White Paper

The Medical-Grade Network: Helping Transform Healthcare

Authors
Mike Gibbs
Howard Quillen

Cisco Internet Business Solutions Group (IBSG)

Table of Contents

The Medical-Grade Network 1

Helping Transform Healthcare 1
Persistent Business Challenges 1
Minimizing Costs 1
More Patients, Fewer Caregivers 2
New Care Model 2
MGN: Providing a Foundation for a Connected Healthcare Ecosystem 3
Inside the Medical-Grade Network 5

Medical-Grade Network Architecture 5

Networked Infrastructure Layer 6
WAN/MAN 8
Data Center 10
Data Center Core Layer 10
Data Center Aggregation Layer 10
Data Center Access Layer 10
Server Cluster Model 11
Multitiered Data Center Model 11
Multitiered Server Farms 11
Data Center Storage Services 11
Data Center Edge 12
Campus 12
Campus Core Layer 12
Campus Distribution Layer 13
Campus Access Layer 13
Enterprise Edge 15
Clinic/MOB 16
Small Office/Telemedicine Site 17
Interactive Services Layer 18
Security Attributes 19
Outbreaks 21
Noncompliant Devices 21
Unauthorized Access 21
Denial of Service 22
Secure Sockets Layer 22
Transparent LAN Service 22
Identity-Based Networking Services 22
Data Center Security 24
Clinic Security 25
Clinic/MOB IP Security 25
Intrusion Detection System 26
Intrusion Prevention System 26
Network Admission Control 26
Remote Clinician Security 27
Business-/Clinician-Ready Teleworker VPNs 28
Teleworker IP Telephony Security 29
Broadband Access Technologies 29
Digital Subscriber Line 29
Cable 29
Satellite 30
IP Telephony Security 30
IP Communications Security Design 30
Mobility Attributes 31
Secure Wireless 34
Passive Attacks 34
Active Attacks 35
WLAN QoS 35
Guest Access 36
WLAN IP Multicasting 36
High Availability 36

Radio Resource Management 37

Automated Interference Avoidance and Power Adjustment 37
Optimized Per-User Performance Through User Load Balancing 37
Asset and Staff Management 37
Location 37
Wi-Fi Location System and Chokepoint System 38
Medical Electromagnetic Compatibility Standards 39

Wireless Architectural Design 39

WLAN Deployment Models 39
Site Survey 41
RF Design Planning 41

Table of Contents (*Continued*)

Data Rate Settings 42
Power Levels 42
Antenna Selection 42
Channel Selection 42
RF Environment 43
RF Deployment Best Practices 43
Wireless Networks Are Targets 44
The Components of the Secure Wireless Solution ..44
Authentication 45
Key Management 45
Required Security Extensions 45
IPsec 46
802.1x/EAP 46
EAP Authentication Benefits 46
EAP Authentication Protocols 47
Mobility Solutions 48
Mobile UC Attributes 49
Voice Traffic Characteristics 49
Wireless Networking Challenges 49
Multifaceted Approach to End-to-End Quality of Service 50
Network and Service Management 51
Storage Attributes 52
Storage Area Network Fabric 53
Storage Area Network Extension 53
Storage Virtualization 53
Network-Attached Storage 54
Storage over a Metro-Optical Network 54
Storage over a Wide-Area Network 54
IP Communications Attributes 55
Productivity Applications 56
Open Standards 56
Flexible Reconfiguration of Hospital Spaces 56
Call Admission Control 57
High-Availability Design 57
Session Initiation Protocol 58
Computing Services Attributes 58
Server Clustering 59
Input/Output Virtualization 59
Utility Computing 59
High-Performance Computing 60
InfiniBand Architecture 60
Quality of Service—Service Levels and Flow Control 60
InfiniBand Subnet Management and QoS 61
Remote Direct Memory Access 61
Identity Services Attributes 62
Identity-Based Network Access Control 63
Application-Layer Attributes 63
Application-Integration Attributes 64
Collaboration/Conferencing Attributes 64
Collaboration/Unified Messaging Attributes 66
Unified Messaging 67
Single-Number Reachability 68
Collaboration/Internet Protocol Contact Center Attributes 68
Collaboration/IP Phone Attributes 70
Computer Telephony Integration Applications 72
Collaboration/Video Delivery Attributes 72
End-to-End IP Video Connectivity 74
Advanced Technologies and Flexible Architecture Combine to Meet Changing Clinical and Business Needs 75
Glossary 76

The Medical-Grade Network: Helping Transform Healthcare

The Medical-Grade Network

Helping Transform Healthcare

Healthcare organizations worldwide are turning to information technology to cope with mounting pressures to reduce costs and improve quality and safety. They are using technology to create an integrated system of care that connects patients, clinicians, payers, and support organizations so that all key stakeholders can exchange information more effectively.

The Cisco® Medical-Grade Network (MGN) provides the industry-specific framework required to meet healthcare's unique needs for interoperability, security, availability, productivity, and flexibility.

Persistent Business Challenges

A number of business challenges confront the healthcare industry. Among these are service quality, safety, rising costs, and a shortage of skilled staff to meet the needs of an ever-expanding number of patients with an increasingly complex burden of illness. Meeting these challenges requires a shift from acute episodic care to preventive and long-term chronic care management. This new care model must be supported by interoperable health information technology and patient-centric care systems.

Minimizing Costs

Controlling costs and administrative waste, while delivering high-quality care, is a primary concern for clinicians and those who pay for healthcare—including insurance companies, employers, patients, governments, and taxpayers. In a May 2006 report, the Centers for Medicare and Medicaid Services estimated that annual health expenditures in the United States would reach $1.9 trillion in 2006, rising to more than $2.4 trillion by 2015. Healthcare costs have risen from 7.2 percent of the gross domestic product (GDP) in 1965 to more than 16 percent today. These costs are projected to be 20 percent of the GDP in just under a decade.

Rising healthcare costs are a global concern, with significant increases seen in several countries in the European Union and Canada. According to the Organization for Economic Co-operation and Development, healthcare spending accounted for 10.9 percent of the GDP in Switzerland, 10.7 percent in Germany, 9.5 percent in France, and 9.7 percent in Canada.

According to the Centers for Disease Control and Prevention (CDC), chronic conditions account for approximately 75 percent of all U.S. healthcare costs. Uninsured or underinsured patients who have acute conditions usually lack basic healthcare access, and without routine preventive care, their conditions can become chronic. The CDC estimates that by 2013, 56 million people in the United States under the age of 65 (nearly 28 percent of the workforce) will not have insurance.

Unnecessary spending also is driving up costs. A 2003 study published in the *Annals of Internal Medicine* reported that 30 percent of healthcare expenditures are unnecessary and wasteful. This is largely the result of inefficient healthcare practices, such as redundant testing, unnecessary hospital admissions, and manual paperwork. In 2004, Harvard Medical School researchers reported that the United States spent $399 billion annually on healthcare bureaucracy—essentially the administrative costs of insurers, hospitals, physicians, nursing homes, and other health-related institutions.

More Patients, Fewer Caregivers

The following statistics show an alarming increase in the number of patients and a decrease in workforce personnel:

- On October 17, 2006, the U.S. Census Bureau announced that the U.S. population had surpassed 300 million—a population increase of more than 5 percent in just five years. The Census Bureau predicts that the U.S. population will increase to 392 million by 2050—a number nearly 50 percent larger than the population in 1995. Yet the *Journal of the American Medical Association* reports that there has been a steady decline in the number of U.S. medical school graduates choosing primary care. Coupled with the worldwide aging population, the skilled staff shortage is reaching crisis levels.
- According to the United States Department of Health and Human Services, there was a 6 percent nursing shortage in 2000; that shortage will double by 2010, resulting in a deficit of 275,000 full-time registered nurses. By 2015, the shortage is expected to more than triple to 20 percent and will escalate to 29 percent by 2020. To offset the widening gap between the number of patients and the number of skilled staff, healthcare organizations must increase their productivity.

New Care Model

To improve healthcare outcomes while decreasing costs, healthcare organizations are emphasizing outpatient and preventive care. Collaborative technologies can play a major role in this new care model by creating new synergies and improving the efficacy of treatment modalities.

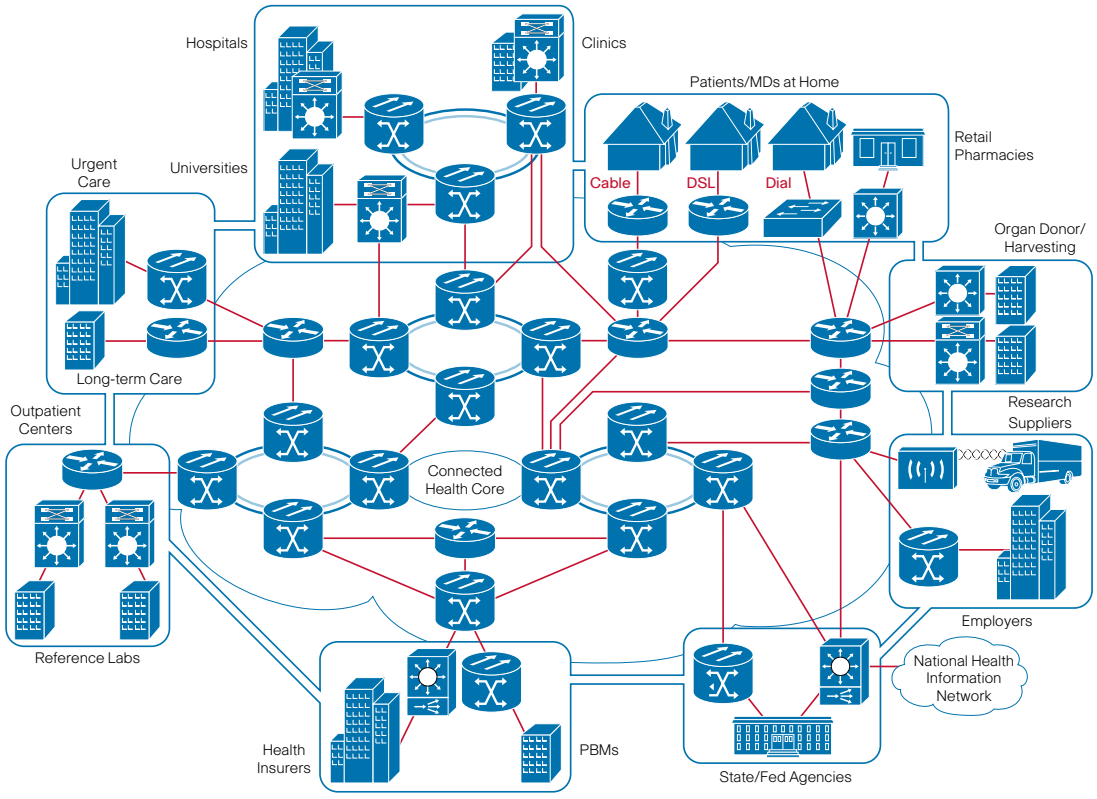
In this new model, patients assume greater responsibility for their personal healthcare, advocating for themselves as healthcare consumers. As a result, they need access to information about their own health and clinicians. Through the Internet and other information sources, patients can access information about treatment protocols and alternatives. In the competitive healthcare world, the transparency of patient and practitioner information may influence practitioner selection and retention. As a result of the increased availability of information, patients are demanding higher-quality services.

The MGN plays a critical role in this new care model by facilitating information sharing across the healthcare delivery system. The network provides the platform for exchanging reliable, accurate, and consistent patient information. This provides the foundation for a connected health ecosystem.

MGN: Providing a Foundation for a Connected Healthcare Ecosystem

Several decades ago, a single physician treated all of a patient's various illnesses. Today, a patient receives treatment from multiple physicians and clinics. This creates the need for medical and clinical information to be shared securely among many healthcare entities. To provide the framework for this new healthcare world, a connected healthcare ecosystem is needed—where networked resources of medical information, knowledge support, and process optimization are all parts of the system. Figure 1 illustrates the envisioned connected health ecosystem where information is quickly and reliably exchanged.

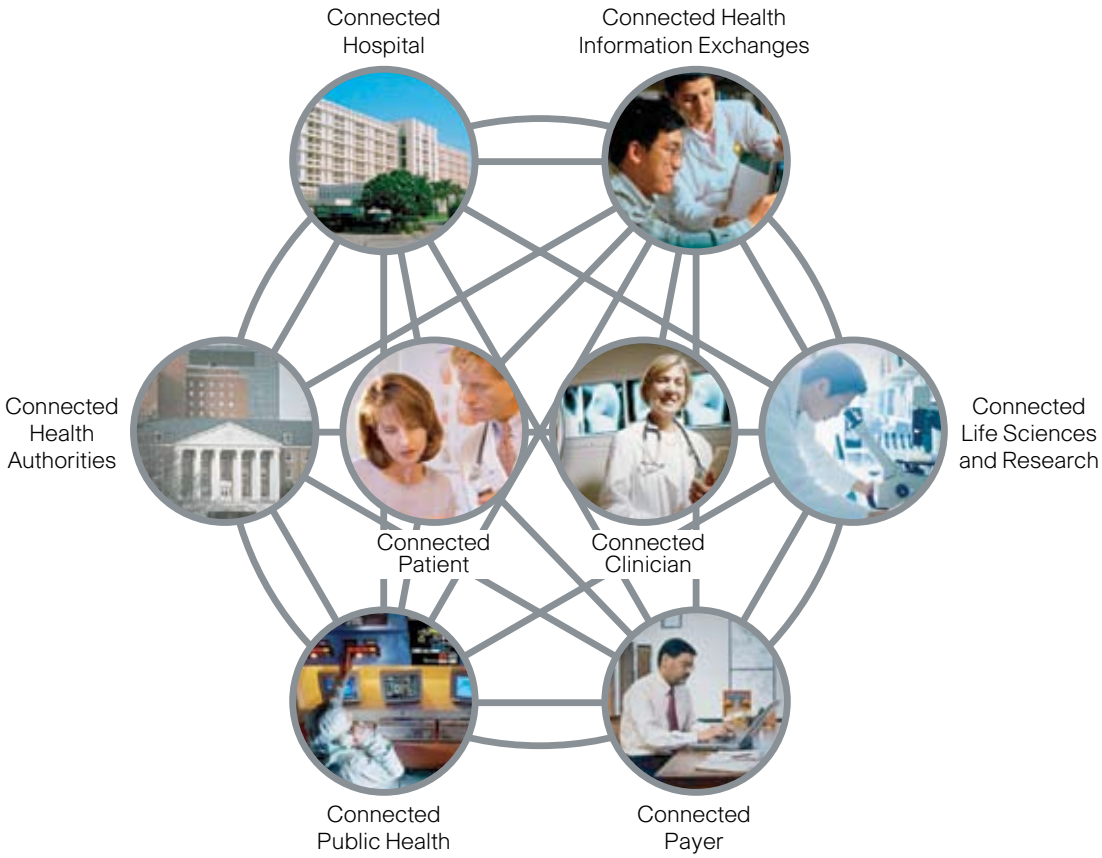
Figure 1. Connected Healthcare Ecosystem Vision



For many healthcare organizations, the first step is to use technology to create a platform where information can be collected and exchanged electronically. The MGN creates the foundation technology from which this information can be appropriately disseminated within the hospital or healthcare system, paving the way for a connected healthcare ecosystem that addresses the business challenges discussed in this paper.

The MGN helps create collaborative relationships that lead to a connected healthcare community with interoperable processes, technology, and people to provide information anywhere, anytime. The resulting patient benefit is the delivery of safe, affordable, efficient, and accessible healthcare. Figure 2 illustrates the beneficiaries within this community.

Figure 2. Interoperable Healthcare Ecosystem



The MGN meets healthcare's unique needs for security, availability, productivity, flexibility, and interoperability by providing integration with each functional area. These capabilities optimize interactions among healthcare participants, processes, applications, and hardware components. The MGN facilitates and integrates diverse business and clinical communications across the continuum of care.

The MGN also meets the storage requirements of the healthcare environment by enforcing identity- and policy-based privacy and security from inside the network to beyond organizational walls. The network also securely stores large amounts of data for extended time periods.

The acute care environment often demands around-the-clock data availability. The MGN's high-availability design can support this requirement along with the convergence of data, voice, video, and imaging. In addition, it enables real-time access to people and information when and where it is needed.

By automating workflow and collaboration, the network helps optimize clinical and business processes; the clinical applications that run on the network now augment clinicians' professional skills.

Access to healthcare, 24 hours a day, seven days a week, is not limited to just healthcare workers; patients and their families demand increased access to their clinicians, regardless of location. The MGN supports clinical requirements offsite, enabling remote collaboration on a global scale. This is driving new solutions, such as the Cisco TelePresence and Collaborative Care conferencing solutions.

The MGN promotes strict adherence to required healthcare service levels. Because each healthcare organization has different business requirements, the network is designed to support service-level requirements based on specific business and clinical needs.

All components of the MGN's end-to-end-framework function cohesively to maximize performance and minimize integration challenges, reducing the network's operational expenses and the capital necessary to procure equipment.

Inside the Medical-Grade Network

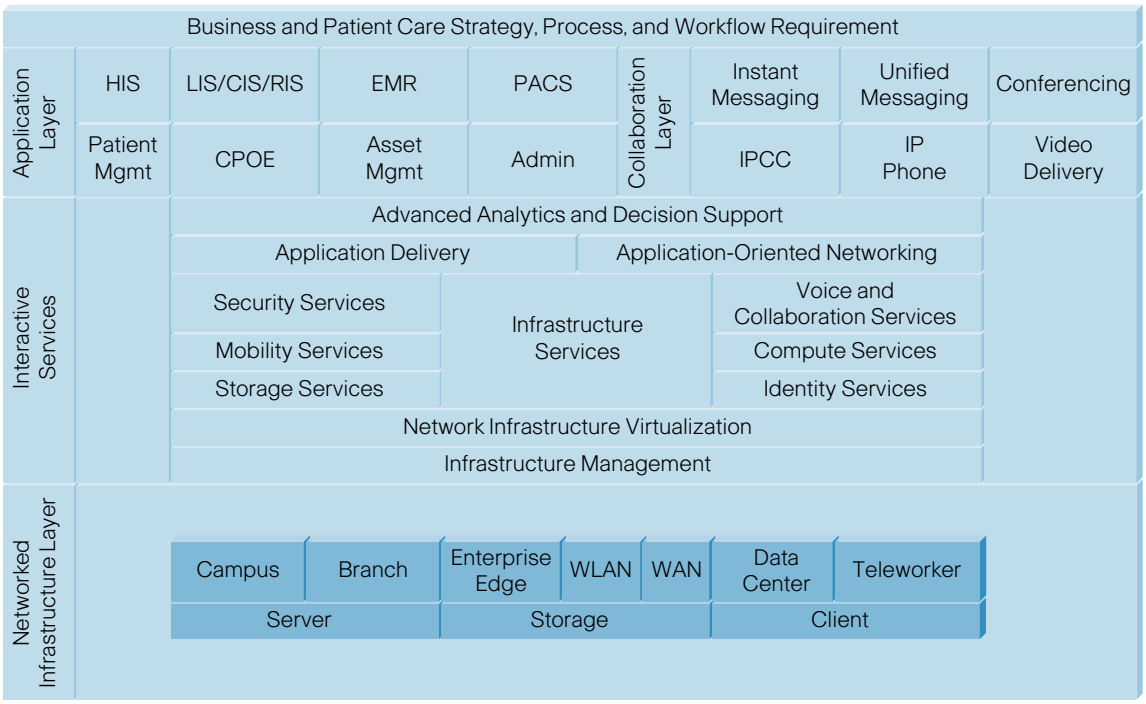
The MGN meets today's healthcare needs while laying the foundation for future requirements. It is based on Cisco's modular Service-Oriented Network Architecture (SONA), which means that new applications, technologies, and equipment can be added easily to the network.

The MGN framework is segmented into three layers: networked infrastructure layer, interactive services layer, and application layer. Each layer enables system-wide communications, allowing the network to operate efficiently and disseminate clinical and business information throughout the healthcare system. Each layer will be discussed, in detail, in the rest of this document.

Medical-Grade Network Architecture

The MGN is an end-to-end solution that streamlines operations and supports a variety of medical applications. As stated above, the MGN architecture is built on three layers: the networked infrastructure layer, which provides a converged network foundation that enables secure, reliable, and highly available connectivity to network-enabled devices; the interactive services layer, which enables mobility, security, and more efficient utilization of resources; and the applications layer, which contains the business, clinical, and collaborative applications that are used in the healthcare environment. This section will describe the technical details of the MGN framework.

Figure 3. MGN Architecture Elements



Networked Infrastructure Layer

The networked infrastructure layer is the source of all IT resources that are connected over a single IP network. This layer demonstrates how a fully integrated network enables quality of service (QoS), security, and high availability even in the most demanding healthcare environment. This layer supports traditional functions, such as routing, switching, and transport technology. The attributes that are required for the MGN at the networked infrastructure layer are identified in Figure 5.

Figure 4. Networked Infrastructure Layer—Structure

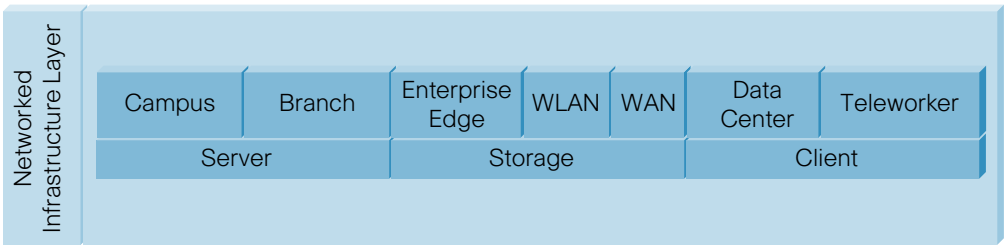


Figure 5. Networked Infrastructure Layer Attributes

Networked Infrastructure Layer Attributes
Network Virtualization · Private VLANs (PVLAN) · Network address translation
Wireless · Convergence of wired/wireless infrastructure, WLAN controllers, access points, VPNs/ VLANs, and distributed antenna systems
High Availability · Spanning Tree Protocol (STP) · Nonstop forwarding (NSF) · Standby Router Protocols (HSRP, VRRP) · Path redundancy · Device redundancy · Stateful switchover (SSO) · High-performance routing protocols (OSPF, EIGRP, BGP, PIM-SM) · In Service Software Upgrade (ISSU), Global Load Balancing Protocol (GLBP) · Application-aware Quality of Service (QoS) · Voice over Wi-Fi support with Fast roaming and WMM (Wi-Fi Multimedia)
Security · Access control lists · Wireless IDS/IPS (Intrusion detection and prevention system) · Wireless rogue devices detection and localization
Scalability · IP multicast · Rate-limiting · Multiprotocol Label Switching (MPLS) · Web Cache Communication Protocol (WCCP) for transparency, load balancing, and failover · Generic Routing Encapsulation (GRE) · Multiple wireless SSIDs
Voice and Multimedia · In-line power—Power over Ethernet (PoE) · Voice over Wi-Fi
Management · Fault and performance indicators (SNMP, syslog, RMON, MIB, NetFlow) · Network management event correlation

The following section details places in the network as they pertain to the networked infrastructure layer. (This section also introduces several interactive services layer components, which are discussed in greater detail later in this document.)

Places in the network refer to locations that require networked interconnectivity. These can include healthcare data centers and campuses, remote clinics, regional facilities, national partners and suppliers, or any other organization that is part of the healthcare ecosystem.

WAN/MAN

Wide Area Networks (WANs) and Metropolitan Area Networks (MANs) provide connectivity between distributed sites, campuses, and/or data centers. The specific transport technology usage is determined by connectivity requirements, such as latency, distance, data replication, and path isolation (network-wide segmented environments). Quality of Service (QoS) is a necessity when voice, video, or multiple types of data traffic need to be differentiated. Voice is more sensitive to latency and loss than other kinds of data traffic. For traffic that requires a timing mechanism, such as voice, video, and audio, as well as traffic that does not have a similar requirement, the QoS classification and policing ensure they receive the expected treatment.

Additional capabilities are required to support healthcare's high-bandwidth, mission-critical applications across a WAN and MAN network. Requirements for deploying voice over IP (VoIP) and videoconferencing include high availability, IP Multicasting (IPmc), and QoS. Most healthcare enterprises rely on private WAN connections, such as Frame Relay, ATM, or leased-line services, to connect their organizations. When deploying a traditional Frame Relay or ATM-based private WAN, network operations must be optimized so that provisioning and management of moves, adds, or changes are not overly complex and costly. The goal is to have reliable connectivity that can be updated easily while scaling to meet evolving business needs.

