services Digital Network
ITU-T	Telekommunikations-Standardisierungssektor der ITU
IVR	Integrated Voice Response
JTAPI	Java-Telefonie-API. Siehe auch TAPI.
LBR	Low-Bit-Rate
LCD	Flüssigkristallanzeige (Liquid Crystal Display)
LDAP	Lightweight Directory Access Protocol
LFI	Verbindungsfragmentierung und -verschachtelung (Link Fragmentation and Interleaving)
LLQ	Queueing mit niedriger Latenzzeit (Low Latency Queuing)

M

MCM	Multimedia Conference Manager
MCS	Medienkonvergenz-Server (Media Convergence Server)
MGCP	Media Gateway Control Protocol
MIME	Multipurpose Internet Mail Extension
MLPPP	Multilink Point-to-Point Protocol
MTP	Media Termination Point
MWI	Message Waiting Indicator

N – Q

NIC	Netzwerkkarte (Network Interface Card)
OSPF	Open Shortest Path First
PBX	Nebenstellenanlage (Private Branch Exchange)
PCM	Puls Code Modulation
PFC	Policy Feature Card
PGP	Pretty Good Privacy
POTS	Herkömmliches Telefonnetz (Plain Old Telephone Service)
PQ	Prioritätengesteuerte Warteschlangen (Priority Queueing)
PRI	Primary Rate Interface
PSTN	Öffentliches Fernsprechwählnetz (Public Switched Telephone Network)
PVID	Port-VLAN-ID
QoS	Quality of Service

R

RAS	Protokoll für Registrierung, Zulassung (Admission) und Status
Routing-Liste	Ersetzt den Routing-Point im CallManager 3.0.
RRQ	Registrierungsanfrage (Registration Request)
RSVP	Ressourcen-Reservierungs-Protokoll
RTP	Echtzeit-Transportprotokoll (Real-Time Transport Protocol)

S

SA/DA	Sendeadresse/Zieladresse (Sending Address/Destination Address)
Skinny Station Protocol	Ein Cisco Protokoll mit Meldungen niedriger Bandbreite, die die Kommunikation zwischen den IP-Geräten und dem Cisco CallManager führen.
SMDI	Simplified Message Desk Interface (oder Station Message Desk Interface)

SMTP Simple Mail Transfer Protocol

SNMP Simple Network Management Protocol

T – U

TAPI Telefonie Application Programming Interface. Siehe auch JTAPI.

TDM Time Division Multiplexing

TFTP Trivial File Transfer Protocol

ToS Type of Service

UPS Unterbrechungsfreie Stromversorgung (Uninterruptible Power Supply)

V

VAD Sprachaktivitätserkennung (Voic Activity Detection)

VIC Voice Interface Card

VLAN Virtuelles LAN

VoIP Voice over IP

VPIM Sprachprofil für Internetmeldungen (Voice Profile for Internet Messaging)

VVID Voice-VLAN-ID

W – Z

WRED Gewichtete zufällige Früherkennung (Weighted Random Early Detection)

WRR Gewichteter zyklischer Warteschlangenbetrieb (Weighted Round-Robin)



A

Adressen **2-12, 2-16**
ANI **11-6**
Anrufauswahlzone **5-8, 5-9**
Anrufdetaildatensatz (Call Detail Record
= CDR) **11-1**
Anruferumwandlung **5-6**
Anrufzugangskontrolle **3-10, 3-12, 6-3**
 für die zentrale Anrufverarbeitung **7-2**
 für QoS **8-10**
Gatekeeper **3-10, 6-7, 6-11**
Standorte **3-12, 7-3**

B

Bandbreite
 für verteilte Systeme **6-13**
 pro Anruf **3-10**
 Versorgung für WAN **8-4**
Berichte für die
 Netzwerkmanagement **11-13**
Bestehendes System **10-1**

C

Campus-Infrastruktur **2-1**
Campus Manager **11-8**
Catalyst Switches **9-1**
 4000-Familie **9-10**
 6000-Familie **2-22, 9-12**
 Conferencing **9-3**
 Transcoding **9-5**
CDP **2-13, 11-1**