To address these needs, the MGN framework enables an enterprise to rapidly introduce new healthcare applications and services from the remote clinic, through the campus, to the data center, while reducing operating costs and network complexity. By converging existing voice and data networks onto a single IP-based network, the groundwork is established for advanced, full-featured services, such as IP telephony, unified messaging, and multifunctional call center applications.

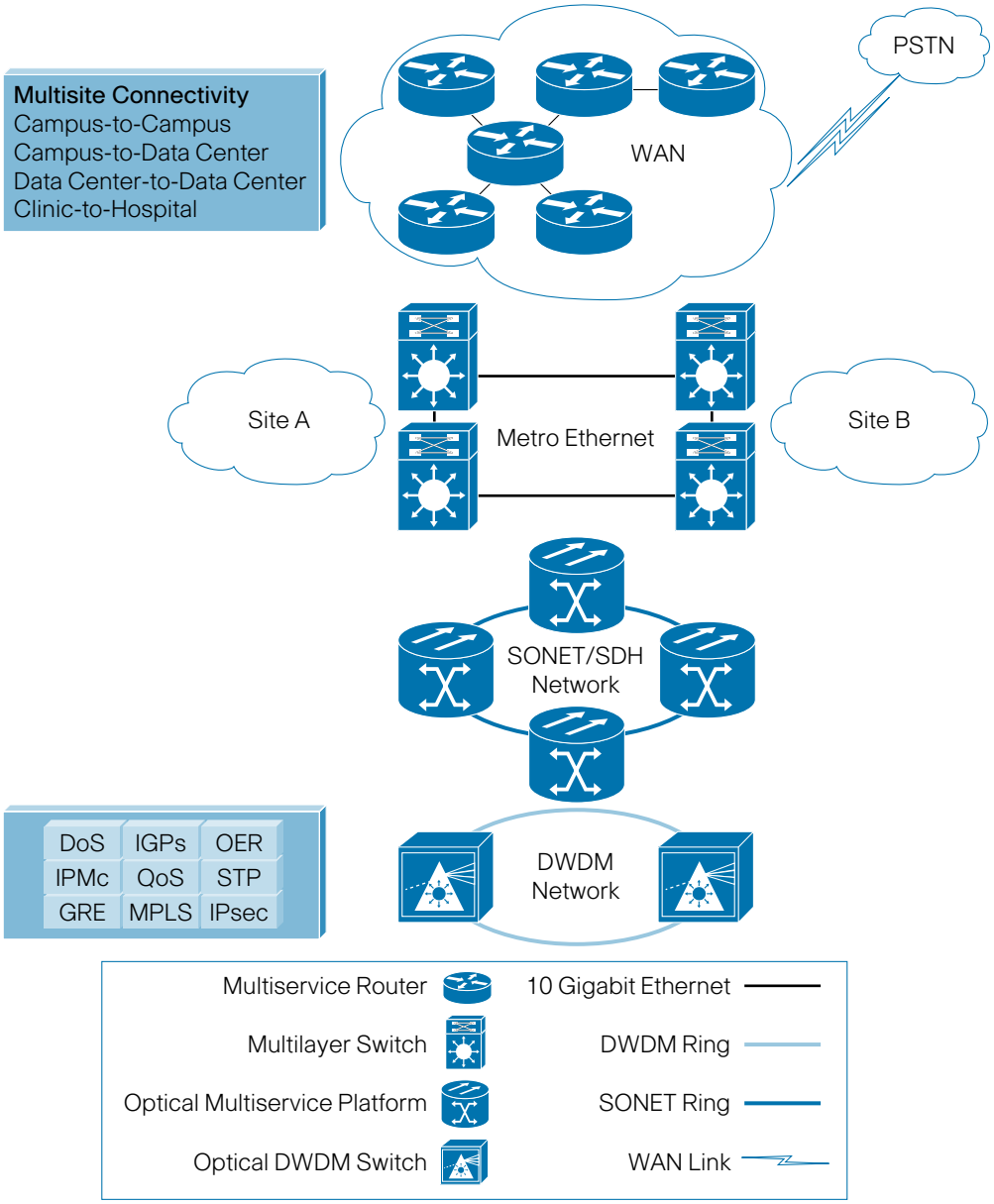
Enterprise WAN and MAN architectures provide numerous options for connecting different locations of patient care, offering multiple technologies to connect data centers, campuses, remote offices, supply chains, call centers, mobile workers, and more. This connectivity promotes greater mobility and collaboration among affiliates. Centralized applications deliver new capabilities, standardize support, and simplify information sharing over the MGN. These intelligent networking solutions, based on embedded device and network-level resiliency, help ensure that patient and treatment data always is securely available wherever it is needed.

Multilayer, multifunctional aggregation routers embed security, connectivity, voice and video services, network analytics, and application acceleration into one device. This reduces the need for separate devices and their associated support costs. The MGN architecture employs a number of MAN and WAN technologies engineered and

optimized to interoperate as a contiguous system. These technologies help connect the entire healthcare ecosystem, provide support for advanced applications, and offer manageability that decreases the time and staff required to grow the network. The MGN MAN/WAN framework includes encrypted private connectivity that takes advantage of existing Frame Relay, ATM, or other connections, and combines them with strong encryption to provide an additional level of security when connecting sites.

Storage services include SAN extension transport, as well as transport for distributed compute farms (EoMPLS, L3VPNs). Large-scale aggregation is used for remote office and multisite connectivity.

Figure 6. WAN/MAN



Data Center

The data center is home to the servers, storage, and applications necessary to support a hospital's clinical and business operations. In a consolidated and centralized architecture, all data and computing resources are supported by the data center's infrastructure. Design considerations include MGN requirements for availability, interactivity, security, and responsiveness. The flexibility to quickly deploy and support new services is another important design aspect. Infrastructure design requires solid initial planning and thoughtful consideration in the areas of port density, access layer uplink bandwidth, true server capacity, and oversubscription. It is vital that patient health data maintain high levels of confidentiality, thereby making security at the data center a critical consideration.

The MGN data center design is based on a layered approach that provides support for Web, application, and database services. This design supports many industry standard Web service architectures, such as those based on Microsoft, .NET, or Java 2 Enterprise Edition. The multitiered model relies on security and application optimization services provided by the network. This design comprises the core, aggregation, and access layers.

Data Center Core Layer

The core layer provides a fabric for high-speed packet switching between multiple aggregation modules. This layer serves as the gateway to the campus core. This is where other modules connect, including the extranet, WAN, and Internet edge.

Data Center Aggregation Layer

The aggregation layer has the primary responsibility of combining multiple sessions leaving and entering the data center. This layer provides integrated security and scalability features, such as server load balancing, firewalling, and SSL offloading to the servers across the access layer switches. The aggregation layer may be the most critical layer in the data center because port density, oversubscription, CPU processing, and service modules introduce unique implications into the overall design. This layer also supports security and application devices and services.

Data Center Access Layer

The access layer is where the servers physically attach to the network. The server components consist of traditional servers, blade servers, clustered servers, and mainframes with open systems adapters (OSAs). The access layer network infrastructure consists of modular switches, fixed configuration switches, and integral blade server switches. These switches provide both routing and switching topologies, fulfilling the various broadcast domain or administrative requirements. The access layer is the most dynamic in the network, and requires special attention due to the frequency of moves, adds, and changes.

Server Cluster Model

The server cluster model is commonly associated with high-performance computing (HPC), parallel computing, and high-throughput computing (HTC) environments. It also is used effectively with grid/utility computing. These designs typically are based on customized and sometimes proprietary application architectures that are built to serve specific business objectives.

Multitiered Data Center Model

The multitiered data center model often is dominated by HTTP-based applications in a multitiered approach. The multitiered model typically includes Web, application, and database tiers of servers. This approach uses software that runs as separate processes on the same machine using Interprocess Communication (IPC) or on different machines that communicate over the network.

Multitiered Server Farms

Multitiered server farms, built with processes running on separate machines, provide improved resiliency and security. Resiliency is enhanced because a server can be taken out of service while the same function is provided by another server belonging to the same application tier. Security is enhanced because an attacker may compromise a Web server without gaining access to the application or database servers. Web and application servers can coexist on a common physical server while, typically, the database remains separate. In the modern data center environment, server clusters are used for many purposes, including high availability, load balancing, and increased computational power. All clusters have the common goal of combining multiple CPUs to appear as a unified, high-performance system using special software and high-speed network interconnects.

Data Center Storage Services

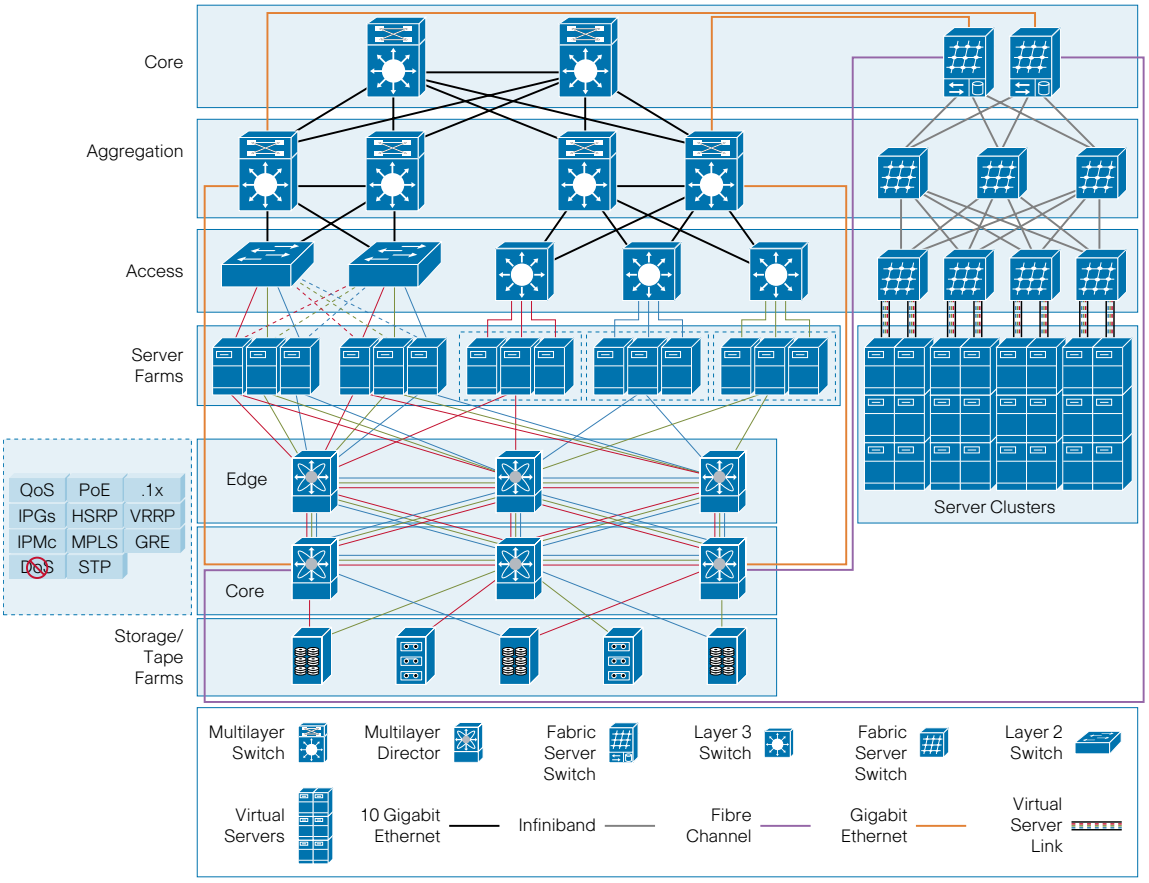
Healthcare data centers are the primary location of health-related information. The data center is where server farms reside and most confidential information is stored. As a result, data centers typically are the main target for information theft and unauthorized access. The data center also is a focus area for network regulations compliance. MGN storage environments benefit from increased storage utilization and simplified manageability. To achieve these benefits, the SAN architecture is scalable and flexible. It supports virtual SANs (VSANs), inter-VSAN routing, virtualization, congestion control, and high QoS. Storage services include high-availability storage fabric, isolation of SAN

islands (VSANs), remote tape backup (write acceleration), and data replication.

Data Center Edge

The data center's highest level of protection is at the edge. The edge implements firewall, intrusion prevention, secure sockets layer (SSL) termination, and network segmentation technologies. Through proven security methodologies, most unwanted traffic is stopped at the edge. Attacks not stopped at the edge will be mitigated using other methodologies in other parts of the network. A more in-depth security discussion will occur in the section labeled "Interactive Services Layer."

Figure 7. Data Center



Campus

The campus network comprises the core, distribution, and access layers. This design model affords a hierarchical structure and modularity, thereby improving the interaction between clients and applications with the use of campus service functions.

Campus Core Layer

In an MGN hierarchical model, the individual building blocks are interconnected using the

core layer. The core serves as the network backbone and is designed for performance resiliency. Since the core is tuned for efficiency, minimal feature configuration in the core reduces complexity, limiting the possibility for operational error.

Campus Distribution Layer

The distribution layer aggregates nodes from the access layer. Additionally, the distribution layer creates a fault boundary that provides a logical isolation point in the event of a failure originating in the access layer. Load balancing, QoS, and provisioning ease are key considerations for the distribution layer.

Campus Access Layer

The campus access layer is the first point of entry into the network for edge devices, end stations, and IP phones. The routers and switches in the access layer are connected to two separate distribution-layer switches for purposes of redundancy. A robust access layer provides high availability supported by hardware and software attributes. These attributes include path and power redundancy, QoS, traffic policing, and inline power. Inline power (PoE) is implemented for IP telephony and wireless solutions by enabling simple power redundancy for the voice and multimedia environment.

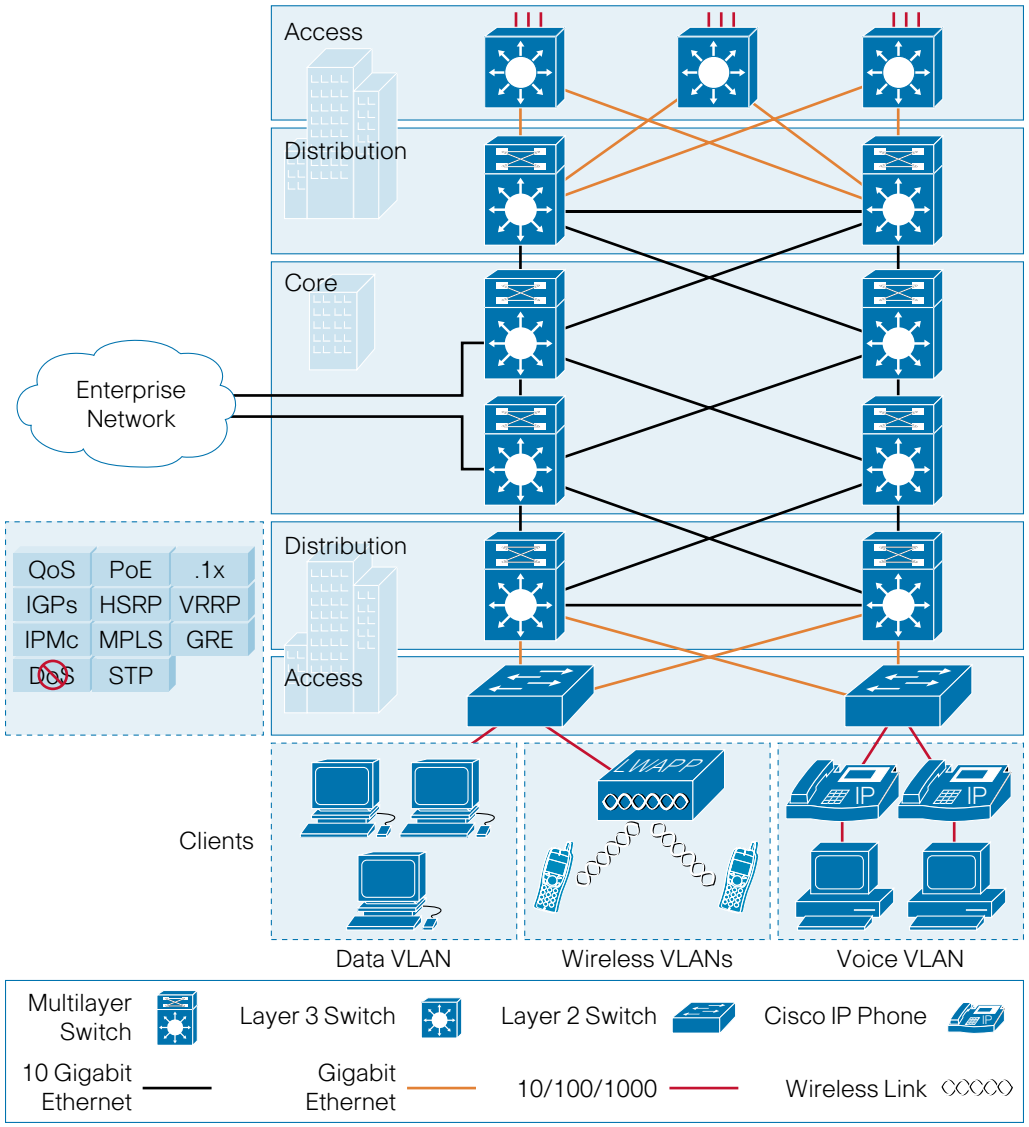
The campus network provides a multiservice environment for current and emerging applications. A healthcare organization may have one or several campuses.

Extensive security risks and threats exist at the campus level. For example, physicians, nurse practitioners, and other roaming clinicians connect to the network with laptops that are not managed by the healthcare system. If a device is infected, it can infect the entire campus network. During a hospital stay, a patient, a patient's family member, or emergency services personnel can attach systems to the hospital's network for EMS reporting purposes. If their systems are compromised, they can infect the healthcare network. The large number of people on the healthcare campus increases the likelihood of unauthorized users or noncompliant devices attempting to gain network access. Without proper security in place, users can bypass external perimeter defenses. The MGN architecture includes significant physical and network security

methodologies to mitigate these risks.

Top security concerns for a campus are device noncompliance, outbreaks, and unauthorized access that can lead to information theft. To this end, the MGN Network Admission Control (NAC) framework systematically enforces endpoint policy compliance. The NAC framework encompasses switches, routers, access points, virtual private network (VPN) appliances, and NAC appliances, thereby enabling flexibility and consistency throughout the network. This section introduces several interactive services layer components, which are discussed in greater detail later in this document.

Figure 8. Campus

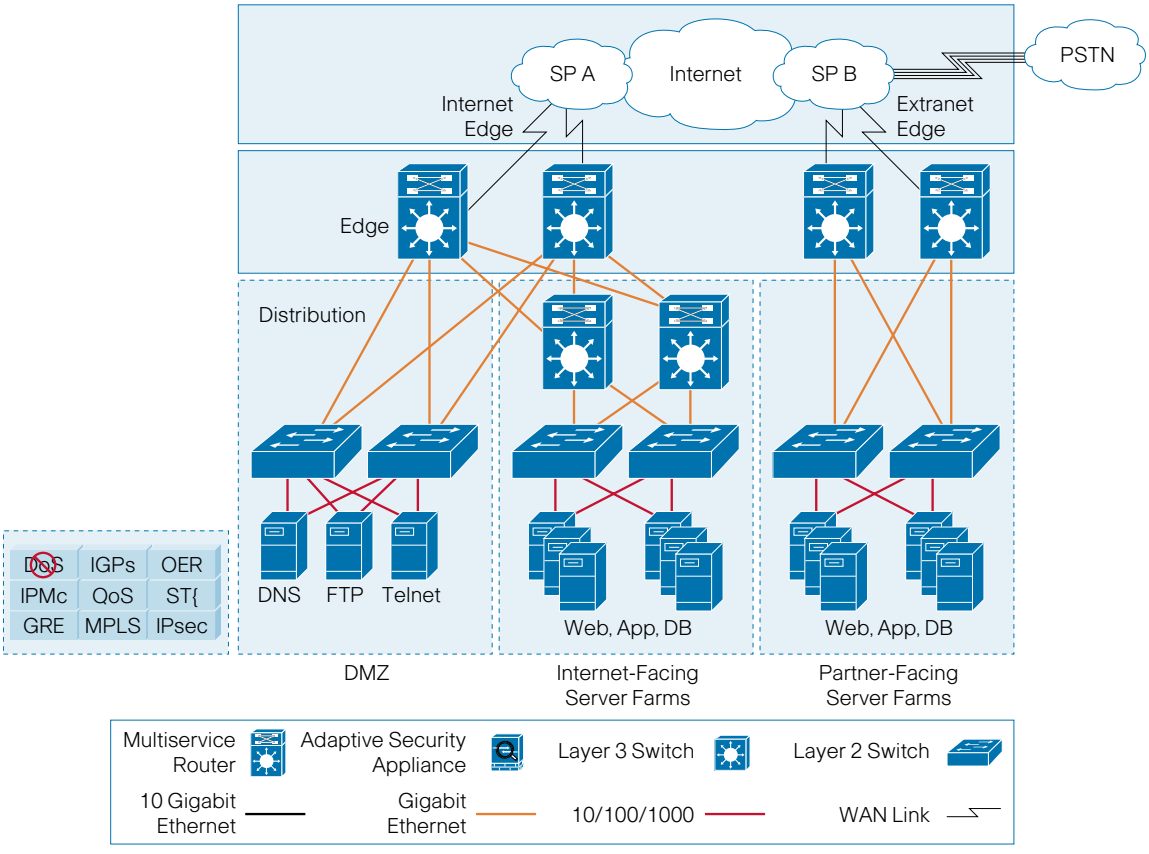


Enterprise Edge

The enterprise edge is the entry point to the Internet and other networks that are external to the healthcare system. Through the consolidation of Internet-facing application environments, the edge is the first line of defense for enterprise networks connected to external networks. The two traditional environments in an enterprise edge are the Internet edge and the extranet. The Internet edge provides enterprise gateway functions in and out of the enterprise network to the Internet while the extranet provides connectivity to business partner networks. The enterprise edge is defined as the area containing the network infrastructure required for a resilient Internet connection. The scope of the area depends on how the enterprise is using the Internet connection.

Connectivity includes all enterprise connections—from facilities to Internet Service Providers (ISP), small or remote office connections using VPN tunnels to access the intranet/Internet, and distributed data center resources. Routing functions ensure Internet access and define the degree of availability of the network edge. Security services are of utmost importance because of the transitional nature of the Internet edge, which represents the outer perimeter of the enterprise. The demilitarized zone (DMZ) provides basic functions for internal or external users, such as domain naming system (DNS), file transfer protocol (FTP), and Telnet. The DMZ area, or Internet edge to the primary network, hosts the public Web servers and the organization's online presence.

Figure 9. Enterprise Edge



Clinic/MOB

The clinic or medical office building (MOB) generally is an extension of healthcare systems. At the clinic, users access the main servers and applications within the data center and require similar access as individuals in the healthcare systems. The clinic is optimized through a converged voice, video, and data network, which provides the foundation for communications, security, and mobility services. This environment demands high availability to provide access to clinical and business applications.

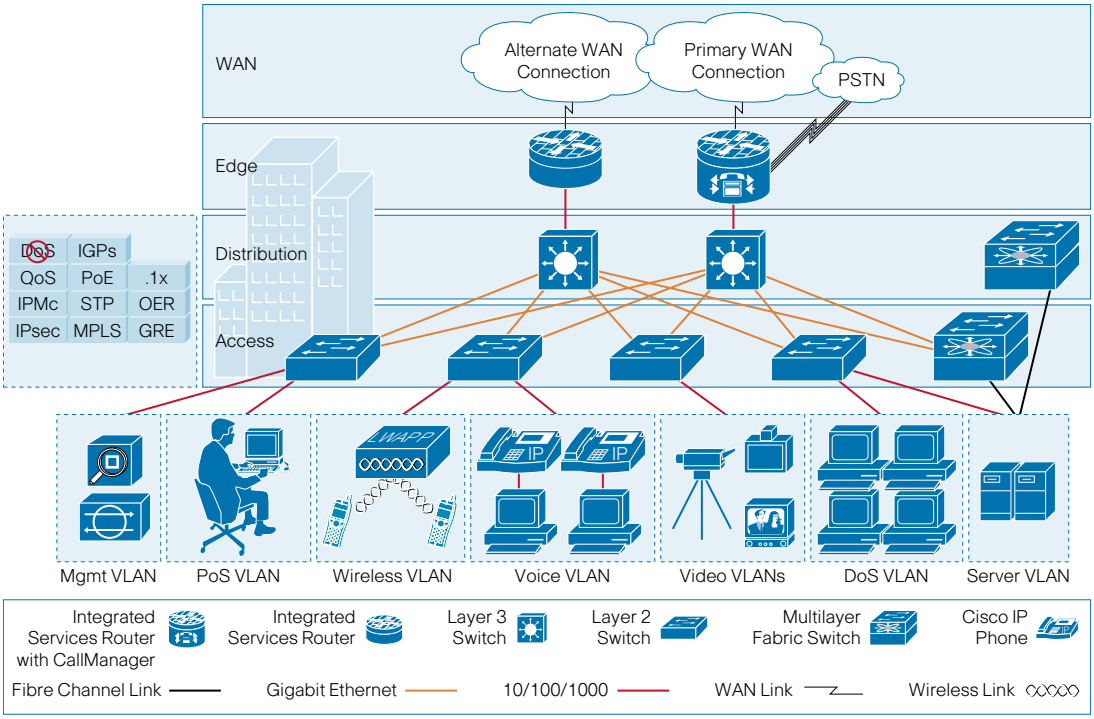
Network services provide end-device connectivity to the corporate network within the clinic. With the convergence of services onto a single network infrastructure, devices such as computers, telephones, and surveillance cameras all need connectivity to the corporate network over the LAN. This assortment of devices requires simplified connectivity tailored to the demands of each device.

To simplify deployment, network devices, such as IP telephones or cameras, may be powered using a LAN switch, automatically assigned an IP address, and placed in a virtual LAN (VLAN) to segment them securely from other devices. Wireless services provide secure mobile access for laptop computers, scanning devices, and wireless IP phones. When deploying a clinic's LAN, it must be determined which devices and services the network needs to support. Other considerations of the network service building block are identified in Figure 10.

Figure 10. LAN Service Considerations

LAN Service Considerations	
Quality of Service (QoS)	Required to maintain high-quality voice or video within the local LAN or wireless LAN. This includes defining trust on ports to prohibit unauthorized QoS usage for preferential treatment of traffic on the office network.
Virtual LAN (VLAN)	Required to segment the office to provide logical division between services. For example, IP telephony should reside on its own VLAN, separate from that used by the data network.
802.1q VLAN tagging	Provides trunking services for IP phones and uplinks to APs or the access router for network routing.
In-line power (PoE)	Provides power to the IP phones, APs, or other IP-enabled devices (for example, IP cameras) over the Ethernet cable.
Port security	Limits the number of MAC addresses allowed on an access port.

Figure 11. Clinic/MOB



Small Office/Telemedicine Site

The small office or telemedicine site provides connectivity for small clinician practices or remote outpatient centers. It furnishes secure, resilient, interactive services to practitioners providing care away from the main healthcare system. Despite small practice size, clinicians at small office locations generally need access to the same applications and services that an on-campus worker needs.

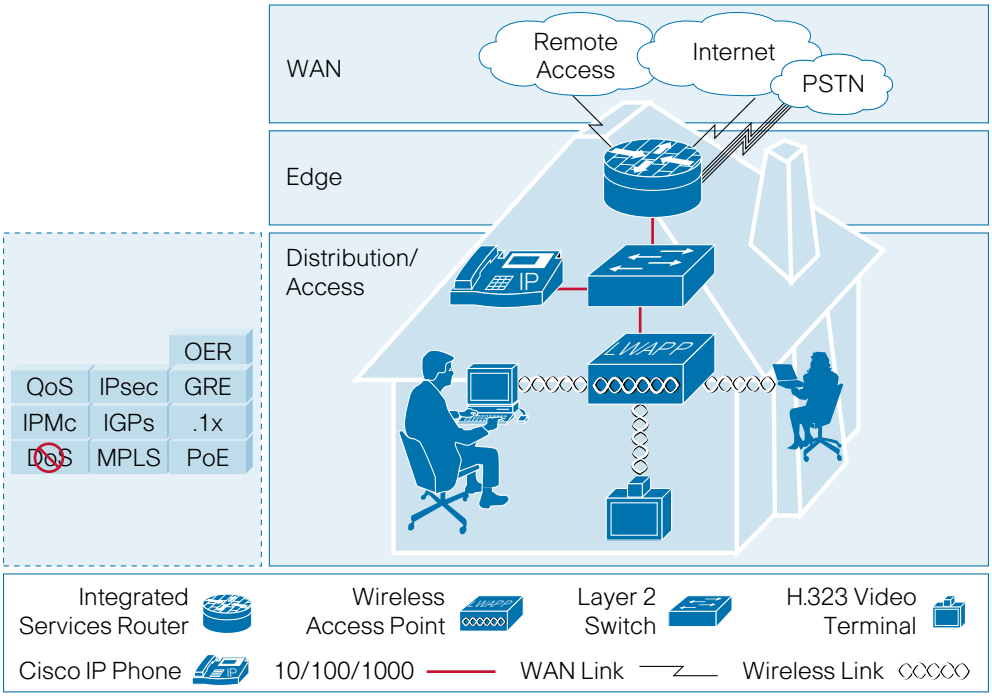
The remote clinic may have a range of WAN connections. If significant IP voice or high-definition video services are required, the office may use private lines or metro Ethernet services. Generally, broadband cable and DSL secured by Internet protocol security (IPsec) provide cost-effective, secure WAN options in this environment. With this large variety of connection options, however, there will be ongoing concerns for data integrity and patient confidentiality.

From a security perspective, special care is required in the small medical office environment. Teleworkers constantly are at risk because they function outside the corporate security perimeter and often lack the latest antivirus and operating system updates. Systems with exposure to the Internet are at risk for day-zero outbreaks, such as newly released worms and viruses for which there are no known antivirus signatures. To mitigate this risk, guest network services can be made available, allowing controlled access to business and clinical resources.

The MGN architecture provides robust support by allowing video, data, and voice to coexist securely in a wired/wireless environment. Integrated voice services include extension mobility for a remote office number dial tone, videoconferencing, and QoS for voice. Integrated wireless and EAP wireless security services also are available in the MGN mobile environment. Additionally, the MGN provides a security agent that prevents execution of any malicious code that penetrates a user's PC.

A broadband gateway is supplied either by the service provider (managed services) or provided by the parent healthcare organization. The ideal choice is a router, which provides firewall, VPN security, and NAC. NAC is enforceable either at the home office with a router or with the edge router at the campus. By enforcing NAC, teleworker machines quickly are scanned, updated, and cleaned from infection.

Figure 12. Small Office/Telemedicine Site



Interactive Services Layer

Centralized, network-based services promote unified administration and heightened performance. The interactive services layer provides direct support for essential applications and the networked infrastructure layer. By using a standardized network foundation and virtualization, interactive services achieve optimal performance and interoperate more effectively than if delivered using standalone devices or networks.

Figure 13. Interactive Services Layer—Structure

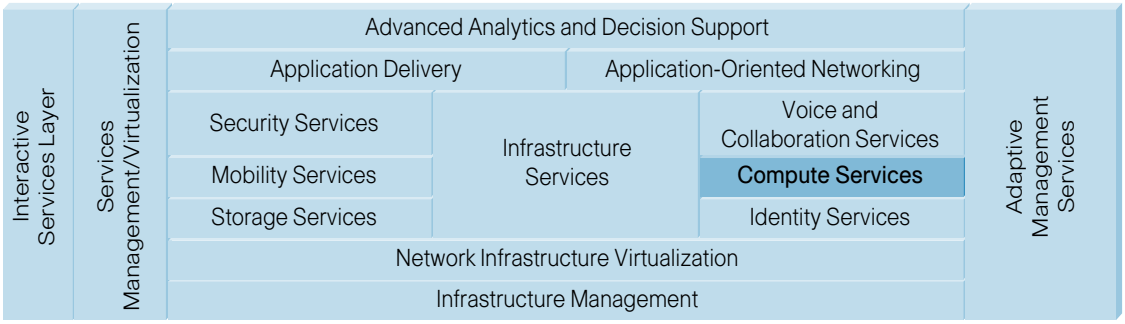


Figure 14 defines the infrastructure services that are crucial for providing a secure, interactive, and collaborative enterprise network environment. The following sections detail these service attributes.

Storage services, such as virtualization, write and tape acceleration, and network-accelerated serverless backup, enhance provisioning flexibility and business-continuance capabilities. Other services, such as adaptive threat defense, virtualized firewalls, and host-based intrusion detection, help secure infrastructure consolidation and virtualization initiatives. Application-delivery services allow consolidation of the infrastructure to centralized locations, making the effective delivery of applications to remote users even more critical.

Figure 14. Interactive Service Layer Attributes

Interactive Services Layer Attributes
Security
IP telephony
Mobility
IPC mobility
Storage
IP communications
Compute services
Identity services

Security Attributes

Data security within the healthcare environment is critical for patient privacy and availability requirements. Information security has a direct relationship with reliability and availability. Additionally, security is necessary to assure data integrity. High availability requires strict security measures to ensure that accidental or intentional system misuse does not degrade system performance to below acceptable service levels. The system must be available to transport data at performance levels that are required to enable caregivers to treat their patients in an accurate and timely manner.

Figure 15. Security—Structure

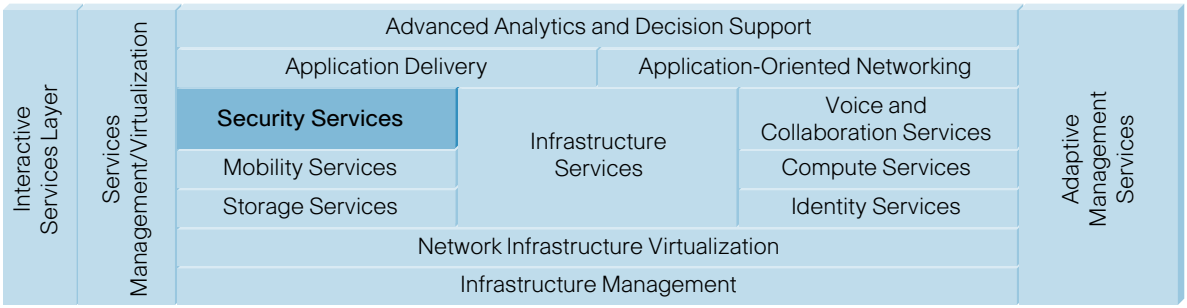


Figure 16. Interactive Services Layer—Security Attributes

Interactive Services Layer—Security	
Self-defending · Integrated security in all network devices · Threat control and containment · Confidential communication · Operational controls	Intrusion detection/day-zero attacks
Endpoint policy enforcement	Rogue device/access-point detection
Network admission control (NAC)	Access control—firewall, IPS, host protection
Data integrity	Data-theft protection
Physical security	VoIP security
Denial-of-service protection	Infrastructure security—switches and routers
Application security	

Information integrity in the data center is vital to patient health. Errors in patient data can lead to mistakes, such as a patient receiving the wrong procedure, erroneous drug administration or interaction, or invalid test results. Data integrity has two primary aspects: error checking to prevent unintentional mistakes and data protection to guard against intentional malfeasance. In terms of privacy, healthcare IT practitioners must follow the relevant regulations regarding patient information. In the United States, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) has motivated many changes in how healthcare organizations treat patient data, from talking in elevators and labeling patient rooms to securing storage facilities and transporting data in digital form. As healthcare delivery service increasingly relies upon the network, preservation of these principles becomes even more important.

Digital radiology, MRI, CT scans, PACS, network-connected bedside devices, PC-based applications, and network-based telemetry are critical systems for patient care. As such, network security becomes even more vital. There are five areas where healthcare organizations must deploy security as part of intelligent networking in their operations.

These are the campus, data center, Internet edge/DMZ, clinical/medical office building, and the small medical office/telemedicine site.

To maintain productivity and resource availability, each of these locations must be protected in a cost-effective manner. Threats to these network locations include outbreaks, unauthorized access to networks and servers, information theft, DoS attacks, and noncompliant devices accessing the network.

Security should be integrated throughout the overall architecture to protect the data integrity and infrastructure assets to the level set forth in the security policy. Furthermore, security should be considered a process, not a product solution.

Any breach can damage a healthcare organization by compromising system availability that is required to provide patient care. Moreover, system integrity breaches from a financial, legal, or competitive perspective ultimately can damage a healthcare organization's reputation.

Outbreaks

Outbreaks are attacks, such as worms and viruses, which either are known or unknown (an example of an unknown attack is a day-zero attack). Over the last few years, outbreaks have caused a significant financial impact to businesses, as highlighted in CSI/FBI surveys conducted annually from 2002-2005. Network downtime can result in the loss of life or business in the healthcare IT environment.

Noncompliant Devices

Noncompliant devices often are associated with network infection. For example, if a laptop does not have the latest antivirus signature or vulnerability patch, the risk of it becoming infected and spreading a virus throughout the network is much higher than that of a laptop with the latest updates. In this era of providing network access to contractors, consultants, partners, and vendors, the potential threat from noncompliant devices has grown exponentially.

Unauthorized Access

Unauthorized access, both to the network and to specific resources, presents a significant security and financial risk. Information theft was one of the three most expensive security breaches, as noted in the 2002-2005 CSI/FBI surveys. Past studies have shown that although the majority of thieves gain access from outside the network, internal thieves (for example, employees or contractors who are connected to the main network) cause the most financial damage. These individuals know what to steal and where to steal it.

Denial of Service

Denial-of-service (DoS) and distributed-DoS (DDoS) attacks have moved from the realm of mischief or revenge performed by hackers to an extortion tool used by highly organized Internet criminals. More than ever before, attackers are targeting corporations with DDoS assaults that are designed not simply to disrupt business networks, but to demand a ransom under the threat of bringing the business to a halt. Until recently, companies either had to pay the ransom or suffer the negative financial impact of the attack.

Security is a holistic, end-to-end process. Security services are provided in the MGN's interactive services layer. The process of securing the MGN starts with user access into the network. The NAC framework is designed to enforce security policy systematically at the point where users and medical devices attach to the network. This framework encompasses switches, routers, access points, VPN appliances, and NAC appliances, enabling flexibility and consistency throughout the network. To increase security levels throughout the network infrastructure, the MGN offers several measures for both the switches and the routers. Integrating security features into the access switch can thwart malicious activity quickly and effectively.

Secure Sockets Layer

The Secure Sockets Layer (SSL) protocol ensures that all credentials, as well as the information that a subscriber enters, are encrypted as the data is sent across the network. This includes information that is used for configuration, administration, reporting, and management.

Transparent LAN Service

The Transparent LAN Service (TLS) is a transport security protocol that evolved from SSL. It provides authentication and strong encryption methods for application communications. TLS is optionally used in IPCC environments to authenticate the signaling devices that prevent spoofing. Additionally, this feature can authenticate devices and encrypt signaling traffic. Encryption helps ensure that signaling information, such as dual tone, multifrequency digits, passwords, PINs, and voice encryption keys, remains secure.

Identity-Based Networking Services

IBNS authenticates and authorizes users and devices to protect against unauthorized access. Using IBNS, the network can determine if users are authorized to access the network and what they are able to access.

The MGN's broad attack-mitigation capabilities focus on identifying malicious content. This includes anti-virus, anti-spam, anti-phishing, anti-DDoS, anti-worm, and anti-malware. These anti-x defenses are not just about breadth of mitigation, but also about distributing those mitigation capabilities throughout key security-enforcement points in the network. This approach stops attacks as close to the source as possible, while greatly diminishing damage, because it prevents widespread propagation. Additionally, communications are encrypted to ensure privacy and protection from attackers or eavesdroppers.

Security and network administrators face numerous challenges, including:

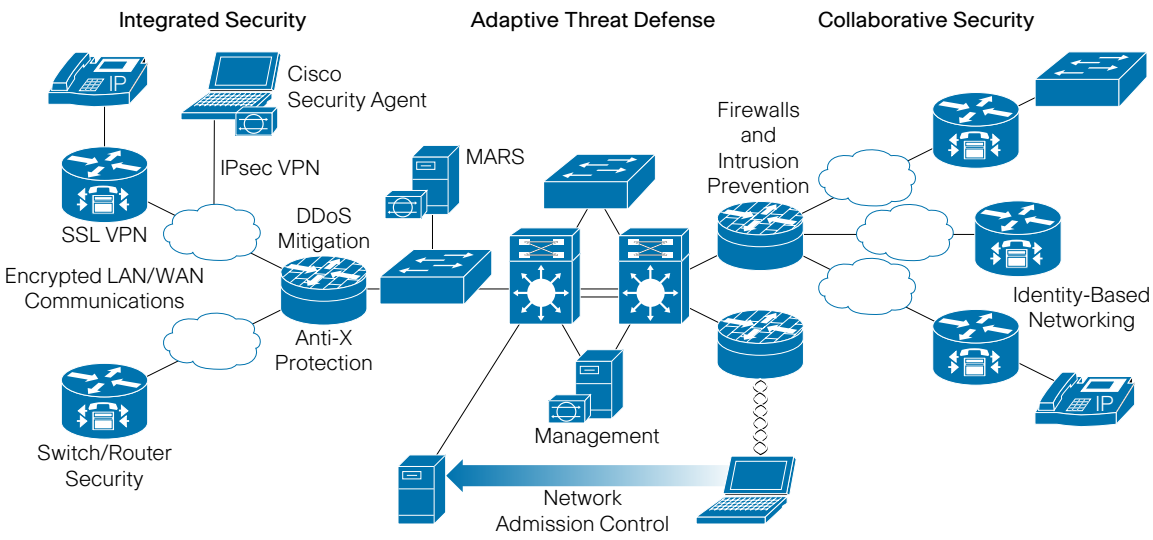
- Security and network information overload
- Poor attack and fault identification, prioritization, and response
- Increases in attack sophistication, velocity, and remediation costs
- Compliance and audit requirement adherence
- Security staff and budget constraints

The MGN addresses these challenges by:

- Integrating network intelligence to modernize correlation of network anomalies and security events
- Visualizing validated incidents and automating investigation
- Mitigating attacks by taking full advantage of existing network and security infrastructure
- Monitoring systems, network, and security operations to aid in compliance
- Delivering a scalable appliance that is easy to deploy and use, with the lowest total cost of ownership (TCO)

Operators are able to centralize, detect, mitigate, and report priority threats using the network and security devices already deployed in the infrastructure.

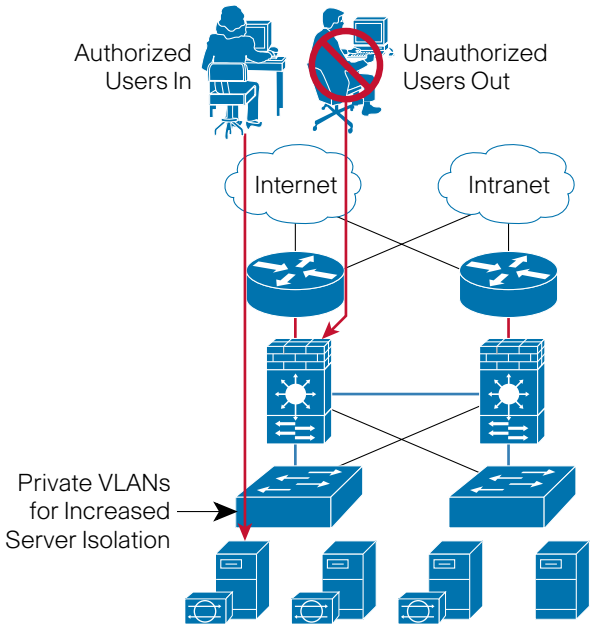
Figure 17. Security



Data Center Security

Typically, the data center is the focal point of most network-delivered services. Therefore, it is most important to maintain data center availability. Operations can be affected by numerous factors, such as environmental issues, power and cooling, backup and disaster recovery, and any of a variety of DoS causes. Within the data center, however, an outage generally will affect services related by function or geography, such as applications delivered by a specific server or a server farm connected to, or through, a network device. To reduce the likelihood of these occurrences, LANs and SANs must be secured. Threats associated with LAN technologies are well-known, and security measures often are deployed to provide a baseline security level when external users attempt to access the Internet server farm. To secure server farms properly, the MGN uses a holistic and thorough approach that takes advantage of the best capabilities of each network product that is deployed, including firewalls, LAN switch features, host- and network-based IDSs and IPSs, load balancers, SSL offloaders, and network-analysis devices.

Figure 18. Data Center Security



Maintaining secure, constant application access is a top concern for the healthcare system's data center. To that end, intrusion detection services (IDS) detect and mitigate attacks from both external and internal threats. An extra layer of security is provided by isolating servers from one another through private VLANs. The MGN's scalable data center architecture ensures that failure of a single component does not affect application availability to external/internal users. Implementing servers with dual network interface cards (NICs), dual homed access switches, and load balancing/ caching reduces or eliminates disruptions to the user in spite of any issues. Availability

further is promoted through the use of fast-converging switching and routing technologies with uplink enhancements.

Clinic Security

The clinic is an extension of a primary healthcare facility or campus. Clinic users access the main servers and applications within the data center and require the same access as users on the main campus network. Security requirements at the clinic are as stringent as those of the campus; the primary challenge remote offices face is keeping information safe from theft as it crosses the WAN. Additionally, the clinic generally has less physical and building security than the main healthcare campus or data center. As in all MGN environments, security concerns include outbreaks, noncompliant devices, and unauthorized access.

Clinic/MOB IP Security

IPsec VPN plays a large part in connecting the clinic/branch office to the main network. Typically, IPsec VPN security is implemented at the remote edge router. Ideally, this is an Integrated Services Router, as it is the optimal remote office WAN router. The VPN tunnel then protects the data as it traverses the WAN until it reaches the main network and the VPN tunnel is terminated. At the clinic, the router then can perform network admission controls. For larger clinics or medical office buildings, NAC can be implemented in the switch, access point, or via an NAC appliance that sits closer to the user.

Security is deployed in three places in the office network: on the WAN, on the perimeter between the WAN and the LAN, and on the office LAN. Securing the WAN consists of using IPsec to secure data traffic traversing the WAN. The IPsec protocol provides data confidentiality through strong encryption, endpoint authentication, and data integrity. It is used as an overlay to the Internet, an enterprise private WAN, or MPLS VPN. VPNs allow using a service provider's shared infrastructure and the Internet to tie together broad-reaching networks and to link geographically dispersed employees and branch offices to mission-critical corporate applications. This contributes to a flexible, converged infrastructure that can scale with the organization.

Using IPsec VPN is a common method of securing enterprise traffic over the Internet. Figure 19 identifies some factors to consider when deploying IPsec VPN as a means of connecting healthcare facilities.

Figure 19. IPsec VPN Connectivity

IPsec VPN Connectivity	
Dynamic IP addressing	Remote offices may have T1 access link to the Internet with fixed IP addresses; cable or DSL as viable alternative access links. Dynamic IP addressing may need to be accommodated by the VPN technology in use.
Acceptable quality level	If voice or video traverses the WAN, then determining the level of acceptable quality over the Internet must be considered. This may require the negotiation of service-level agreements with service providers.
High security level	Support of a higher level of security may be required for the office network because of the direct connection to the public Internet. Split tunneling of traffic for local Internet used at the branch office requires a firewall for protection.
Authentication type	Authentication may include Easy VPN, digital certificates, or static pre-shared keys. Digital certificates should be used because of their high level of security and ease of key management when deploying several branch offices.

Intrusion Detection System

IDS provides security at the office network perimeters. A firewall provides integrated, inline security services and lock-tight security and control for each protocol traversing the office router. It is recommended that IDS run on all office perimeter interfaces, but tuning may be required to prevent oversubscribing IDS monitoring capabilities.

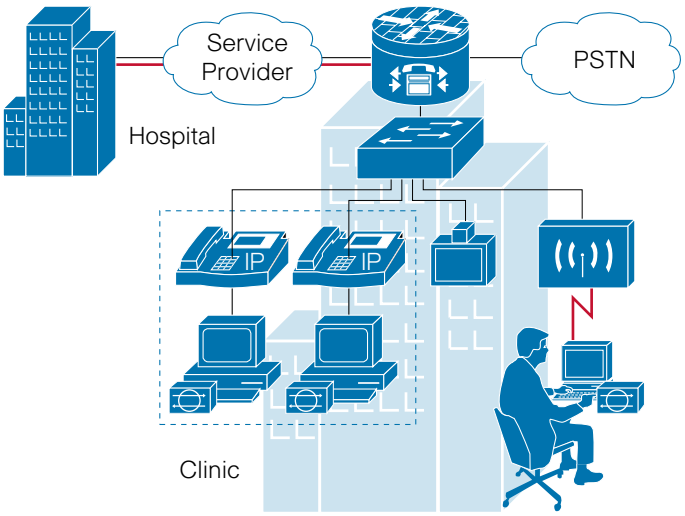
Intrusion Prevention System

The Intrusion Prevention System (IPS) acts as an inline intrusion detection sensor, watching packets and sessions as they flow through the router, then scanning each packet to match any of the IPS signatures. When it detects suspicious activity, it responds before network security can be compromised and then logs the event.