CDR **11-1**

Cisco CallManager-Cluster **3-1**

Cisco Discovery Protocol (CDP) **2-13, 11-1**

CiscoWorks2000 **11-1, 11-6, 11-10**

Asynchronous Network Interface
(ANI) **11-6**

Campus Manager **11-8**

Common Management Framework
(CMF) **11-6**

Resource Manager Essentials
(RME) **11-12**

User Tracking (UT) **11-9**

Class of Service (CoS) **2-18**

Cluster **3-1**

 für verteilte Systeme **6-15**

 für zentrale Systeme **7-4**

Größe **3-1**

Kommunikation in einem Cluster **3-4**

Kommunikation zwischen Clustern **3-9**

 mit verteilter Anrufverarbeitung **3-10**

 mit zentraler Anrufverarbeitung **3-12**

Nutzung **3-9**

Richtlinien **3-7**

CMF **11-6**

Common Object Request Broker
Architecture (CORBA) **11-3**

Conferencing **9-3**

CORBA **11-3**

CoS **2-18**

D

Datenbank

 Publisher **3-1, 3-4**

 Subscriber **3-4**

Designziele 1-1
 DHCP 2-12
 Digital Signal Processor (DSP) 9-1
 Dokumentation
 beziehen 3
 CD-ROM 3
 World Wide Web 3
 DSP 9-1
 für verteilte Systeme 6-15
 für zentrale Systeme 7-5
 Dynamic Host Configuration Protocol
 (DHCP) 2-12

E

Einzelner Standort 1-3
 Empfängerumwandlung 5-6
 Ethernet 2-3
 Externes Patch Panel 2-10

F

Funktionstransparenz 3-15
 Für die Gateway-Auswahl erforderliche
 Funktionsmerkmale 4-1

G

Gatekeeper 3-10, 6-7, 6-11
 Gateways 4-1
 erforderliche Funktionsmerkmale 4-1
 Liste 4-1
 Standortanforderungen 4-3
 unterstützte Protokolle 4-1
 unterstützte
 Standortanforderungen 4-4
 Geräte
 Gewichtung 3-1, 3-2

In Route-Gruppe 5-5
 Sitzungen 3-2
 Gerätegewichtung 3-1, 3-2

H

H.323 in Verwendung bei
 VoIP-Gateways 4-1
 Hervorhebungen und Markierungen 1
 Hohe Verfügbarkeit 2-5

I

Ideale Vorgehensweisen für QoS 8-9
 Infrastruktur 2-1
 Inline-Strom 2-7
 Intercluster-Kommunikation 3-9
 Interface-Queueing 8-2
 Intracluster-Kommunikation 3-4
 IP-Adressen 2-12, 2-16
 IP-Telefone 2-15
 Adressen 2-12, 2-16
 externe Stromversorgung 2-10
 Innenleben 2-3
 Strom 2-7
 Strom aus der Steckdose 2-12
 Stromverbrauch 2-9
 IP-Telefonie
 Designziele 1-1
 Netzwerkmodelle 1-2

K

Kommunikation
 in einem Cluster 3-4
 zwischen Clustern 3-9
 Komprimieren von Sprachsignalen 9-6
 Konventionen in diesem Handbuch 1