Network Admission Control

NAC provides a high level of protection to network devices by determining the health of the device before it is allowed to access the office network. When a device attempts to contact another device beyond its own local subnet, the office access router can facilitate a security posture check. This is achieved by communicating with a software agent on the device, requesting its antivirus posture, and comparing the received credentials against a database that specifies the minimum requirements for network access. If a PC does not meet the requirements, it is denied access and the network administrator is notified so that remedial action can be taken.

Figure 20. Clinic Security



To protect the clinic, the security services identified in Figure 21 are implemented on the MGN.

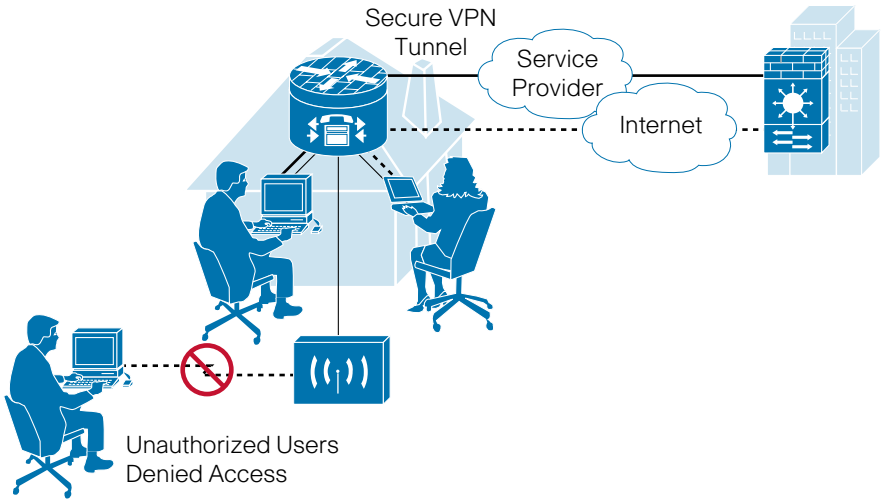
Figure 21. Clinic Security Services

Clinic Security Services
Private line services or IPsec-protected VPN
Firewall services
MAC and IP address NAC
Network-based intrusion detection
Host-based intrusion protection
Identity-based networking services
802.1x integration

Remote Clinician Security

Often, clinicians work in small offices, away from the main hospital or facility. These remote workers, and their equipment, must have protection as they access the campus network.

Figure 22. Remote Clinician Security



The MGN teleworker solution requires secure voice and data solutions in a combination of existing VPN and IP telephony solutions. VPNs provide secure communications across non-secure networks. Through VPNs, users accessing enterprise services have the same functions as those in office. VPNs enable using a service provider's shared infrastructure to tie together broad-reaching networks and cost effectively link geographically dispersed employees and branch offices with corporate applications. This contributes to a flexible, converged infrastructure that can grow with the organization. VPN usage promotes cost savings because Internet connectivity is less costly than private line access. Due to the VPN's inherent flexibility, it is easy to change site locations or bring up new sites. Mobile users can connect to their network securely using any Internet connection.

Two kinds of VPNs are used to connect remote clinicians to the main healthcare institution. These include site-to-site and remote access. Site-to-site VPNs provide a relationship between two network devices to forward encrypted traffic between networks. Usually, the two devices are peers and either one can create a VPN tunnel. These VPNs primarily are used between the main healthcare institution and the branch office. Remote access VPNs are beneficial to clinicians or ancillary personnel that work from sites other than a primary office. For healthcare practitioners who travel to patients' homes or provide other types of offsite services, remote access VPNs are most useful.

Business- / Clinician-Ready Teleworker VPNs

The MGN is built upon years of experience in providing business-ready, site-to-site, teleworker solutions. The teleworker environment supports multiple devices (for example, IP phones, enterprise user laptops, and home PCs accessing the Internet) and is similar to a small branch office. Unlike many site-to-site VPNs, the main site typically does not request the VPN tunnel to the small office/home office (SOHO). Instead, it prefers fewer definitions in SOHO devices for easy, scalable implementation.

Teleworker IP Telephony Security

IP telephony allows voice and data to be converged into a single system. The MGN's teleworker solution enables full delivery of voice and data to a user's home office over a broadband connection. This solution includes a router that provides superior security and remote management capabilities. For example, upon detection of a worm, it automatically will shut down an open connection. Business resilience and continuity are assured with an always-on, secure, IT-managed enterprise connection. Security posture is enhanced with IPsec Triple Data Encryption Standard (3DES) for all traffic. Corporate IT centrally handles security and policy management services. Cost containment and reduction are realized through consistent and reliable performance for mission-critical and real-time applications over a common network connection, with distinct handling of diverse traffic types (home versus data center users).

Broadband Access Technologies

With a large variety of connection options, there is ongoing concern about data integrity and confidentiality for the teleworker. Teleworkers are outside the corporate security perimeter and often lack the latest antivirus and OS updates. The broadband gateway is supplied either by the service provider or by the teleworker. The ideal choice is a router, which provides a firewall, VPN security, and NAC. Enforcing NAC results in teleworker machines being scanned, updated, and possibly cleaned of infection much more quickly. It's crucial that the teleworker use a VPN back to the main network to ensure data integrity and confidentiality.

There are four available broadband access types for SOHO connectivity. Digital Subscriber Lines (DSL) and cable dominate this space. In addition, satellite and last mile wireless are viable options.

Digital Subscriber Line

DSL services feature a dedicated access circuit and a service similar to Frame Relay or Asynchronous Transfer Mode (ATM), in which a single, permanent virtual circuit (PVC) is provisioned from the SOHO to the service provider aggregation point. In DSL networks, delay and jitter are very low, but are not guaranteed.

Cable

Cable offers a shared service with symmetric speeds varying from 100 Kbps to 4 Mbps. In the past, delay and jitter varied greatly, which made cable unsuitable for packet voice. With the new Data over Cable Service Interface Specifications (DOCSIS), more intelligent cable modems and routers can provide traffic shaping for transmission into the cable network.

Satellite

Satellite communication often is asymmetrical in nature because the uplink speed is different from the downlink speed. There also are other considerations when utilizing this type of transport medium. The MGN ensures that applications traversing this link are not affected by delay, error, or congestion. If the applications are affected, proper compensation techniques are employed so that the applications perform as expected. This is an alternative communication link for rural areas not served by broadband landline services, such as DSL, Cable, T1, T3, optical, and so forth.

IP Telephony Security

In the healthcare information technology community, securing voice communications and protecting IP telephony are topics of primary concern. Several design and configuration actions are required to safeguard against malicious and unintentional events that could compromise the system's integrity. The MGN takes proactive steps to ensure a secure communications network, including the establishment of a secure physical boundary for communications equipment. Network designs and software configurations cannot protect a network whose assets are not physically protected from potential malicious threats. Routers, switches, and VoIP gateways define network boundaries and act as gateway interfaces to all networks. Securing these vital data network pieces is a requirement for the data, voice, and video applications running across the infrastructure. Understanding and following sound IP network design principles not only allows the network to scale and perform, but also increases the security of all attached devices. One of the most vital steps in ultimately guarding the network is securing the actual voice call processing platform and applications. Establishing QoS throughout the infrastructure ensures that bandwidth and queuing are available for delay-sensitive voice traffic so that IPT users will not feel the impact of many network events. Through these actions, the MGN offers a comprehensive security solution, with all network elements, applications, call control, and endpoints having integrated security components.

IP Communications Security Design

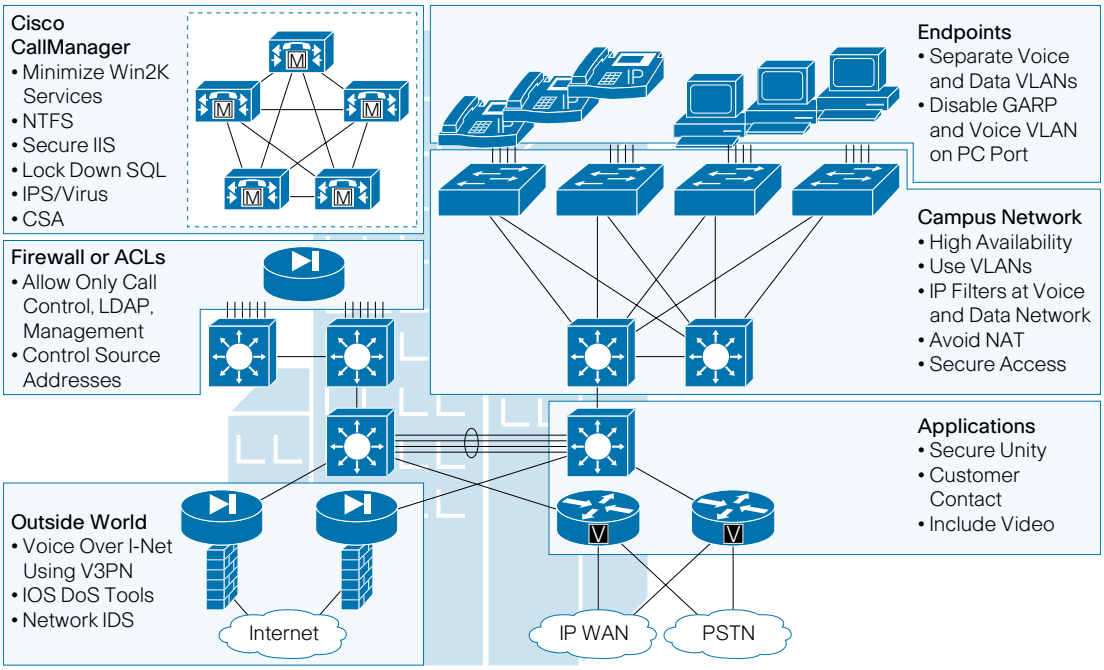
The MGN call manager offers many security features that ensure data integrity and provide communication privacy via encryption.

As a software-based call processing component, the call manager extends telephony features and capabilities to telephony network devices, such as IP phones, media processing devices, VoIP gateways, and multimedia applications. A firewall prevents unauthorized connections to the call manager.

Multiple call manager servers are clustered and managed as a single entity, yielding scalability, load balancing, and call processing service redundancy. System capacity can be increased when needed through the addition of clusters. Clustering aggregates the power of multiple, distributed call managers while triple call processing server redundancy improves overall availability and security.

CAC helps ensure that voice QoS is maintained across constricted WAN links. It automatically diverts calls to an alternate public switched telephone network (PSTN) route when WAN bandwidth is not available. A Web interface enables remote device and system configuration.

Figure 23. IP Telephony Security



Mobility Attributes

Mobility services enable efficiencies in clinical and business workflows in the healthcare environment. Clinician mobility is critical to providing cost-effective and efficacious care. Secure mobile networking requires using industry-standard security protocols, which control authentication, heighten data encryption, minimize latency, and support roaming among access points. Mobility services are inherent in the MGN. Figure 25 identifies a list of attributes afforded by the MGN's mobility services. These are considered necessary when deploying a wireless network in a medical environment.

Figure 24. Mobility Attributes—Structure

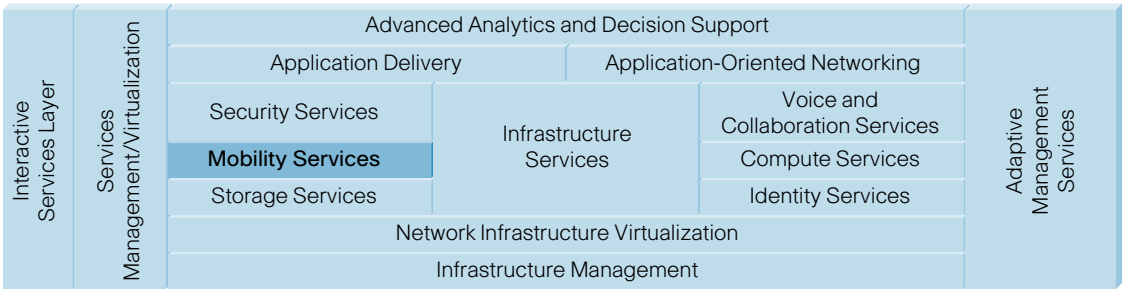


Figure 25. Interactive Services Layer—Mobility Attributes

Interactive Services Layer—Mobility Attributes	**Technical Benefits**
Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access2 (WPA2) • WPA-TKIP encryption enhancements such as key hashing (per-packet keying), message integrity check (MIC), initialization vector (IV) changes, and broadcast key rotation • WPA2-AES for government-grade, highly secure data encryption using Counter Mode with Cipher Block Chaining Message Authentication Protocol (EAS-CCMP)	Access control via per-user, per-session mutual authentication and data privacy via strong dynamic encryption Proactive Key Caching (PKC) Supports the latest IEEE 802.11 security standards
Authentication of messages between the client, access point and Authentication, Authorization and Accounting (AAA) server	Confidentiality, integrity and replay protection
Authentication algorithm to validate client credentials, such as LEAP, PEAP, or EAP-FAST	Client inclusion, containment and remediation
Quality of Service (QoS) • Controlling jitter and latency (required by real time traffic) • Managing and minimizing network congestion • Shaping the network traffic to smooth the traffic flow. Setting network traffic priorities.	Voice over WLAN
Multiple Broadcast SSID	Increased flexibility to specify individual BSSIDs to meet their unique WLAN requirements
Wireless IDS server support (AP as scanner and IPS)	Threat control and containment
Location Solution	Rogue AP detection, location and containment, asset tracking, sensoring

Interactive Services Layer—Mobility Attributes	Technical Benefits
RF interference detection	802.11 and non-802.11 signals such as CellularPCS9 1900MHz, bluetooth
IDS signature-based detection	Mitigate threat from hackers, malicious code and suspect signatures
Secure Unified Wireless/Wired Guest Access Customizable network segregation Bandwidth policy control Guest user name, associations and disassociations via MAC address	Leverages Cisco Self Defending Network Supervised guest user patterns and statistics for network sizing
Next Generation 802.11n • Data rates of up to 300 Mbps per radio and aggregate of 600Mbps • New multiple-input, multiple-output (MIMO) technology for predictable WLAN coverage and reliable connectivity • Operates in 2.4GHz and 5GHz • Fully power the dual-radio 802.11 n AP from a single Ethernet port	Support for mission-critical, bandwidth-intensive applications such as video

Wireless LAN (WLAN) implementations integrated with a wired network often are installed in hospital facilities, in large organizations down to the individual practice level, and in teaching and research hospitals. These systems are required to remain highly available as part of mission- and life-critical systems and applications. They provide a high level of security, including interference notification and detection of rogue access points.

Due to the nature of RF equipment, wireless brings a set of special challenges to the medical environment. The WLAN must not give off any signals that will interfere with medical systems, applications, or instrumentation. Nor can it otherwise negatively impact the ability to provide patient care. Moreover, the wireless network's inherent flexibility should not provide a means of unauthorized access into patient records or information.

Wireless installations are complicated by the fact that healthcare facilities often are built using a combination of different materials, thereby making RF behavior in these varying environments highly unpredictable. Additionally, there are areas surrounded by lead shielding or other substances that RF signals cannot penetrate. Consequently, it is strongly recommended that healthcare facility deployments always include a professional physical site survey.

Frequently, medical environments use equipment that shares the industrial, scientific, and medical unlicensed RF bands that 802.11b/g at 2.4-GHz and 802.11a at 5-GHz occupy. Therefore, it is recommended that when a healthcare facility is surveyed for installation of an 802.11a/b/g wireless infrastructure, a full RF spectrum analysis also be conducted. At a minimum, this analysis should cover the 2.4-GHz and 5-GHz ISM bands.

Secure Wireless

Availability, confidentiality, and integrity are the primary goals of WLAN security. Since August 1996, U.S. healthcare providers have been required by law to comply with HIPAA in terms of privacy of medical information. All WLAN security must assure medical information confidentiality and HIPAA regulations. Cisco Secure Wireless enables healthcare organizations to confidently deploy mobile applications and services, such as electronic health records, decision support, e-prescribing, and e-research. In addition it offers the wireless foundation needed to deploy mobile care applications, and location-aware services. Hospitals that deploy Cisco Secure Wireless solutions can be confident that patient information is protected to help comply with regulatory requirements:

- Information privacy & integrity: All information is encrypted as it travels over the wireless network. Cisco Secure Wireless solutions protect information such as prescription dosages from accidental or deliberate alteration as it travels over the wireless network.
- Network access control: Before providing access to services, the network validates that the right user is authorized to access the network and the right application and that their devices conform to the hospital's security policy for required security software and settings.
- Performance and reliability: Cisco Secure Wireless Solution constantly and automatically adapts to changes in usage patterns as people move around and use different applications over time. This ensures a better end-user experience as the wireless network delivers optimized performance and availability. In addition, if laptops are missing software or are not configured properly, remediation is performed automatically, without any action from the doctor or nurse.

Cisco Secure Wireless helps mitigate, both passive and active WLAN attacks.

Passive Attacks

A passive attack involves an unauthorized user gaining access to the network but not modifying any network resources. During the attack, the hacker may analyze WLAN traffic or eavesdrop on transmissions through packet capture methods. Hackers use this traffic analysis to gain basic network knowledge, sometimes in order to launch more damaging active attacks. Such information can include WLAN existence via access point detection and war driving, WLAN activity, and protocol information. Eavesdropping attacks, similar to traffic analysis attacks, are difficult to identify. Strong encryption methods, such as WPA2, however, mitigate these types of attacks.

Active Attacks

In an active attack, the unauthorized user may modify and/or disrupt network resources. Disruptions may include the presence of rogue access points or man-in-the-middle attacks, packet replay attacks, session hijacking, and DoS attacks. Rogue access points and DoS attacks can be identified via access point management devices. Strong encryption countermeasures must be used to prevent man-in-the-middle attacks, packet replay, and session hijacking attacks. The MGN service offering provides a number of tools and techniques to mitigate such threats.

Even security authentication and encryption methods have pre-existing vulnerabilities that can be compromised. Only a complete network assessment can determine the vulnerabilities that exist based on current and future WLAN security posture, including authentication and encryption methods.

The Cisco Unified Wireless Network integrates wired and wireless intrusion detection and prevention to mitigate threats from hackers and malicious code. The network inspects the traffic flows from the IP layer up to the application layer (L3 to L7) and monitors for potentially harmful signatures or suspicious application behavior. In the event that a signature is detected, the wired IPS solution will alert the wireless LAN controller that the signature is originating from the wireless network. The Wireless Control System alerts network managers to the security threat and provides a graphical view of the network, including the location and threat level of rogue access points. The wireless LAN controller will then issue a client shun to the identified client and then physically block its association with the access point. This integration of wired and wireless solutions offers zero day alerting and response to potential viruses, malware and suspect signatures.

A unified wired and wireless network allows security policies to be extended uniformly across the entire network. Pervasive WLAN deployments enhance network visibility and can use network intelligence to mitigate risks. The combination of these management capabilities provides the most comprehensive and intuitive management framework of any wireless security architecture available today.

WLAN QoS

The MGN demands end-to-end QoS to deploy interactive applications. As more and more interactive applications use wireless infrastructures, QoS becomes even more important. QoS allows network managers to establish SLAs with network users. It enables more efficient network resource sharing, expedites handling of mission-critical applications, and prioritizes time-sensitive multimedia and voice application traffic. QoS does this by:

- Supporting dedicated bandwidth for critical users and applications
- Controlling jitter and latency (required by real-time traffic)
- Managing and minimizing network congestion
- Shaping network traffic to smooth traffic flow
- Setting network traffic priorities

Note: In a healthcare environment, QoS implementation is a policy decision and applications used in each unique environment will dictate the QoS policy.

Guest Access

An increasingly common medical application is guest access, which delivers Internet access to individuals who are not directly under the control of the healthcare system's IT policy. To maintain the organization's needs, guest traffic should take lower precedence than medical applications. For example, in terms of application priority:

Guest traffic = 0, bedside applications = 1–5, and voice traffic = 6.

In another approach, some hospitals use two different wireless frequencies for wireless access; 802.11b is for guest access and 802.11a is for clinical communications.

In addition to the classic guest user class, medical facilities also require a *physician guest* class of users. These physicians need access beyond a simple Internet connection and typically require access to resources within the facility's private network. Because these physicians are not necessarily employees, they are likely to use a variety of uncontrolled client devices. Additional security considerations are necessary to prevent the spread of viruses and the possibility of opening doors into the private network.

The Cisco Secure Wireless Solution offers two levels of guest access. The baseline guest capability uses a secure tunnel from the controller within the network to a guest controller in the unsecured network area (e.g. DZM) to direct guest traffic directly outside of the enterprise network. Additionally, the guest controller offers a customizable Web interface for user login and liability clauses and has a lobby ambassador feature to support variable login permissions on a per-user basis.

For more advanced guest services, including the ability to define role-based access, bandwidth privileges and conduct client posture assessment and remediation, the Cisco Secure Wireless Solution incorporates the Cisco NAC Appliance to supplement the inherent capabilities of Cisco wireless LAN controllers.

WLAN IP Multicasting

In healthcare, IPmc is predominant in wireless voice applications, most notably in the increasingly popular push-to-talk and nurse-call applications. These rely on IPmc to send voice data to wireless handsets.

Note: When wired solutions exist, multicasting on the WLAN should be discouraged.

High Availability

As greater numbers of wireless applications are brought to the bedside, availability 24 hours a day, 7 days a week becomes increasingly important. The MGN best practice is deploying multiple access points within the same coverage area, giving the facility better management of bandwidth, traffic, and downtime. This approach also provides infection containment. Access points are deployed in environments that must remain clean and uncontaminated to prevent the risk of spreading disease. Multiple access points help hospitals minimize technical work in sensitive spaces, even when failures occur.

Radio Resource Management

Automated Interference Avoidance and Power Adjustment

Network radio coverage can be optimized for signal to noise ratio and signal strength coverage. The network configures the access points automatically to avoid interferences or coverage gaps while maximizing the bandwidth available. If it detects an access point failure, a point of interference, or traffic density shifts, it will immediately take action tuning the radio power or frequency of surrounding access points to compensate and maintain business continuity without impacting the devices connected to the wireless network.

Optimized Per-User Performance Through User Load Balancing

802.11 gives each network element equal access to the air. Each client decides which access point it will roam to next. When client devices enter a coverage area, they may roam to the access point with the strongest signal. Therefore, all clients may associate with the same access point and RF throughput for all clients can be potentially reduced. This is commonly called the "meeting room effect".

Load balancing optimizes throughput for all clients by constantly optimizing user associations to give each client optimal throughput. This improves the throughput for each client and dynamically balances the client load for the network.

Asset and Staff Management

Asset tracking and management are major concerns in healthcare organizations. It is vital to know exactly where certain high-value pieces of equipment are located, particularly in the event of an emergency. Yet studies show that hospitals cannot find 15 to 20 percent of the devices they own. Loss and asset mismanagement lead to significantly increased replacement and manpower costs, time delays, and overall strategic setbacks.

Location

As part of the Cisco® Medical-Grade Network, the Cisco Location-Aware Healthcare solution enables healthcare organizations to improve clinical processes and responsiveness with real-time resource location information. It also enables access to environmental information (for example, temperature or humidity) to provide an optimal patient experience. The solution enables both real-time tracking of assets and staff as they move throughout the campus and event-driven tracking as they exit and enter areas.

The Cisco Location-Aware Healthcare solution offers multiple configurations, so Healthcare organizations can deploy a solution that perfectly fits their needs. Using Wi-Fi location for pervasive location tracking and sensor capabilities, while deploying chokepoint technology only when and where it is necessary to optimize business-critical processes.

Wi-Fi Location System and Chokepoint System

By simply adding the Cisco Wireless Location Appliance to the Cisco Unified Wireless Network, Healthcare organizations can instantly benefit from the ability to locate any Wi-Fi devices on their premises. Locatable devices can include the existing wireless devices within the network such as Wi-Fi laptops or Wi-Fi phones as well as Wi-Fi tags added to mobile assets. The floor location of mobile assets in regular and irregularly shaped buildings can more accurately be determined with the Cisco inter-floor location differentiation feature.

Wi-Fi location services offer the following features:

- Regular updates of location and sensor information (temperature, pressure, humidity)
- Pervasive tracking of the location and sensor information (throughout the facilities)
- Calculation of location using an adaptive algorithm that reflects the environmental characteristics and enables locating an asset within 10 meters
- Wi-Fi devices and tags can be divided into groups for simplified tracking

The chokepoint location system consists of multiple-frequency tags (Wi-Fi 2.4 GHz and a lower frequency) and chokepoints transmitting at the lower frequency. As the multiple-frequency tags come close to a chokepoint, their lower frequency side receives energy from it and transmit their location and telemetry information through the Wi-Fi side of the tag to the access point. Tracking requirements that benefit from adding chokepoint technology are:

- The need to determine the precise location of an asset in less than a 10 meter radius, for instance within a specific storage room
- The need to know the location of an asset from a predefined set of places such as in specific departments or buildings of a healthcare facility
- The need to be alerted to the location of an asset during certain events for example when an asset enters or leaves a building

Medical Electromagnetic Compatibility Standards

It is important to determine if equipment must meet the electromagnetic compatibility (EMC) standards and safety requirements for implanted medical devices that are used to provide direct patient care or peripheral support. EMC means that any equipment used in proximity to such devices should not cause harmful interference. To adhere to EMC standards, Cisco equipment operates on a non-interference basis.

The operational frequencies of 802.11b/g and 802.11a radios are not normally used by patient monitoring systems. In all but extreme cases, these devices should not interfere with telemetry patient monitoring services. Nor should they, in most cases, interfere with nonwireless, non-mission-critical medical equipment, such as heart monitors, defibrillators, or other digital devices. As with all hospital equipment, the biomedical department should perform an analysis and review for safety and compatability purposes.

Wireless Architectural Design

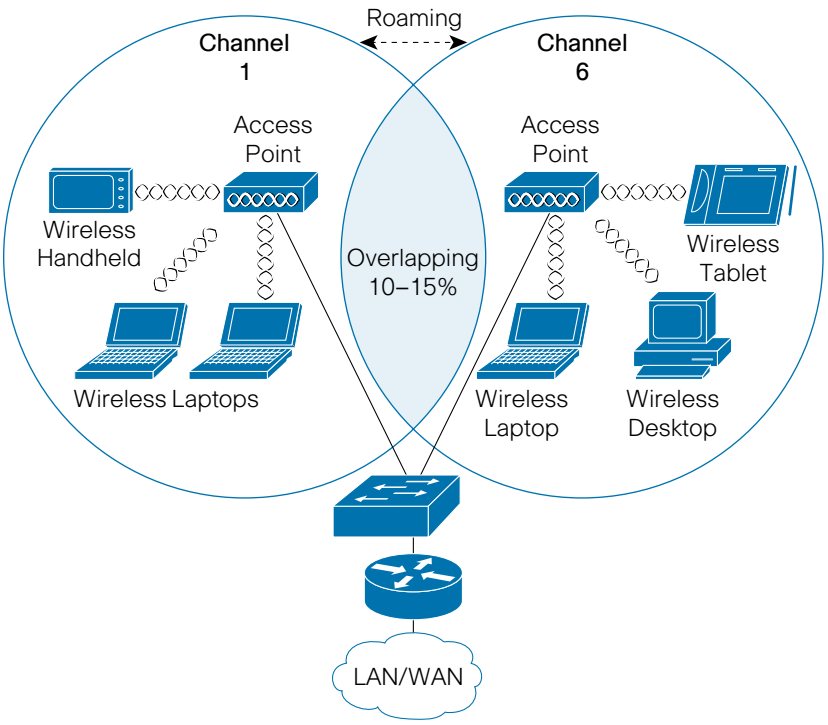
WLAN Deployment Models

Wireless technology is highly dependent on its environment. All medical facilities have different construction materials, populations, and interference factors for which the wireless environment must be customized. For this reason, WLANs are based on high-availability enterprise architecture and can adapt to an institution's specific needs. Typically, this architecture consists of a service set identifier (SSID) on the wireless side, mapping to a VLAN or mobility groups on the wired side, thereby allowing multiple models to coexist on the same WLAN. This mapping permits a combination of security measures based on client requirements or user policies. The MGN recommended security model is Wi-Fi Protected Access (WPA), which creates optimum network architecture and addresses all known WLAN encryption threats. WPA uses Extensible Authentication Protocol (EAP) to transport authentication information between client and authentication servers.

In a typical wireless LAN configuration, clients communicate through an access point where wireless clients gain access to the network. The access point has connectivity to other clients associated with it or to the wired LAN. The basic service area (BSSID) is the area of RF coverage provided by an access point, also known as a cell. Adding an access point can extend the BSSID, enable the addition of wireless devices, and extend the range of an existing wired system. It attaches to the Ethernet backbone and allows communication between all devices on the Ethernet backbone and those in the cell area. These remote devices communicate with the access point, not directly with each other.

If one cell does not provide enough coverage, the range can be extended by adding cells. This is known as an extended service area (ESSID). It is recommended that coverage overlap 10-15 percent to allow remote users to roam without losing RF connections. The recommended amount of overlap between cells is different, however, if voice over WLAN (VoWLAN) is deployed.

Figure 26. Wireless LAN Configuration



A peer-to-peer network between two or more clients may be established without an access point. In this configuration, however, security is a concern and it is not recommended for hospital applications.

Site Survey

Conducting a site survey using the same frequency plan as intended for the actual deployment facilitates a more accurate estimate of how a particular channel, at a particular location, reacts to interference and multipath fading. Channel selection also helps in planning for co-channel and adjacent channel interferences while providing information about where a frequency may be reused.

Performing a site survey in a healthcare environment requires some special considerations. Many hospitals have management spaces (another floor between floors) that are used to run operations such as patient support systems or bed locations. Typically, these are considered maintenance spaces where various patient care systems are deployed and managed. These maintenance spaces include emergency power runs, oxygen, dedicated telemetry networks, phones, and data network connections. Due to what is contained in these spaces, a hospital's wireless site survey may generate results that are very different from those of a regular office building. Additionally, many radiology departments have numerous shielding areas that can affect the manner in which wireless systems are dispersed. These design features completely distort findings if they are not identified at the start of the survey.

Aside from these issues, in multistory buildings, such as office towers, hospitals, and university classroom buildings, cell overlap between floors requires investigation. In some instances, it might be required to resurvey and relocate access points. Multistory structures introduce a third dimension to coverage planning: 2.4-GHz signals of 802.11b and 802.11g, which can pass through floors, ceilings, and walls. The 5-GHz signal of 802.11a also can pass through floors, ceilings, and walls, but at a lesser degree due to its higher frequency. With 2.4-GHz Wi-Fi LANs in particular, surveyors must avoid overlapping cells on the same floor, as well as on adjacent floors. With only three channels, overlapping is avoided through careful three-dimensional planning.

When powered on, an access point can be configured to search automatically for the best channel. The automatic search is configured using network interfaces: 802.11x radio settings and the least congested frequency.

It is necessary to involve the hospital's biomedical engineering department to test the WLAN in a controlled environment against other sources of electromagnetic interference. This department has an understanding of the equipment and its usage in the hospital environment. Most biomedical engineering departments have a standard test set based on known industry issues and the electromagnetic devices that the health system already has installed.

RF Design Planning

Many RF design considerations are interdependent or implementation-dependent. A number of factors affect WLAN coverage, including the selected data rate, channel selection, power level, antenna type (dipole, omnidirectional, directional, or wall mount), and environment.

Data Rate Settings

Data rates affect cell coverage and, consequently, the number of required access points. Lower data rates (such as 1 Mbps) can extend farther from the access point than can higher data rates (such as 54-Mbps). Different data rates are achieved by sending a more redundant signal on the wireless link, allowing data to be more easily recovered from noise.

Data rate settings are used to select transmission rates. Wireless devices always attempt to transmit at the highest possible data rate on the browser-based interface. If RF rates are insufficient to support the highest rate, the wireless device steps down to the highest rate that supports reliable data transmission. The data rate often is confused with the aggregate data throughput. Throughout, however, takes into account the overhead associated with protocol frame structure, collisions, and the implementation processing delays associated with frames that are processed by clients and access points. The overhead associated with the 802.11b standard exceeds the overhead for 802.3 Ethernet, resulting in better throughput for 10-Mbps Ethernet than 11-Mbps Wi-Fi.

Power Levels

The higher the signal power, the larger the cell. Higher powered signals, however, also require greater power consumption. Battery consumption for wireless endpoints is higher for 802.11a than for 802.11g/b. If enclosures are implemented, low-loss cable should be used between the access point and the antenna that is external to the enclosure.

Antenna Selection

Power level and antenna selection can be used to modify and optimize the coverage area. Distributed antenna systems are popular in healthcare environments but they disrupt all radio management features. In healthcare, enclosures with third-party antennas often are needed for infection containment. If a paddle antenna (802.11a) is selected, installers must ensure that the antenna is beyond the reach of patients or other passersby. A misaligned antenna could result in poor coverage and performance for bedside or clinical applications. In all cases, antennas must be installed via manufacturer's directions and recommendations pertaining to building codes and regulations.

Channel Selection

Channel selection depends on the frequencies permitted for a particular region. For example, the North American and the European Telecommunications Standards Institute (ETSI) 2.4-GHz channel sets permit allocation of three non-overlapping channels (1, 6, and 11), while the 5-GHz channel set permits 12 channels. The channels should be allocated to the coverage cells so that overlapping cells use non-overlapping channels. Where channels must be used in multiple cells, ensure that those cells minimally overlap each other.

RF Environment

The performance of the WLAN and its equipment depends upon the RF environment. Adverse RF environmental variables include the following:

- 2.4-GHz cordless phones
- Wire mesh and stucco walls
- Filing cabinets and metal equipment racks
- Transformers
- Heavy-duty electric motors
- Firewalls and fire doors
- Concrete
- Refrigerators
- Sulphur plasma lighting (fusion 2.4-GHz lighting systems)
- Air-conditioning ducts
- Other radio equipment
- Microwave ovens
- Other WLAN equipment

Real Time Spectrum and Intelligence is improved when RF interference is quickly detected and mitigated. Healthcare organizations can now identify and resolve RF problems more efficiently with an integrated spectrum intelligence, resulting in improved performance, security, and lower operational costs.

The Cisco WCS now supports advanced spectrum analysis features to monitor interference detected by the Cognio Spectrum Expert. It allows clear visualization and also offers menu options, and interference search capabilities. Up to 10 Cognio Spectrum Expert sensors can simultaneously interface with Cisco WCS to monitor RF interference.

A Cisco WCS table displays detected interferer types with severity, impacted channels, affected access points and affected client devices. Searches for interferers can be performed using a variety of interferer properties.

The approximate location of interferers can be determined by locating the Cognio Spectrum Expert sensors with Cisco WCS, displaying the affective range of the sensors and correlating this with the suspected interferer.

RF Deployment Best Practices

Some deployment considerations are addressed with general best practices for WLANs. The following guidelines apply to most situations:

- The number of users versus throughput and a given access point. Generally, the recommended number of users per access point is 15 to 25 for data-only networks

and seven to eight for voice applications. Wireless phones add a maximum concurrent call-per-access-point limit.

- The distance between access points can cause throughput variations for clients based on distance from the access point. The recommendation is limiting the access point data rate to the higher data rates.
- The number of access points depends on coverage and throughput requirements.
- Based upon the variability of environments, a site survey is highly recommended to determine the number of access points required and their optimal placement.

Wireless Networks Are Targets

While wireless networks offer significant benefits in the healthcare environment, wireless security, especially for Wi-Fi based wireless LANs, must be a priority for IT organizations given the rapid growth of wireless adoption.

Cisco® helps Healthcare organizations meet their data security requirements through the Cisco Self-Defending Network strategy. The self-defending network is Cisco's long-term strategy to protect an organization's business processes by identifying, preventing, and adapting to threats from both internal and external sources. This protection helps organizations take better advantage of the intelligence in their network resources, thus improving business processes and cutting costs.

Characteristics of Cisco Self-Defending Network security solutions include:

- The integration of security throughout all aspects of the network
- Collaborative processes between the various security and network elements
- The ability of the network to adapt to new threats as they arise

The self-defending methodology provides businesses with guidelines for creating a secure communications infrastructure and helping the business to achieve its compliance goals. To address wireless security requirements, Cisco recommends providers take an architectural approach to designing and building the wireless network.

The Components of the Secure Wireless Solution

The Cisco Secure Wireless Solution is an end-to-end architecture that integrates key security and wireless solutions to deliver standards-based, industry-leading network protection. The architecture combines both wired and wireless security services to present a unified suite of security capabilities that not only deliver a more robust threat defense but also lower the total cost of implementing and maintaining a secure wireless network.

Critical features of the Cisco Secure Wireless Solution include:

- Unified wired and wireless intrusion protection system/intrusion detection system (IPS/IDS)
- Client validation, posture assessment, and remediation

- Wireless single sign-on and 802.1x integration
- Granular control for secure guest access
- Host intrusion prevention
- Rogue detection via automatic RF monitoring
- Wireless security management

Authentication

The 802.11 standard supports two means of client authentication: open and shared key authentication. Open authentication involves little more than supplying the correct service set ID (SSID). With open authentication, Wired Equivalent Privacy (WEP) prevents the client from sending data to, and receiving data from, the access point unless the client has the correct WEP key. With shared key authentication, the access point sends the client device a challenge text packet that the client then must encrypt with the correct WEP key and return to the access point. If the client has the wrong key or no key, authentication fails and the client cannot associate with the access point. Shared key authentication is not considered secure because a hacker who detects both the clear text challenge and the same challenge encrypted with a WEP key can decipher the WEP key.

Key Management

Another type of key that often is used (but is not considered secure) is a *static* WEP key. A static WEP key, composed of either 40 or 128 bits, is statically defined by the network administrator on the access point and the clients communicating with the access point. When static WEP keys are used, a network administrator must perform the time-consuming task of entering the same keys on every device in the WLAN.

If a device that uses static WEP keys is lost or stolen, the possessor of the stolen device can access the WLAN. An administrator can't detect an unauthorized user until and unless the theft is reported. The administrator then must change the WEP key on every device associated with the missing device. In a large enterprise WLAN, with hundreds or thousands of users, this can be daunting. If a static WEP key is deciphered through a tool, such as AirSnort, the administrator has no way of knowing that the key has been compromised.

Required Security Extensions

MGN tenets recommend deploying elements of the three technologies discussed as an alternative to WEP as specified by IEEE 802.11. The technologies include a network layer encryption approach based on IPsec, a mutual authentication-based key distribution method using 802.1x, and some Cisco proprietary improvements to WEP. Additionally, IEEE 802.11 Task Group "i" and the Wi-Fi Alliance compliance testing committee are working on standardizing WLAN authentication and encryption improvements.

IPsec

IPsec is a framework of open standards for ensuring secure private communications over IP networks. IPsec VPNs use the services defined within IPsec to ensure confidentiality, integrity, and authenticity of data communications across public networks, such as the Internet. When deploying IPsec in a WLAN environment, an IPsec client is placed on every PC connected to the wireless network and the user establishes an IPsec tunnel to route traffic to the wired network. Filters prevent wireless traffic from reaching any destination other than the VPN gateway or DNS server. IPsec provides IP traffic confidentiality, as well as authentication and anti-replay capabilities. Confidentiality is achieved through encryption using a variant DES, called Triple DES (3DES), or the new Advanced Encryption Standard (AES). Though IPsec is used primarily for data confidentiality and device authentication, extensions to the standard allow user authentication and authorization to occur as part of the IPsec process.

802.1x/EAP

An alternative WLAN security approach focuses on developing a framework for providing centralized authentication and dynamic key distribution. This approach is based on the IEEE 802.11 Task Group "i" end-to-end framework using 802.1x and EAP to provide this enhanced functionality. Cisco has incorporated 802.1x and EAP into its WLAN security solution. The three main elements of this approach are mutual authentication between client and authentication (remote access dial-in user service [RADIUS]) server, dynamically derived encryption keys after authentication, and centralized policy control (where session time-out triggers reauthentication and new encryption key generation).

When these features are implemented, a wireless client that associates with an access point cannot gain access to the network until the user logs on to the network. After association, the client and the network (access point or RADIUS server) exchange EAP messages to perform mutual authentication, with the client verifying the RADIUS server credentials and vice versa. An EAP supplicant is used on the client machine to obtain user credentials (user ID and password, user ID and one-time password, or digital certificate). Upon successful mutual authentication, the RADIUS server and client then derive a client-specific WEP key to be used for the current logon session.

EAP Authentication Benefits

EAP provides three significant benefits over basic 802.11 security:

- Mutual authentication scheme, which effectively eliminates man-in-the-middle attacks, introduced by rogue access points and RADIUS servers.
- The centralized management and distribution of encryption keys. Even if the WEP implementation of RC4 was flawless, there still exists the administrative difficulty of distributing static keys to all access points and clients in the network. Each time a wireless device is lost, the network must be rekeyed to prevent the lost system from gaining unauthorized access.

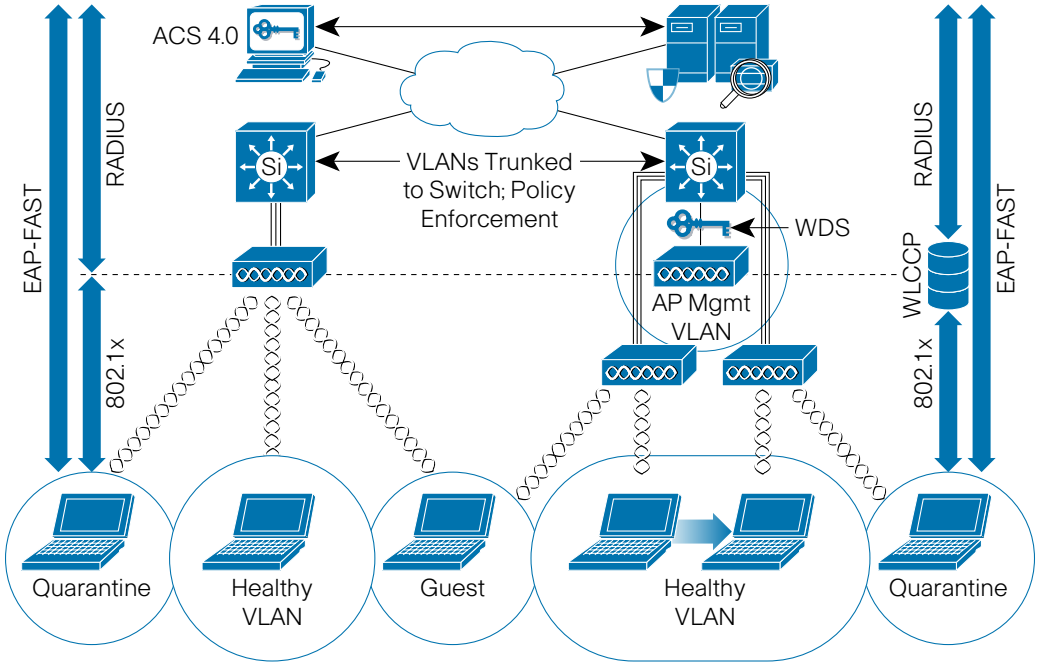
- The ability to define centralized policy control, where session time-out triggers reauthentication and new key derivation.

EAP Authentication Protocols

Numerous EAP types are available for user authentication over wired and wireless networks:

- Light Extensible Authentication Protocol (LEAP)
- EAP-Transport Layer Security (EAP-TLS)
- Protected EAP (PEAP)
- EAP-Tunneled TLS (EAP-TTLS)
- EAP-Subscriber Identity Module (EAP-SIM)

Figure 27. Mobility Best Practices

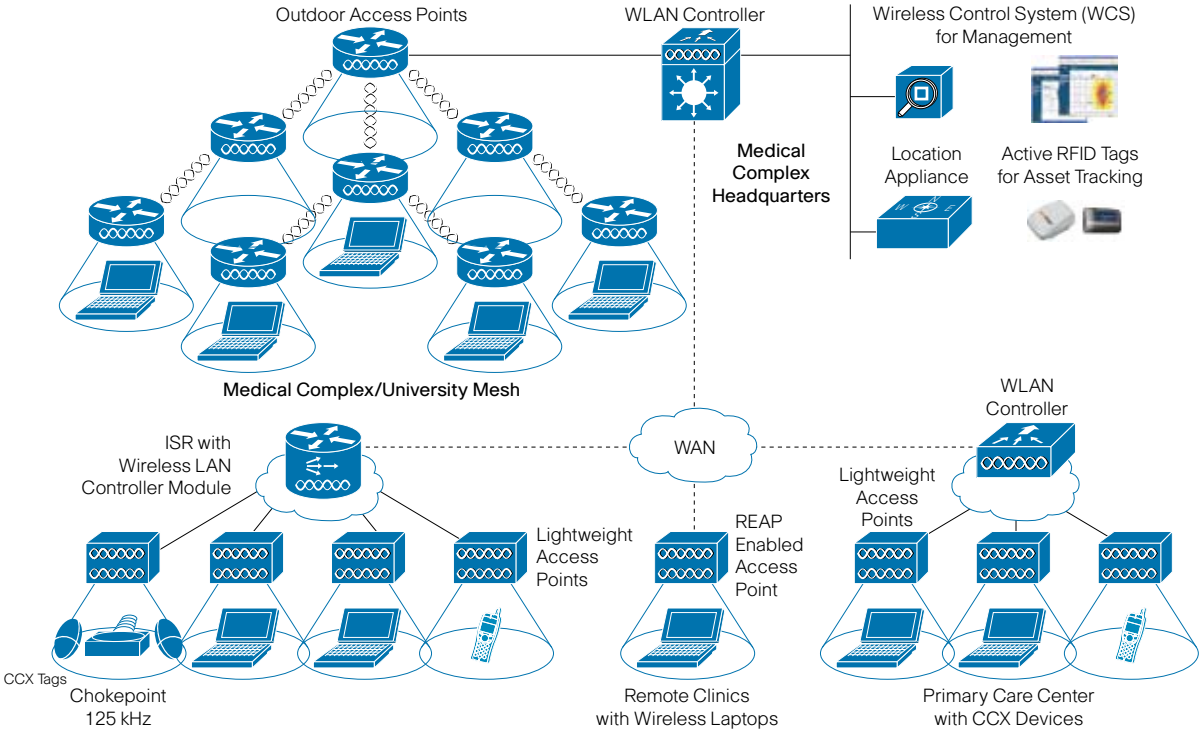


Wireless networks improve patient care by making healthcare safer, more accessible, and more affordable. In addition to augmenting staff effectiveness, wireless solutions transform bedside care by providing immediate access to important health information, such as prescription databases, dosage recommendations, and patient records.

Mobility Solutions

As part of the MGN infrastructure, the Cisco unified wireless network provides access to critical information when and where it is needed. This networking solution provides mobility, security, and instant access to voice and data applications. Health organizations improve responsiveness to patients, increase productivity, and enhance patient care while reducing costs through improved efficiencies and streamlined processes.

Figure 28. Mobility



Mobile UC Attributes

Voice services place stringent performance requirements on the entire network. Because digitized voice is a sampling of an analog signal (verbal communication), its transmission is very sensitive to delays during transit. In fact, in order for voice to work correctly over any infrastructure, the end-to-end transit time (cumulative time encoding the packet, leaving the sending client, traversing the network, then being decoded at the receiving client) must be less than 150 ms. Issues encountered during transit result in imperfections in the reconstituted signal; also known as "jitter". To meet these requirements, the wireless IP telephony architecture includes features such as traffic classification, queuing and shaping.

Voice Traffic Characteristics

Voice traffic typically has some consistent characteristics. VoIP packets are sent at consistent intervals with uniform packet sizes, making voice traffic smooth. Bandwidth is not wasted since VoIP packets attempt to use only the amount of bandwidth necessary to transmit from end to end. VoIP traffic is extremely sensitive to packet loss, and excessive loss degrades overall voice quality. Additionally, VoIP is very sensitive to delay and jitter. While a small amount of delay is tolerated, excessive delay or jitter degrades overall voice quality.

Wireless Networking Challenges

Wireless networking provides clinician and ancillary personnel immediate access to clinical and business applications. Adding IPC to the wireless network increases collaboration, responsiveness, and productivity. Voice, however, places unique requirements that differ from those of data applications on a WLAN.

Quality of service for a VoIP call must be maintained whether the call is being delivered to a wired or wireless endpoint. End-to-end delay and jitter must be minimized for VoIP packets to provide optimal audio quality. To maintain QoS, it is critical to establish priority across the WLAN and translate the packet priority from the wireless to wired infrastructure during transit.

Due to VoIP time sensitivity, reauthentication must occur quickly as a client roams across the campus so that network security is maintained. A wireless LAN voice client must maintain its security association from one access point to another, even across IP subnets, with as little latency as possible.

WLAN systems that support IPC also present operational challenges that are not faced by traditional wireless networks. The wireless medium is a shared resource. When coupled with a client's ability to roam freely throughout the enterprise, reliable service must be maintained at the radio frequency layer as well as the application layer. Another operational requirement is high availability. In order for the IPC solution to be effective over the WLAN, the solution's availability must parallel that provided by the wired network.