L

LAN-Infrastruktur **2-1**

M

Management Information Base
(MIB) **11-2**

Maske für Ziffernübersetzung **5-6**

Media Gateway Control Protocol
(MGCP) **4-1**

Media Termination Point (MTP) **9-5**

Migration auf ein
IP-Telefonie-Netzwerk **10-1**

MGCP **4-1**

MIB **11-2**

MTP **9-5**

Multisite **1-5**

mit unabhängiger
Anrufverarbeitung **1-5**

mit verteilter Anrufverarbeitung **1-7, 6-1**

mit zentraler Anrufverarbeitung **1-9, 7-1**

N

Netzwerkdesign **1-1**

Einzelner Standort **1-3**

Infrastruktur **2-3**

mehrere Standorte mit unabhängiger
Anrufverarbeitung **1-5**

mehrere Standorte mit verteilter
Anrufverarbeitung **1-7**

mehrere Standorte mit zentraler
Anrufverarbeitung **1-9**

Modelle **1-1**

Topologie **1-1**

Zusammengesetztes Modell **1-1**

Netzwerkmanagement **11-1**

O

Off-Net-Route-Muster **5-8**

On-Net-Route-Muster **5-7**

P

Partitionen **5-8, 5-9**

PBX-Migration **10-1**

Physikalische Verbindungen **2-6**

Protokolle

CDP **2-13**

DHCP **2-12**

für PBX und Voice Messaging **10-2**

H.323 **4-1**

Media Gateway Control Protocol **4-1**

Skinny Gateway Protocol **4-1**

unterstützt in VoIP-Gateways **4-1**

PSTN/ISDN **5-8**

Publisher der Datenbank **3-1**

Q

QoS **2-17, 8-1**

Quality of Service (QoS) **2-17**

Queueing **8-2**

R

Redundanz **2-5, 3-4**

Redundanzgruppen **3-4**

Remote-Bedienbarkeit **11-1**

Ressourcenverbrauch **3-2**

RME **11-12**

Route-Gruppe **5-1, 5-5**

Route-Liste **5-1, 5-4**

Route-Muster **5-1, 5-4**

Off-Net 5-8

On-Net 5-7

S

SAC 11-3

SAenvProperties.ini-Datei 11-3

Schutz vor Stromausfall 2-3

Server

pro Cluster 1-4

TFTP 3-1

Service

Class 2-18

Quality 2-17

Type 2-18

Simple Network Management Protocol
(SNMP) 11-2

Sitzungen 3-2

Skinny Gateway Protocol 4-1

SNMP 11-2

Sprachkomprimierung 9-6

Standortanforderungen für die
Gateway-Auswahl 4-3

Standorte 3-12, 7-3

Strom

Anschlüsse 2-10

Empfehlungen 2-12

externes Patch Panel 2-10

Inline 2-7

IP-Telefone 2-7

Schutz 2-3

Steckdose 2-12

unterbrechungsfreie
Stromversorgung 2-3

Verbrauch 2-9

vom Catalyst Modul 2-7

Strom aus der Steckdose 2-12

Subscriber der Datenbank 3-4

Syslog

Analyzer Collector (SAC) 11-3

Berichte 11-13

Collector 11-1, 11-3

Empfänger 11-3

Komponenten 11-3

Message Filtering 11-14

Protokollverwaltung 11-13

Verwaltungsschnittstelle 11-4

Warnungen 11-15

T

TFTP-Server 3-1

Tools für QoS 8-4

ToS 2-18

Transcoding 9-5

Transparenz der Funktionen 3-15

Type of Service (ToS) 2-18

U

Übersetzung von Ziffern 5-6

UDP 11-3

Umwandlung von Ziffern 5-6

Unabhängige Anrufverarbeitung 1-5

Uninterruptible Power Supply (UPS) 2-3

UPS 2-3

User Datagram Protocol (UDP) 11-3

User Tracking (UT) 11-9

UT 11-9

V

Verbindungen

IP-Telefon 2-6

Mit dem Netzwerk 2-15

PC 2-6
Verbindungseffizienztechniken 8-7
Verbrauch von Ressourcen 3-2
Verfolgungspfadanalyse 11-10
Verkehr
 Klassifizierung 2-18, 2-19, 2-22, 8-1
 Setzen von Prioritäten 8-5
 Steuerung 8-8
Verteilte Anrufverarbeitung 1-7, 3-10, 6-1
Vertrauensgrenzen 2-18
VLAN 2-13, 2-14
Voice Messaging
 für verteilte Systeme 6-17
 für zentrale Systeme 7-7
 Migration auf ein IP-Netzwerk 10-1
Voice-VLAN-ID (VVID) 2-14
VVID 2-14

W

Wählplan 5-1
 Anrufauswahlzone 5-8
 für verteilte Systeme 6-11
 Partitionen 5-8
WAN
 Bandbreitenversorgung 8-4
 Multisite mit verteilter
 Anrufverarbeitung 6-1
 Multisite-WAN mit zentraler
 Anrufverarbeitung 7-1
 QoS 8-1
Warnungen 11-15

Z

Zentrale Anrufverarbeitung 1-9, 3-12, 7-1
Ziele 1-1
Ziffernübersetzung 5-6

Zugangskontrolle 3-10, 3-12, 6-3
 für die zentrale Anrufverarbeitung 7-2
 für QoS 8-10
 Gatekeeper 3-10, 6-7, 6-11
 Standorte 3-12, 7-3
Zusammengesetztes Modell 1-1
Zusätzliche Dienste
 unterstützt in IOS H.323-Gateways 4-2
Zusätzliche Informationen 2