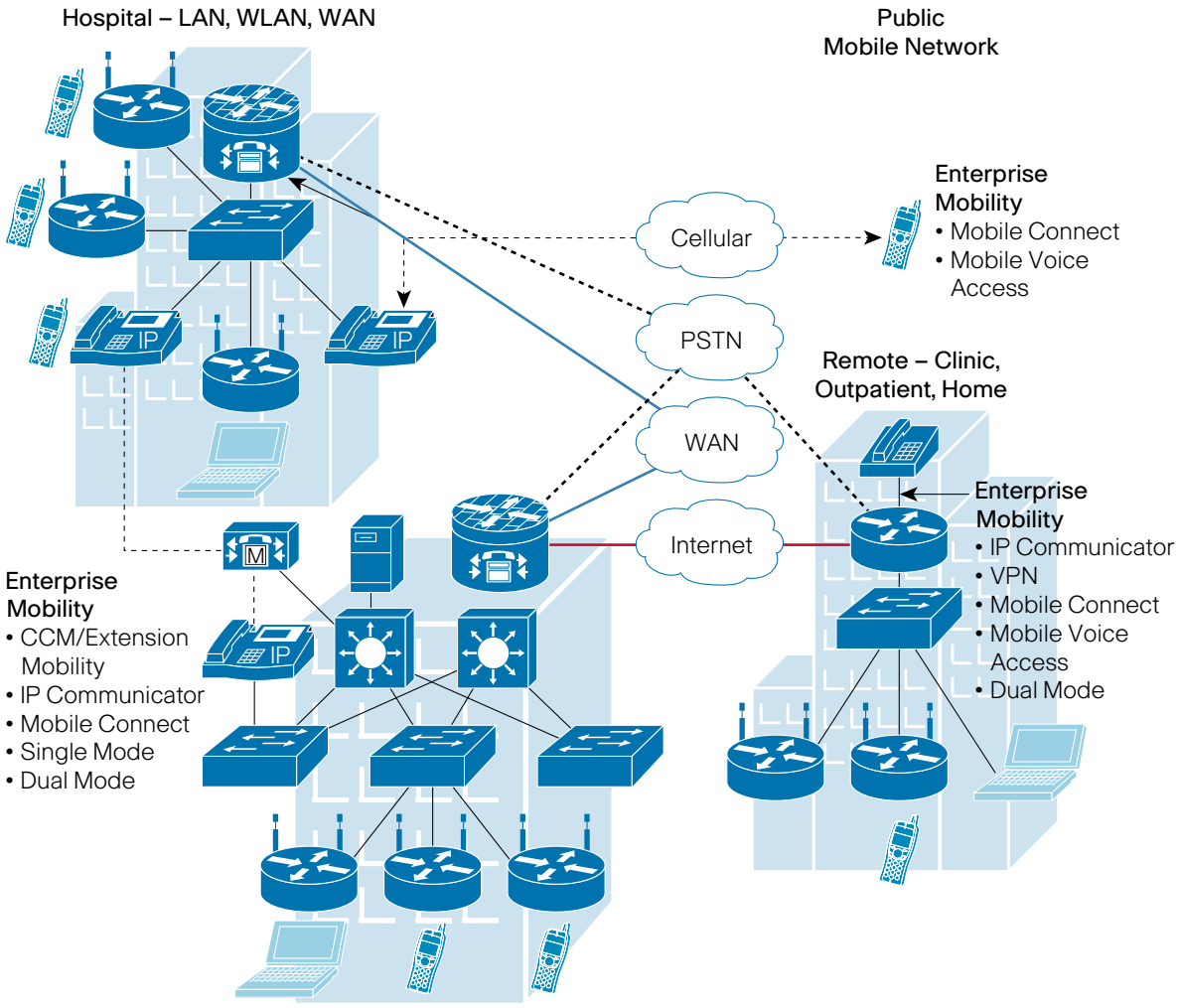
Multifaceted Approach to End-to-End Quality of Service

QoS on a WLAN is more than simply prioritizing one type of packet over another. WLAN traffic is nondeterministic, with channel access based on a binary back-off algorithm defined by the IEEE 802.11 Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) standard. The nature of this standard is to have clients back off for a random period of time to minimize contention for the channel. In an operational network, such as that of a healthcare enterprise WLAN, channel access times become more variable and generally longer. These factors make delivering reliable voice service on a WLAN exponentially more difficult as network usage increases. The dynamic nature of mobility makes this even more challenging because the number of active users in any one location changes often and patterns aren't predictable through the capacity-management tools used in wired networks. The very nature of physicians and clinicians in a healthcare organization makes them more likely to be mobile within the network and to cluster with other workers at different locations and times during the day. Meeting the WLAN QoS needs of this key demographic ultimately determines the success or failure of the Voice over Wireless LAN (VoWLAN) deployment.

Network and Service Management

VoWLAN solutions are built on a powerful foundation for WLAN systems management. IT managers can design, control, and monitor healthcare enterprise wireless networks from a centralized location, thereby simplifying operations and reducing total cost of ownership. These advanced services help organizations prepare for, and manage, the migration to VoWLAN with high-level designs and detailed RF site surveys all the way through ongoing performance and optimization of voice network applications. Working together, these elements create an integrated systems-level approach for providing essential communications for mobile clinical employees.

Figure 29. IPC Mobility

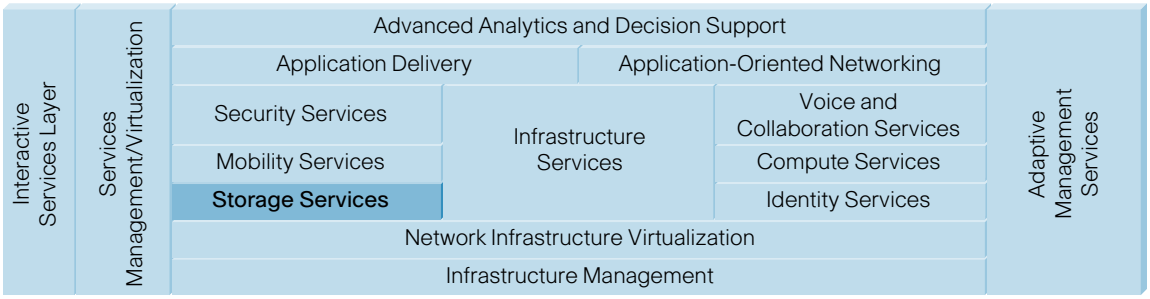


Storage Attributes

To meet the healthcare environment's storage requirements, the MGN uses a high-performance, highly available storage network architecture.

Applications, such as electronic medical records (EMRs), Computerized Physician Order Entry (CPOE) systems, and imaging systems require consistent and accurate access to system data. In support of these requirements, the MGN's healthcare storage environment provides real-time, consistent access to relevant patient and application information where and when it is needed. To facilitate business continuity and disaster recovery planning, the MGN supports reliable backup and archiving of valuable patient information, including digital images and EMRs.

Figure 30. Storage Attributes—Structure



The attributes necessary for storage networking in the healthcare environment are identified in Figure 31.

Figure 31. Interactive Services—Storage Attributes

Interactive Services Layer—Storage Attributes	
Backup and recovery	Zoning (read only, LUN)
Business continuity (disaster recovery), virtualization storage, consolidation terminology storage, HBA OS concepts, persistence building, HW path and FC_ID	Fabric security
Synchronous and asynchronous replication	Inter-VSAN routing
Serverless backup	Congestion control
Point-in-time copy, data migration, write acceleration, remote backup	Traffic engineering
FSPF	Switch interoperability
Zoning	AAA
Buffer-to-buffer credit	Internet small computer system interface (iSCSI)

Interactive Services Layer—Storage Attributes	
ISL init	Fibre Channel over Internet Protocol (FCIP)
Port Channel	Fiber CONnection (FICON)
VSAN	FICON

The MGN provides high-speed and reliable access to storage over IP networks. Using this storage infrastructure, healthcare providers can transmit patient data across the network to provide clinicians with rapid access to key patient information regardless of their physical location. The MGN storage architecture takes advantage of best practices in storage design to enable cost-effective, scalable storage architectures. The following sections illustrate methods to utilize storage networking that address healthcare's unique storage requirements while simultaneously minimizing costs.

Storage Area Network Fabric

The Storage Area Network (SAN) fabric is the MGN's base storage architecture. The storage fabric is built upon intelligent applications that maximize information availability. These fabric applications advocate a tiered approach to storage, assigning data to storage based on retention requirements, access rules, and business policies. The features that make up this approach to storage networking specifically address key problems with storage provisioning, data migration and replication, backup and recovery, storage utilization, and costs. The SAN fabric promotes sharing SAN resources, as well as the ability to isolate SAN groups.

Storage Area Network Extension

SAN extension is an enabling technology for business continuity. SAN extension allows key clinical and business data to co-locate across a geographic distance, facilitating disaster recovery planning. By replicating or copying data to an alternate site, an organization can protect its data in the event of a disaster at the primary site. Additionally, this functionality enables resiliency in the architecture, which is a critical MGN tenet. In the event of a disaster or emergency that affects the primary medical facility's normal operations, SAN extension facilitates disaster recovery planning by providing access to applications and data, thereby enabling resumption of operations in another location.

Storage Virtualization

To promote cost-effective storage in the medical environment, the MGN liberally uses storage virtualization. Storage virtualization promotes sharing of storage arrays by different applications, as well as seamless usage of heterogeneous storage arrays. Furthermore, each Virtual SAN (VSAN) is inaccessible outside the VSAN without inter-VSAN routing. This storage seclusion facilitates cost benefits by enabling a single infrastructure to fill the needs of several discrete networks concurrently. Additionally, when information sharing across differing SAN networks is required, policies and applications can facilitate secure and efficient information sharing.

The MGN has three types of storage architectures based upon requirements of the healthcare institution or system.

Network-Attached Storage

Network-attached storage provides high-performance access, data protection, and disaster recovery for file-based storage over an IP network. These features are particularly important for healthcare providers since they must comply with strict regulations regarding data backup and archiving. Additionally, any loss of patient data could result in negative patient outcomes, liability, or damage to the healthcare institution's reputation.

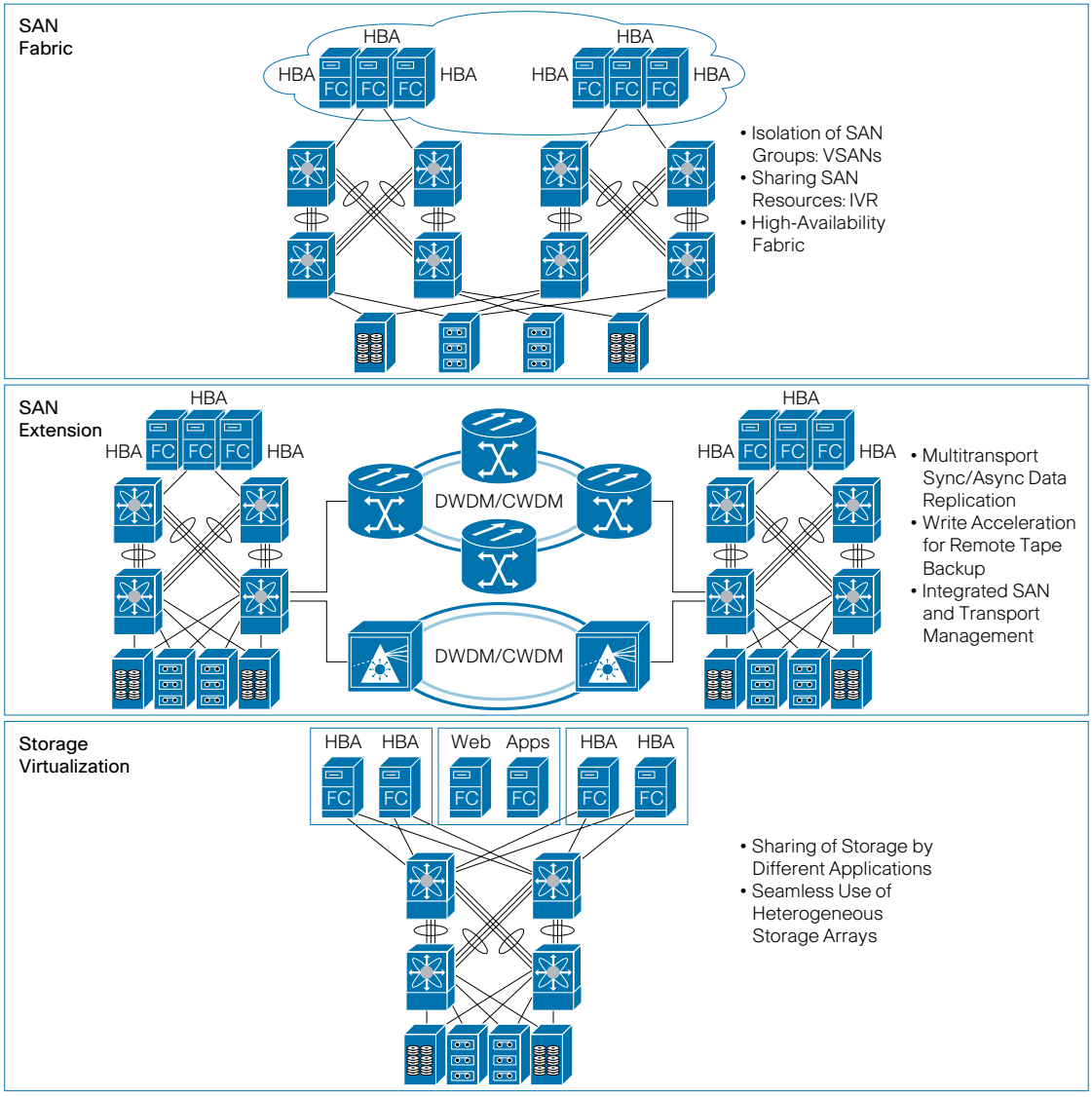
Storage over a Metro-Optical Network

Storage over a MAN enables the healthcare institution to use high-speed, often inexpensive, and highly reliable fiber-optic networks. This facilitates information sharing across a city or across the globe and enables an entire healthcare system to utilize a single physical SAN. In addition to the cost benefits, clinicians and business personnel realize improved information access, regardless of physical location. Extending storage networks across MANs using an optical network infrastructure enables transmitting large files.

Storage over a Wide-Area Network

Using storage over a wide-area network (WAN) enables simple, secure, and highly available storage network interconnection over large geographic distances. In this environment, WAN optimization techniques are deployed to enhance the speed and capabilities of the backup solution, which is particularly beneficial to the clinic, remote provider, and medical office building.

Figure 32. Storage



IP Communications Attributes

IPC represents the ultimate evolution of voice and video integration, encompassing IP telephony, video telephony, unified messaging, IP video and audioconferencing, customer contact solutions, voice gateways and applications, security solutions, and network management. The MGN facilitates operational efficiencies by converging multiple discrete networks into a single network. IPC creates opportunities for real-time, anywhere collaboration by bringing advanced telephony services into the clinical and business environments. Through the use of IPC's integrated features and applications, clinicians at either remote or central locations obtain access to enhanced voice and data collaboration. This technology creates the basic foundation for enhanced application integration in the telephony environment. Figure 34 identifies the attributes that are associated with IPC.

Figure 33. IP Communications Attributes—Structure

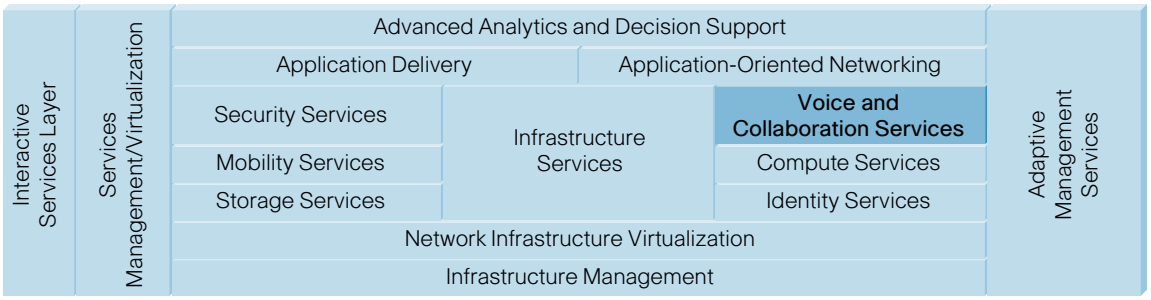


Figure 34. Interactive Services Layer—IP Communications Attributes

Interactive Services—IP Communications Attributes	
MGCP, SIP, QSIG, SCCP, H.323	Standards: H.245, G.711, G.726, G.729, H.225 PCM RTP VAD CRTP Fax Relay
ISDN	Inline power CDP discovery
Analog FXS, FXO, E&M	High availability—SRST, clustering, gatekeepers
FXO answer/disconnect Supervision	Echo cancellation
PRI NFAS	Call detail records
CAMA	E-911

Productivity Applications

Productivity-enhancing applications can be deployed directly to the displays of IP-based phones. These applications enable staff to manage time and attendance at their stations while allowing physicians to view schedules, patient information, and test results.

Open Standards

The IPC solution uses open standards, such as XML, that enable an ecosystem of partners to develop clinical and business applications. XML applications have been widely deployed on mobile phones.

Flexible Reconfiguration of Hospital Spaces

In large healthcare systems, individuals commonly move to different areas or locations within the organization. For medical environments, which regularly move patients as well as personnel, the ability to reconfigure IP-enabled equipment rapidly is a valuable cost-control measure. Hospitals can benefit from the ability to relocate an IP phone from one area of a building to another with automatic re-registration to the phone system. This greatly reduces the cost of moves, adds, and changes that occur frequently in an hospital environment.

Call Admission Control

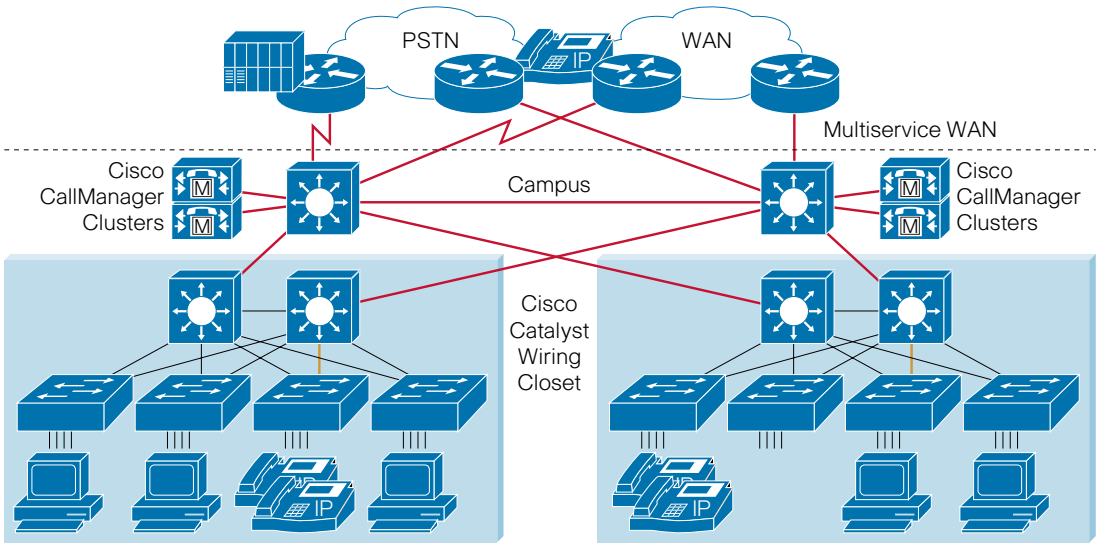
CAC is a concept that applies to voice traffic. When real-time, delay-sensitive traffic, such as voice, experiences network congestion, it is better to deny network access under these conditions than to allow traffic onto the network. Without CAC, traffic may be dropped or delayed, causing intermittent impaired voice transmission that can result in customer dissatisfaction. CAC is, therefore, a deterministic and informed decision that is made before a voice call is established. It is based on whether the required network resources are available to provide suitable QoS for the new call. CAC works to ensure that voice QoS is maintained across constricted WAN links. It also can be used to alternate PSTN routes when WAN bandwidth is not available.

High-Availability Design

The MGN IPC solution is built on high availability for IPC networks, which addresses a user's need to place and receive calls under peak load call rates or during device maintenance or failure. The solution's design addresses various failure situations ranging from planned maintenance downtime to catastrophic failure. The complexity of a high-availability solution is determined by a hospital's availability needs and by the amount of system interruptions that can be tolerated. High-availability solutions improve the IPC network's availability, lower the costs associated with downtime by preventing outages, and reduce the impact of outages when they do occur. In a clinical environment, system interruptions are not tolerated, thereby placing increased importance on high availability. In addition to the high-availability features supported by CallManager clustering, survivable remote site telephony (SRST) is offered.

SRST provides triple call processing redundancy for centralized call management deployments by enabling the remote office router to perform call processing in the event of a WAN failure. Once the disrupted WAN link is restored, the CallManager automatically reregisters the phones and functionality is resumed.

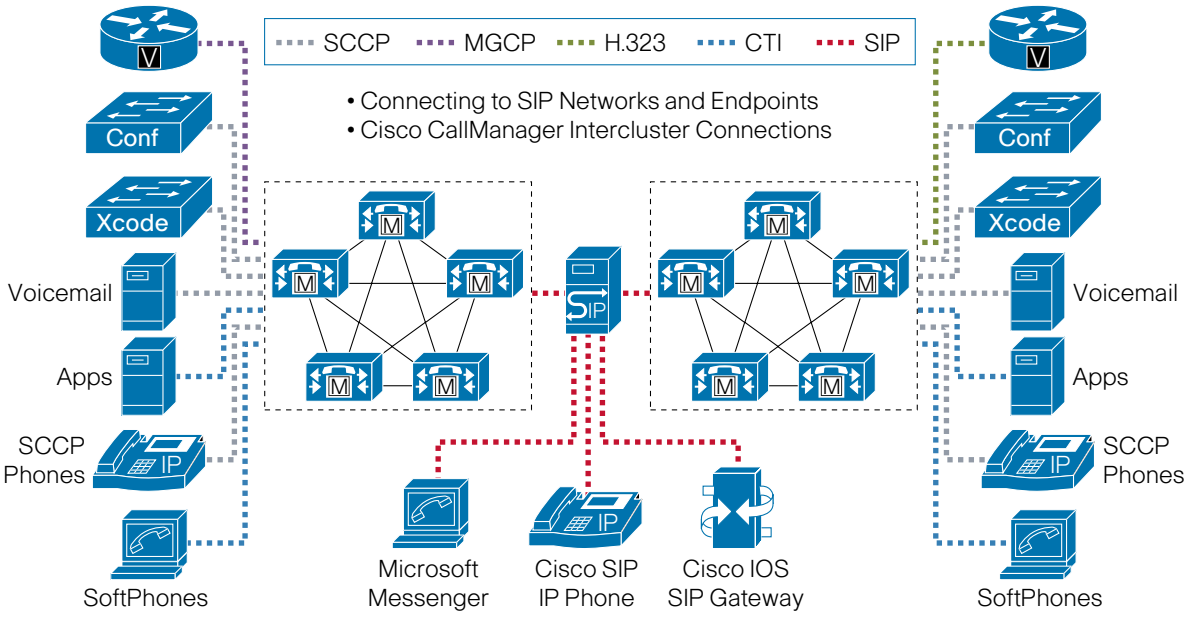
Figure 35. IP Communications



Session Initiation Protocol

The rapid evolution of voice and data technology is changing the healthcare environment significantly. The introduction of services, such as instant messaging, integrated voice and e-mail, and Follow Me, has contributed to a work environment where clinicians and caregivers can communicate much more efficiently and productively. To meet changing demands, healthcare organizations are beginning to deploy converged voice and data networks based on Session Initiation Protocol (SIP).

Figure 36. Session Initiation Protocol



Computing Services Attributes

The medical environment requires intense and highly available computing services. Virtualization and communication across hardware platforms can minimize the hardware necessary to satisfy a healthcare systems' computing requirements. In addition to minimizing the number of servers required, high-performance computing can optimize the space, power, and cooling required to meet the medical data center's needs. Figure 38 identifies the attributes required to support high-performance computing.

Figure 37. Computing Services Attributes—Structure

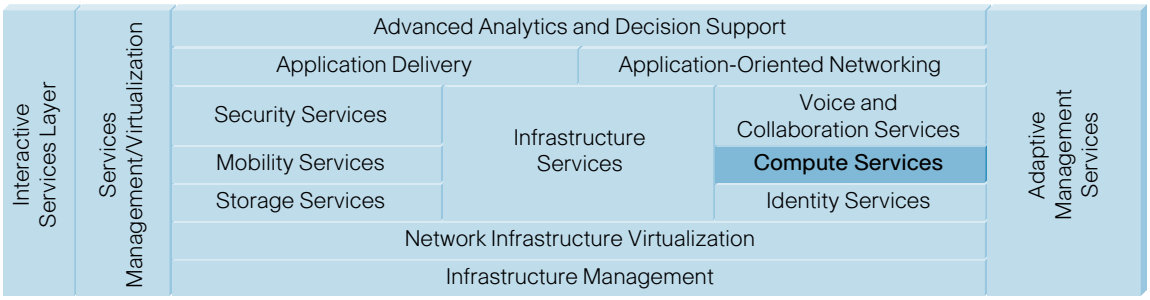


Figure 38. Interactive Services Layer—Computing Services Attributes

Interactive Services Layer—Computing Services Attributes	
High-performance computing • Low-latency fabric (Ethernet or InfiniBand), high-throughput capabilities • Linkage to Inter-Process Communication (IPC) across multiple hosts, such as RDMA	Server virtualization Tools to manage resource pools in a demand-driven environment (VFrame)

The computing service focuses on the server fabric itself and the virtualization capabilities of VFrame.

Server Clustering

Server clustering often is referred to as *high-performance computing*. In server clustering environments, servers are pooled to make applications believe they are running on one large, unified server. In fact, it is many servers working together to process an application as needed. If one server is busy, another one is used. InfiniBand, a high-performance, multipurpose network architecture based on a switched fabric, is a technology that can be used to provide a low-latency, high-speed interconnect between servers.

Input/Output Virtualization

The server switch can connect servers with input/output (I/O) over a unified fabric, promoting server and storage consolidation. This provides operational expenditure reductions by minimizing the amount of computing and storage requirements while making optimal use of the available computing infrastructure.

Utility Computing

VFrame is a data center provisioning and orchestration product that enables utility computing. It provides the ability to commission and decommission shared pools of server and I/O resources rapidly on demand. VFrame system management software creates virtual computing services by programming server switches to map diskless servers to a shared pool of I/O and storage resources.

Cost of ownership can be reduced dramatically by enabling administrators to provision computing services in seconds, not days or weeks; automate tasks based on business policies; and simplify network and server architectures. VFrame also reduces data center downtime through automated server failover, centralized I/O management, and diskless servers.

High-Performance Computing

High-performance computing is achieved through a low-latency fabric with high-throughput capabilities. Linkage to IPC spans multiple hosts, such as RDMA. InfiniBand provides capabilities for efficient data transfer between server memory and I/O devices, without CPU intervention. These characteristics, plus usage of efficient software libraries and protocols, enable clusters of commodity servers to cooperate in executing large, complex calculations that are the basis of many high-performance applications. InfiniBand, along with cluster software, has moved high-performance computing from the realms of expensive supercomputers to an economically viable proposition.

Computers are made up of a number of addressable elements (CPU, memory, screen, hard disks, LAN and SAN interface, and so forth) that use a systems bus for communications. As these elements become faster, the systems bus and the overhead associated with data movement become gating factors in computer performance. To address the problem of server performance with respect to I/O, InfiniBand was developed as a standards-based protocol to provide data movement offload from the CPU to dedicated hardware. This allows more CPU resources to be dedicated to application processing.

InfiniBand Architecture

InfiniBand defines an architecture that incorporates networking principles, switching, and routing to provide a scalable, high-performance server I/O fabric. InfiniBand provides transport services for upper-layer protocols. It supports flow control and QoS to enable ordered, guaranteed packet delivery across the fabric. An InfiniBand fabric may comprise a number of InfiniBand subnets, or links, that are interconnected using InfiniBand routers. Each subnet may consist of one or more InfiniBand switches and InfiniBand attached devices.

Quality of Service—Service Levels and Flow Control

To ensure reliable, sequenced packet delivery, InfiniBand uses flow control and service levels in conjunction with VLanes to achieve end-to-end QoS. InfiniBand VLanes are logical channels that share a common physical link. VLane channels are ranked based on priority. VLane 15 has the highest priority and is used exclusively for management traffic, while VLane 0 is the lowest level of priority. The concept of a VLane is similar to that of hardware queues in routers and switches.

For applications that require dependable delivery, InfiniBand supports reliable packet delivery using flow control. Within an InfiniBand network, the receivers on a point-to-point link periodically transmit information to the upstream transmitter to specify the amount of data that can be transmitted, without data loss, on a per-VLane basis. For applications that do not require reliable delivery (for example, some management traffic), InfiniBand also supports unreliable delivery of packets (they can be dropped with little or no consequence).

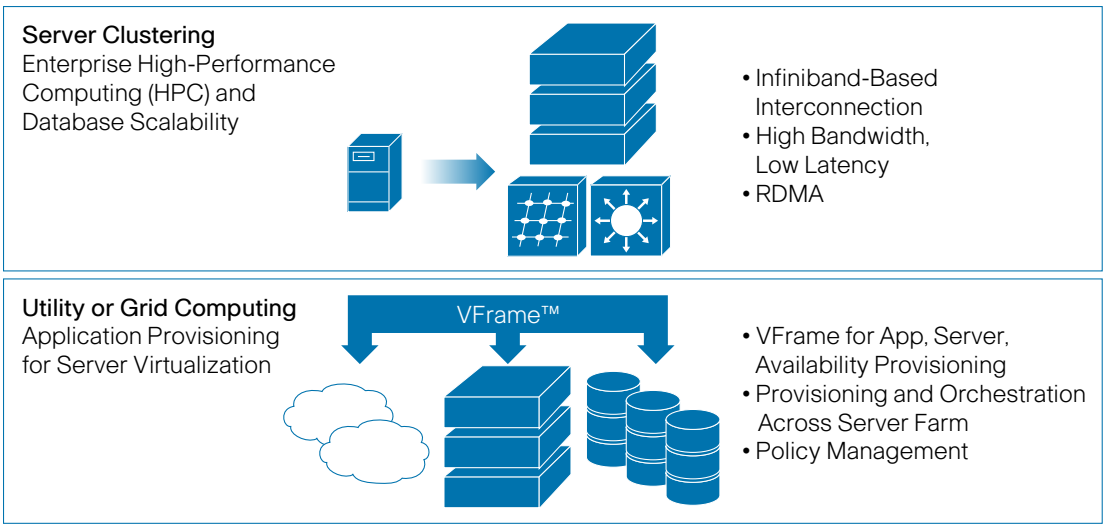
InfiniBand Subnet Management and QoS

InfiniBand supports two levels of management packets: subnet management and the general services interface (GSI). High-priority subnet management packets (SMP) are used to discover the network topology and are transported within the high-priority VLane, which is not subject to flow control. The low-priority GSI management packets handle managerial responsibilities, such as chassis management, and other functions not associated with subnet management. As these are not critical services, GSI management packets are neither transported within the high priority VLane nor subject to flow control.

Remote Direct Memory Access

One of the key problems with server I/O is the CPU overhead associated with data movement between memory and I/O devices, such as LAN and SAN interfaces. InfiniBand uses RDMA to offload data movement from the server CPU to the InfiniBand host HCA. RDMA is an extension of hardware-based Direct Memory Access (DMA) capabilities that allows the CPU to delegate data movement within the computer to the DMA hardware.

Figure 39. Compute Services



Identity Services Attributes

Identity management services are a key component of the holistic security architecture. These service attributes are identified in Figure 41.

Figure 40. Identity Services Attributes—Structure

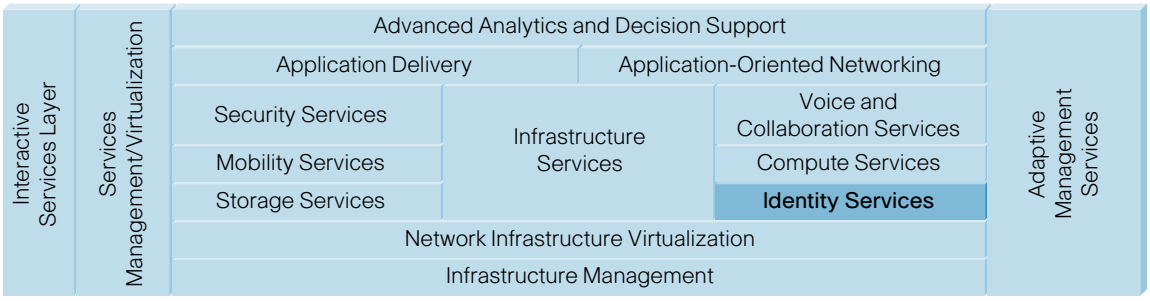


Figure 41. Interactive Services Layer—Identity Services Attributes

Interactive Services Layer—Identity Services Attributes	
Open Standards: WSS, SAML, WS-Trust	Unique asset/location identification
Federated network identity	Identity authentication and authorization to originate, verify, disclose, transmit, or receive clinical content
Opt-in account linking and simplified sign-on within an authentication domain created by business agreements	PKI X.509 certificates
Permissions-based attribute sharing	Identity-based Services • 802.1x with dynamic VLANs • 802.1x with port security • 802.1x with VVID (IP Telephony) • 802.1x guest VLANs • 802.1x with ARP inspection • 802.1x with DHCP • 802.1x and auto QoS • 802.1x with wake on LAN • 802.1x accounting enhancements • 802.1x authenticated identity to port description mapping • 802.1x one-to-many logical VLAN name-to-ID mapping • 802.1x DNS resolution for RADIUS server • 802.1x and ACL/VACL propagation
Schema/protocols for core identity profile service	
Authentication context	
Single sign-on/sign-off	
CCOW compliant	
Electronic signature verification	
SSL sessions based on application ID	
Network admission control (NAC)	
Network-based application recognition (NBAR)	
Standard LDAP, Microsoft Active Directory	
Accounting, audit trails	
Unique patient/clinician identification	

Identity-Based Network Access Control

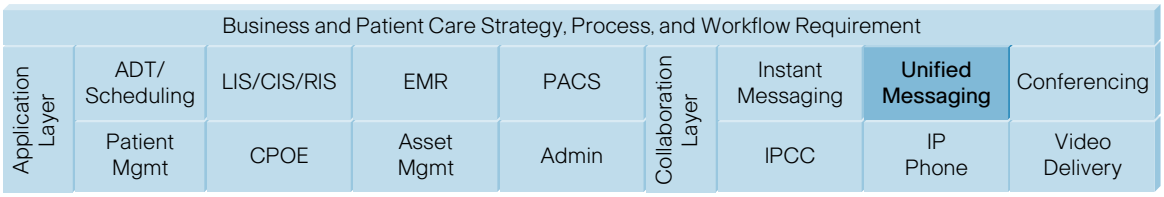
The MGN provides a framework, along with technology standards, for the implementation of true identity-based network access control down to the user and individual access port at the network edge. The system provides user and device identification using strong, reliable authentication technologies. Identities of users or devices are mapped to policies that grant or deny network access, set network parameters, and work with other security features to enforce items such as posture assessments. Mapping to a defined set of policies, identity-based networking provides user and device authentication along with networking identity. Configured authorization policies determine whether to grant or deny access at the port level. Identity-based networking enforces additional policies, such as resource access, to individuals granted access.

Additional capabilities are introduced when an end-to-end system is implemented with switches, wireless LAN access points and controllers, and a secure access control server. Protocols, such as IEEE 802.1x, combine with network devices and components to communicate, thus providing the flexibility to manage network access control and policies. Effective design and deployment offer increased security and control of access to network segments and resources.

Application-Layer Attributes

The application layer facilitates collaboration and visibility between departments, facilities, and organizations. It performs internal business functions, such as back-office systems for business intelligence and network management.

Figure 42. Application-Layer Attributes—Structure



To fulfill its intended tasks, each application must be secure, reliable, flexible, and responsive. The attributes are identified in Figure 43.

Figure 43. Application-Layer Attributes

Application-Layer Attributes
Integration
Collaboration · Conferencing · Unified messaging · Internet Protocol Contact Center · IP Phone attributes · Video delivery

Application-Integration Attributes

The MGN has mission-critical requirements for applications that support healthcare. In the future, Application-Oriented Networking may be used to optimize message routing, improve information sharing, and assist in application integration. Application-integration services could provide application delivery to the end user, as well as communication among application tiers and business services. Using these defined protocols and standards can provide a way for public and private health institutions to transmit important patient record information electronically.

Figure 44. Application-Integration Attributes—Structure

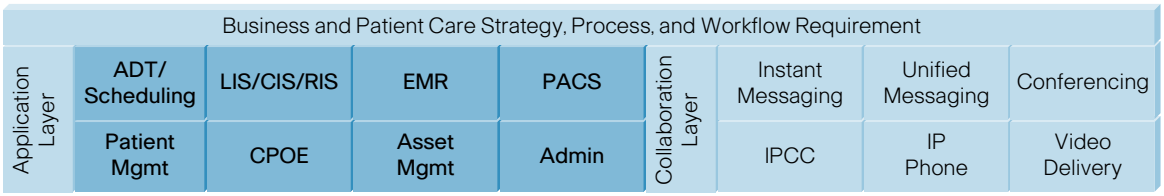


Figure 45 includes the attributes necessary at the MGN's application layer.

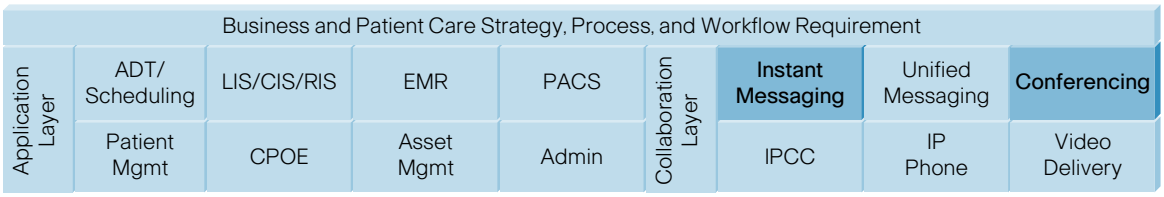
Figure 45. Application Layer—Integration Attributes

Application Layer—Integration Attributes	
HL-7 V2/V3 for data, HL7 CDA (XML for structured text documents)	MIME
XML/HTML/Secure HTTP, SOAP	CORBA
ICD-9, SNOMED	.Net
UB92, HCFA 1500	Common Internet file system (CIFS)
X12 EDI, EDIFACT, NCPDP	Network file system (NFS)
ASTM	HTTP, HTTPS
DICOM	FTP, trivial file transfer protocol (TFTP)
Record locator service (RLS) for locating patient data	Domain name system (DNS)
Patient indexing and matching system	Business video: real-time streaming protocol (RTSP), Microsoft Media Streaming (MMS)
SSL/TLS encryption among application clients for patient data	Notification system for public health alerts

Collaboration/Conferencing Attributes

Collaborative and conferencing services are critical to advancing patient care, training, and other information-sharing initiatives. A Unified Communications system of voice and IP products and applications enables organizations to communicate more effectively. Business processes are streamlined, giving clinicians and ancillary personnel the ability to reach the right resource the first time. Unified Communications offer an integrated solution for a healthcare organization's conferencing needs.

Figure 46. Collaboration/Conferencing Attributes—Structure



The MGN offers enterprise-class, rich-media conferencing, incorporating voice, Web, and video. These real-time collaborative functions are essential features of the healthcare communications landscape. Using high-reliability components and component redundancies helps ensure high availability. Servers and software are customizable and integrate with common enterprise communication software to fit easily into any corporate infrastructure. In order to meet these mandates, the MGN has stringent conferencing requirements. The attributes necessary to support conferencing in the healthcare environment are identified in Figure 47.

Figure 47. Application Layer—Collaboration/Conferencing Attributes

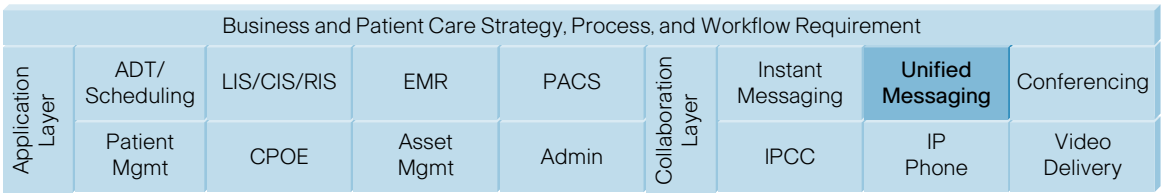
Application Layer—Collaboration/Conferencing Attributes	
In-conference features · Announced entry and departure · Roll call · Breakout sessions · Mute · Out-dial capability · Lock meeting · Screened entry	Integrates with directory services, e-mail systems, and other applications through standard protocols such as LDAP, SMTP, and HTTP/HTTPS
Reservationless meeting option	Multilanguage support
Meeting record and playback	Custom scripting
Lecture-style meetings	Fully integrated voice and Web conferences
Conference user interface · Identifies conference speakers · Lists meeting attendees · Meeting organizer can mute, unmute, change speaking ability, record, lock, eject, and end a meeting · Search for users by primary phone, alternate phone, and pager number	Integrates with Lotus Notes or Microsoft Outlook calendaring

Application Layer—Collaboration/Conferencing Attributes	
Ability to prerecord messages for other participants prior to entering a meeting	Integration to LDAP or Microsoft Active Directory for directory services
Slide annotation	Whiteboarding
Voice and Web recording	Application sharing
Chat	Instant-messaging integration

Collaboration/Unified Messaging Attributes

Unified messaging is a feature-rich solution that makes it easier for clinicians, staff, and caregivers to perform their jobs. Unified messaging in the medical environment facilitates improved communication by merging traditional and IP-based communications, allowing patients and clinicians to collaborate better.

Figure 48. Collaboration/Unified Messaging Attributes—Structure



The attributes necessary to support conferencing in the healthcare environment are listed in Figure 49.

Figure 49. Application Layer—Collaboration/Unified Messaging Attributes

Application Layer—Collaboration/Unified Messaging Attributes	
Archived and new messages	Navigation
Archiving (voicemail)	Online help system
Broadcasting (bullets and boards)	Password administration
Broadcasting (system)	Password policy
Change prompt levels	Personal mailing list
Destination options	Prompts and levels
Erase messages	Rapid brief prompts
Extended prompts	Record extended absence greeting
Fax	Record messages
Forward messaging	Record personal greetings
Greeting bypass	Reply to a message
Listening controls	Spoken name
Locating message sent	System distribution
Locating messages received in mailbox	Undeleted erased messages
Message notification	

Unified Communications integrates the two separate worlds of phone and Internet over a single, unified network.

Unlike time-division multiplex-based proprietary messaging solutions, MGN's Unified Communications platform is built on open-protocol voice and data architecture. The standards-based services platform is designed to carrier-class specifications, providing scalability to support millions of subscribers. Synchronous and asynchronous message types, including VoIP, Internet fax, store-and-forward voicemail, and e-mail, are combined under a common message store and directory. This arrangement eliminates the need to synchronize disparate message stores and directories while dramatically reducing operational and maintenance costs.

Unified Messaging

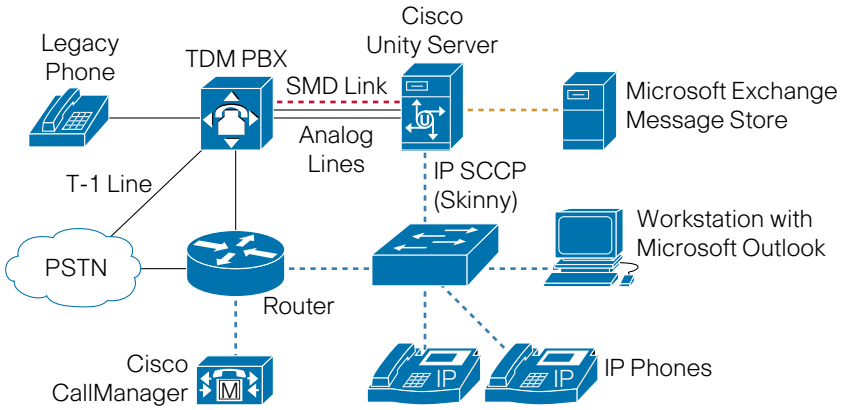
E-mail messaging over IP enables subscribers to access e-mail messages from a telephone by using one access device for all messages. Voice messages are played as streaming audio or .wav files. Paging notification indicates the arrival of e-mail messages, which can be listened to from a telephone using the text-to-speech feature and responded to by creating an audio attachment. E-mail messaging over IP supports both POP and Internet messaging access protocol clients.

Fax messaging over IP lets subscribers receive faxes anywhere by redirecting fax messages from their unified messaging mailbox to a nearby fax machine. Fax messaging over IP also enables subscribers to determine, via phone, which faxes have arrived, the arrival time, and the sender's identity. Paging notification occurs when faxes arrive. Faxes are viewable as .tif files and then can be saved in separate folders. Faxes also may be forwarded as e-mail attachments. Users are afforded greater privacy by printing faxes from their mailboxes when they are ready to view them.

Single-Number Reachability

The single-number reachability feature improves accessibility by providing one phone number that callers use to locate a subscriber in multiple locations. With single-number reachability, callers can use one number to dial a subscriber's work phone, home phone, or wireless phone. Callers can elect to locate the subscriber or leave a message, and are not trapped in the system waiting to locate the subscriber.

Figure 50. Collaboration/Unified Messaging



Collaboration/Internet Protocol Contact Center Attributes

In the medical environment, it is critical that calls are delivered to the appropriate clinician. Through the IP Contact Center (IPCC), using skills-based routing, calls are forwarded based upon personnel skill set or caller requirements. Additionally, calls are prioritized and serviced in a manner that promotes the best quality care. This technology can be used on healthcare's business side to optimize both workflows and communication pathways.

A contact center handles more than inbound telephone calls; it is a fully integrated, multifunction customer contact center. IPCC solutions enable a hospital to implement a single service to blend multiple communications mediums, including voice, Web, and e-mail. This offers the choice of interacting with a contact center via telephone, Web callback, VoIP, text chat, or e-mail. To provide these alternatives, the contact center, Web collaboration, e-mail, and telephony services are offered as tightly integrated components. As with all other MGN components, the contact center requires a holistic security architecture.

The attributes necessary for effective contact center interactions are identified in Figure 52.

Figure 51. Collaboration/IPCC Attributes—Structure

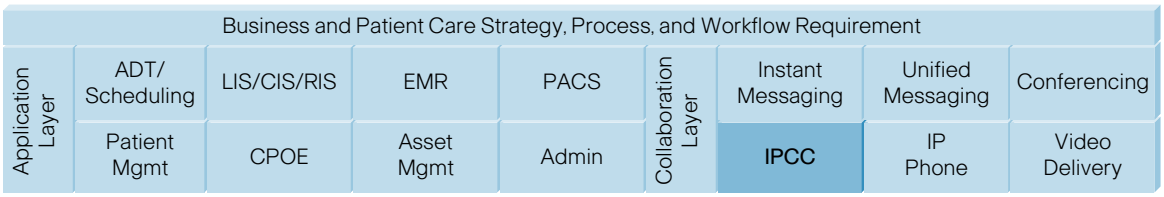
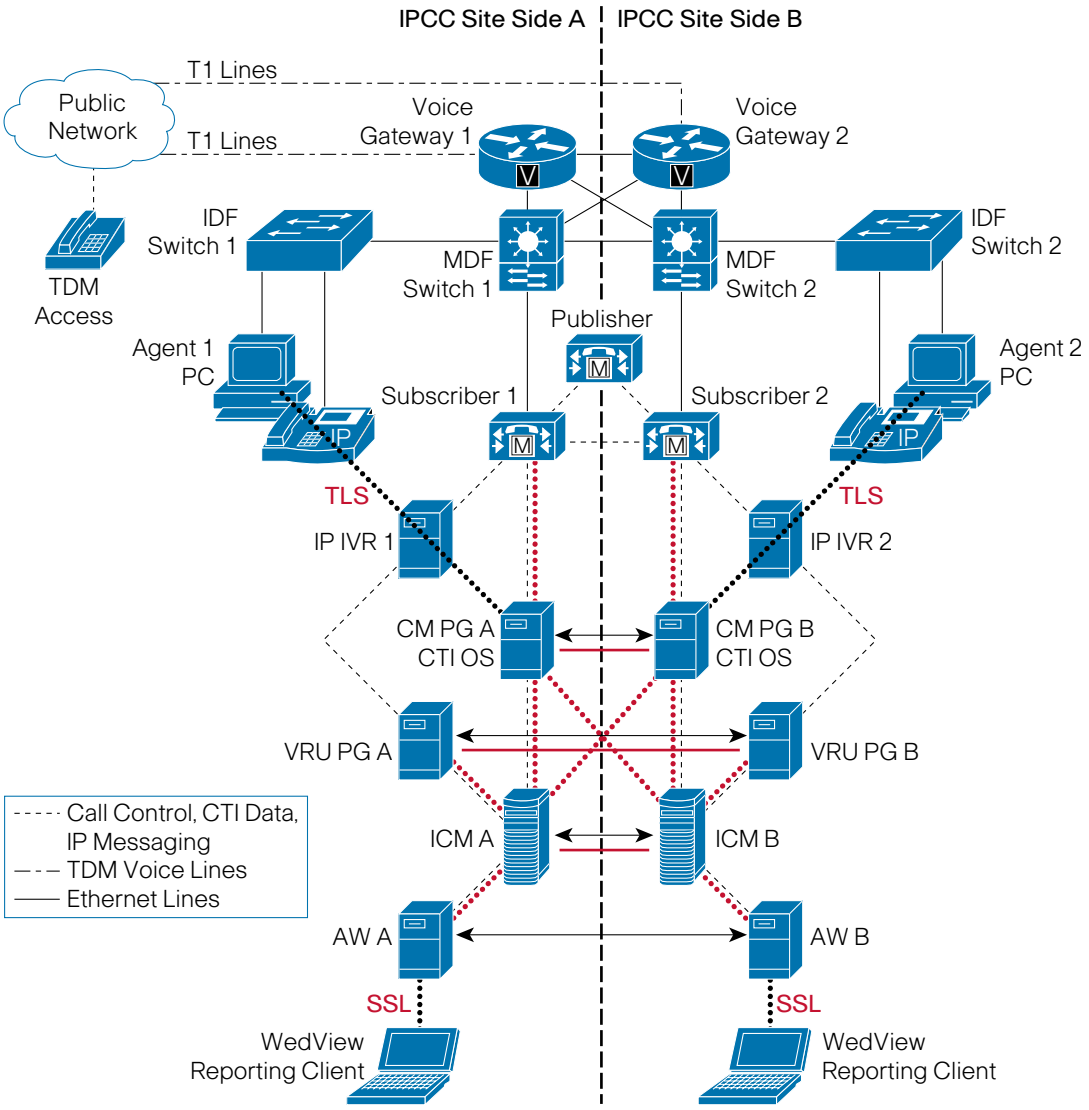


Figure 52. Application Layer—Collaboration/IPCC Attributes

Application Layer—Collaboration/IPCC Attributes	
Custom scripting	Dynamic priority queuing
ANI	Automated attendant
DNIS	Automatic speech recognition
Skill-based routing	Integrated CTI/screen pop
Conditional routing (time of day, day of week, custom variables, and so forth)	Call log for tracking incoming and outgoing calls
Overflow, interflow, intraflow routing	Unified-messaging support
Custom routing based on enterprise data (for example, priority routing)	Voice-messaging interface

Figure 53. Application Layer—Collaboration/IPCC



Collaboration/IP Phone Attributes

The IP phone is designed to enhance the communication capabilities of both clinicians and support staff. IP phones, by their very nature of merging telephony and computers, provide a platform for enhanced communications applications. The attributes required in an IP phone are identified in Figure 55.

Figure 54. Collaboration/IP Phone Attributes—Structure

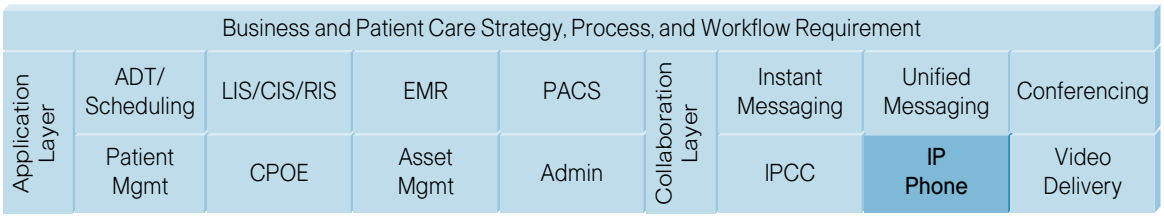


Figure 55. Application Layer—Collaboration/IP Phone Attributes

Application Layer—Collaboration/IP Phone Attributes	
Click to dial	Automatic camp-on
Call processing delivered over a distributed architecture	Automatic recall
Global directory	Automatic alternate routing
Consolidated dial plan (ENUM)	Meet-me conferencing
Routing functions in network	Trunk callback queuing
Global resource management	Hunting
Call transfer, call forwarding, automatic callback	Uniform call distribution
Calling number and name on voice terminal display	Call detail recording
Trunk ID on voice terminal display	Uniform dial plan
Call diversion information on voice terminal display	Trunk group busy warning indicators
Add-on conference	Trunk group access and control
Call waiting, barge-in (busy override)	Serial call
Emergency access to attendant	Call distribution to attendants
Paging system access	Night service
Station user roaming (logical station assignment)	Paging
Message-waiting activation	Override of diversion features
APIs for advanced applications (JTAPI; XML)	

The MGN takes advantage of IP communications to enhance the information interchange flexibility of clinicians and ancillary personnel. The IPC solution is holistic and uses security, QoS, in-line power, and other features in the network fabric. IP phones provide rich call features and functions while supporting additional information services, including XML capabilities.

Computer Telephony Integration Applications

Computer telephony integration (CTI) applications allow interactions on a telephone and a computer to be integrated or coordinated. CTI technology is used to integrate applications, such as interactive voice response (IVR), intelligent routing, and agent workflow automation, into a telephone system. CTI automates several functions, increasing the number of calls that can be managed. Using CTI applications, hospitals and medical offices handle patient, pharmaceutical, and insurance information; schedule appointments; forward medical transcripts; and provide telemedicine services.

Collaboration/Video Delivery Attributes

The MGN augments collaboration in the healthcare environment. Possibly the most beneficial changes to collaborative care occur with enhanced videoconferencing. High-definition TelePresence increases a provider's reach to patients in other geographies. Videoconferencing enables a clinician to pick up cues regarding a patient's condition from verbal and nonverbal findings. Additionally, videoconferencing facilitates on-demand clinician-to-clinician conferencing.

Videoconferencing provides instant worldwide connectivity. Through changes in communications technology, low-cost bandwidth, and continuous improvements in hardware and performance, these solutions provide physicians and caregivers the tools they need to be more productive, make decisions faster, provide care more effectively, save time, and avoid the burden of travel. The rising penetration of high-speed access technologies, such as optical networks, broadband, and satellite connectivity, is driving an increase in the use of telemedicine by healthcare providers. Audio and videoconferencing technologies enable instant communication between clinicians, first responders, and other health experts, thereby improving collaboration and patient care.

Figure 56. Collaboration/Video Delivery Attributes—Structure

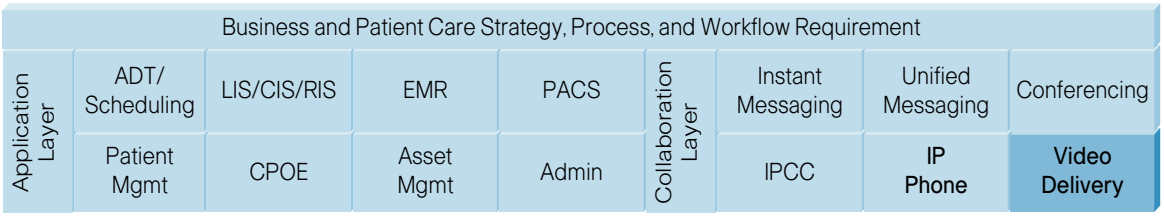


Figure 57 includes the attributes necessary for effective communication in the healthcare environment.

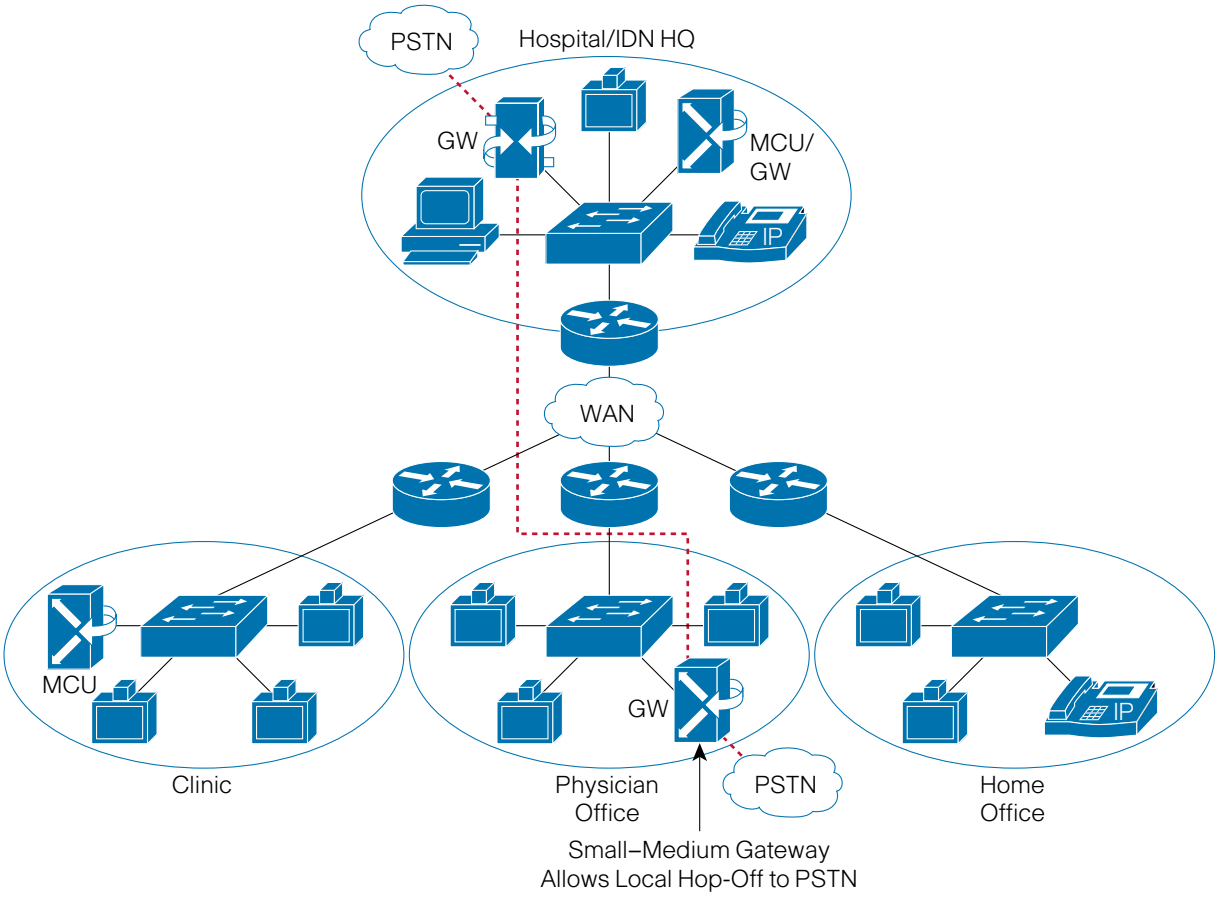
Figure 57. Application Layer—Collaboration/Video Delivery Attributes

Application Layer—Collaboration/Video Delivery Attributes	
Video Codec • MPEG1, MPEG2 (~1.5MB to 15MB), MPEG4, WMV, DivX, MJPEG	Jitter control • QoS architecture and policy • QoS Design—proper classification and prioritization of voice and video packets
Transmission Standard • H.320 (legacy systems) • H.323, SIP (TCP/IP-based) • SCCP (Video Telephony)	H.263 Annexes (F, J, N)
Bandwidth Control • QoS, admission control	G.722.1
4CIF, 16CIF	VGA, XVGA, SVGA
DuoVideo	DownSpeeding

The MGN IP Video Telephony solution fully integrates video into the call management service, making video easy to deploy, manage, and use. The solution consists of a call management system, multipoint control units (MCUs) for both H.323 and Skinny Client Control Protocol (SCCP) conference calls, H.320 gateways, H.323 gatekeeper, SCCP endpoint solutions, and the existing range of H.323-compliant products.

Through this architecture, legacy H.320 circuit-switched networks are connected to H.323 IP networks, preserving original videoconferencing investments. IP videoconferencing MCUs work with an external T.120 server to provide coordinated audio, video, and data streams to endpoints with T.120 capability.

Figure 58. Collaboration/Video Delivery



End-to-End IP Video Connectivity

The MGN takes full advantage of videoconferencing. Employing interactive video over an IP network provides significant savings through the convergence of video and data traffic over a common path. Video terminals need only to rely on simple Ethernet NICs for network connectivity. Multipoint conferencing and multimedia gateways are converged into a single, modular, and flexible platform for high-performance videoconferencing deployments. Built upon industry-standard H.323 technology, the MGN videoconferencing solution enables a wide range of customized voice, video, and data features.

The H.323 protocol builds on top of existing IP data networks, thus saving money and scaling to larger deployments. The resulting decrease in expense allows an exponential increase in the deployment of H.323 terminals. The MGN promotes movement of shared videoconferencing assets from common areas to the user desktop. For example, clinical meetings and remote patient visits can take place with H.323 over IP networks.

H.323 endpoints provide user-interface and human communications. These endpoints can call through the gateway to H.320 endpoints anywhere in the world or join conferences hosted on H.320 MCUs. Endpoints can be rooms, groups, or desktop systems. Via the IP infrastructure, audio and video streams are routed directly to a doctor, nurse, or caregiver.

Advanced Technologies and Flexible Architecture Combine to Meet Changing Clinical and Business Needs

To address the growing challenges of providing healthcare, all members of the healthcare system—including patients—must be part of the connected ecosystem. The MGN provides the foundation for this ecosystem by supporting healthcare's requirements for interoperability, security, availability, productivity, and flexibility. This is accomplished while helping ensure the highest-quality outcomes and maximizing operational efficiencies.

We have detailed the attributes and capabilities of each of the three functional layers of the MGN. Each layer provides the necessary collaborative capabilities to maximize communications efficiencies, facilitating sharing of critical clinical, business, and collaborative information throughout an organization as it evolves to a connected healthcare ecosystem. Because the MGN and its layers are built on SONA, they enable the adoption of new technologies and resolve how to apply these technologies. The MGN's end-to-end framework helps healthcare organizations and providers solve today's business and clinical issues while preparing for the future.

The following glossary has been compiled to assist the reader in understanding the Medical-Grade Network and related technologies. It contains industry-accepted definitions of terms and acronyms obtained from a wide variety of informational sources, corporate guidelines, and public domain Websites. Many of the definitions/acronyms contained in this glossary could have different meanings in other contexts.

Glossary

Term	Acronym	Definition
.Net		A business strategy from Microsoft and its collection of programming support for Web services, which provide the ability to use the Web rather than an individual computer for various services.
802.11		802.11 is the generic name of a family of standards for wireless networking. The numbering system for 802.11 comes from the IEEE, which uses 802 for many networking standards like Ethernet (802.3). 802.11 standards define rules for communication on WLANs. Popular 802.11 standards include 802.11a, 802.11b, and 802.11g. 802.11 was the original standard in this family, ratified in 1997. 802.11 defined WLANs that operate at 1–2 Mbps. This standard is obsolete today.
		Each extension to the original 802.11 appends a unique letter to the name, as follows:
		802.11a—54-Mbps standard, 5-GHz signaling (ratified 1999)
		802.11b—11-Mbps standard, 2.4-GHz signaling (1999)
		802.11c—Operation of bridge connections (moved to 802.1)
		802.11d—Worldwide compliance with regulations for use of wireless signal spectrum (2001)
		802.11e—Quality of Service (QoS) support (not yet ratified)
		802.11f—Protocol for communication between access points to support roaming clients (2003)
		802.11g—54-Mbps standard, 2.4-GHz signaling (2003)
		802.11h—Enhanced version of 802.11a to support European regulatory requirements (2003)
		802.11i—Security improvements for the 802.11 family (2004)

Term	Acronym	Definition
		802.11j—Enhancements to 5-GHz signaling to support Japan regulatory requirements (2004)
		802.11k—WLAN system management (in progress)
		802.11l—Skipped to avoid confusion with 802.11i
		802.11m—Maintenance of 802.11 family documentation
		802.11n—Future 100-plus-Mbps standard (in progress)
Access Control List	ACL	Access lists filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces.
Access Point	AP	Specially configured nodes on wireless local area networks (WLANs). Access points act as a central transmitter and receiver of WLAN radio signals.
Active Attack		A hacker attack in which the unauthorized user may modify or disrupt network resources. These can be detected through a variety of methods. Disruptions may include the presence of rogue access points or include man-in-the-middle attacks, packet replay attacks, session hijacking, and denial-of-service (DoS) attacks.
Adaptive Differential Pulse Code Modulation	ADPCM	A widely used variation of PCM that codes the difference between sample points, such as differential PCM (DPCM), but also can dynamically switch the coding scale to compensate for variations in amplitude and frequency.
Adaptive Management Services		Services composed of infrastructure management (automated management of collections of devices), services management (management of interactive services), and advanced analytics and decision support. These management services are implemented though APIs to other parts of the infrastructure to enable the network to share policy and control information across all layers of the IT infrastructure.
Address Resolution		A method for resolving differences between computer addressing schemes. Address resolution usually specifies a method for mapping network-layer (Layer 3) addresses to data-link-layer (Layer 2) addresses.
Address Resolution Protocol	ARP	A protocol used by IPv4 to map IP network addresses to the hardware addresses used by a data link protocol. The protocol operates below the network layer as part of the interface between the OSI network and OSI link layer.
Admission, Discharge, Transfer	ADT	The systems used by healthcare facilities to track patients from arrival to departure.
Advanced Encryption Standard	AES	A block cipher, and the most current encryption method currently available for network protection. AES has been adopted by the National Institute of Standards and Technology (NIST).

Term	Acronym	Definition
Agent		An object or application that can be a server, client, or both.
Allowed Charge		The amount a payer approves for payment to a physician.
Ambulatory Patient Classifications	APC	A system for classifying outpatient services and procedures for purposes of payment. The APC system classifies some 7,000 services and procedures into about 300 procedure groups.
American National Standards Institute	ANSI	The American National Standards Institute is a private not-for-profit organization that oversees the development of voluntary consensus standards for products, services, processes, systems, and personnel in the United States. The organization also coordinates U.S. standards with international standards so that American products can be used worldwide.
American Society for Testing and Materials	ASTM	The ASTM develops voluntary consensus standards, related technical information, and services having internationally recognized quality and applicability that promote public health and safety and the overall quality of life. It contributes to the reliability of materials, products, systems, and services, and facilitates national, regional, and international commerce.
Ancillary Care		Additional healthcare services performed, such as lab work and X-rays.
Annual Maximum Limits or Caps		The limit an insurance plan sets on a given service. It may be a certain number of visits or a dollar amount.
Anti-X		A Cisco solution that combines enterprise-grade firewall and high-quality malware protection. In addition, it provides strong protection and control for business network communications, stops network threats, and controls unwanted mail and Web content.
Application Program Interface	API	The language and message format by which an application program talks to communications software. Standardized APIs allow application programs to be developed independently of the underlying method of communication.
Application Services Virtualization		Applies to both application delivery and Application-Oriented Networking services. Example: load balancing instances applied to various application environments independently from the same hardware. To the network administrator, each instance appears to be a separate device with its own configuration, CLI, and access control. Yet all instances can be supported by a common physical device.

Term	Acronym	Definition
Application-Oriented Networking	AON	A technology that provides message processing, routing services, and application-message-based networking.
Applications Layer		Contains the business and collaborative applications that take advantage of efficiencies from interactive services and networked infrastructure.
Architecture		The overall system design, structure, and components of software or hardware, an operating system, or a network.
ASC X12		The committee chartered by the American National Standards Institute to develop uniform standards for inter-industry electronic interchange of data for business transactions.
ASLEAP		A tool designed to recover weak passwords on Cisco LEAP networks. Works by mounting an offline dictionary attack against weak passwords. See Dictionary Attack.
Assessment		The regular collection, analysis, and sharing of information about health conditions, risks, and resources in a community. The assessment function is needed to identify trends in illness, injury, and death; the factors that may cause these events; available health resources and their application; unmet needs; and community perceptions about health issues.
Asymmetric Digital Subscriber Line	ADSL	A technology that allows higher data rates over standard telephone lines.
Asynchronous Transfer Mode	ATM	A high-speed networking standard designed to support both voice and data communications. It is normally used by Internet service providers on their private long-distance networks. ATM operates at the data link layer (Layer 2) over either fiber or twisted-pair cable. The performance of ATM often is expressed in the form of OC (Optical Carrier) levels, written as OC-xxx. Performance levels as high as 10 Gbps (OC-192) are technically feasible with ATM.
Audio Messaging Interchange Specification	AMIS	A protocol supported by Cisco that provides an analog mechanism for transferring voice messages between different voice messaging systems.
Authentication		The method used to confirm a user's identity, preliminarily by user ID and password, but may require other technologies, such as biometrics (electronic capture and analysis of patterns of fingerprinting, retinal scans, or voice recognition) and/or PKI.
Authentication, Authorization, and Accounting	AAA	An architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing authentication, authorization, and accounting services.

Term	Acronym	Definition
Automated Dispensing		A service that provides healthcare facilities a point-of-use dispensing system. These systems are integrated with healthcare facilities' information.
Automatic Call Distributor	ACD	A programmable device at a call center that routes incoming calls to targets within that call center. After the ICM software determines the target for a call, the call is sent to the ACD associated with that target.
Automatic Number Identification	ANI	A feature that provides the billing phone number from which a call originated or the phone number itself.
Balance Billing		The practice of billing a patient for any portion of healthcare charges that are not covered (paid for) by health insurance.
Bandwidth	BW	The amount of data (in bits) that can be transmitted per second over a particular network connection or through a system.
Bandwidth Control		Implementing QoS provides bandwidth control and predictable service for a variety of networked applications and traffic types. QoS ensures desired results and enables efficient, predictable services for business-critical applications.
Basic Rate Interface	BRI	One of two levels of ISDN service. The BRI provides two bearer channels for voice and data and one channel for signaling (commonly expressed as 2B+D).
Basic Service Area	BSA	The basic service area is the area of RF coverage provided by an access point, also referred to as a cell.
Beacon		A wireless LAN packet that signals the availability and presence of a wireless device.
Bits per Second	bps	A measurement of how much data can be transmitted across the medium or channel. A bit is the smallest piece of computerized information—a binary digit—representing on (1) or off (0).
Blade Server		A server chassis housing multiple thin, modular electronic circuit boards, known as server blades. Each blade is a server in its own right, often dedicated to a single application.
Border Gateway Protocol	BGP	BGP performs interdomain routing in Transmission Control Protocol/Internet Protocol (TCP/IP) networks. It is an exterior gateway protocol (EGP), which means that it performs routing between multiple autonomous systems or domains and exchanges routing and reachability information with other BGP systems.

Term	Acronym	Definition
Bridge Protocol Data Unit	BPDU	This unit is a part of the spanning tree protocol that helps describe and identify attributes of a switch port. BPDUs allow switches to obtain information about each other.
Bridges		Bridges filter data traffic at a network boundary and reduce the amount of traffic on a LAN by dividing it into two segments. Bridges operate at the data link layer (Layer 2) of the OSI model, inspecting incoming traffic and deciding whether to forward or discard it. An Ethernet bridge, for example, inspects each incoming Ethernet frame (including the source and destination MAC addresses, and sometimes the frame size) in making forwarding decisions.
Broadband	BB	A user access network connection with bandwidth of approximately 1 Mbps or more. Broadband is essential for graphic-intensive Websites, music services, and video applications. Common forms of broadband include Digital Subscriber Line (DSL), cable modem, wireless access (Wi-Fi), and Metro Ethernet (Ethernet access over optical fiber).
Building Automation		A programmed, computerized, intelligent network of electronic devices that monitor and control the mechanical and lighting systems in a building.
Business Applications		Horizontal and vertical applications that Cisco partners and others offer to meet businesswide or departmental requirements.
Call Admission Control	CAC	The set of actions taken by a network during the set-up phase of a call event to determine if the event should be accepted or rejected.
Call Center		A single site at which incoming phone calls are received and answered.
Call Detail Record	CDR	A term used to describe log records for calling services. This information includes the call's origination, the start time, to whom the call was made, what time the call ended, and so forth.
Call Management System	CMS	A system designed to manage incoming and outgoing calls.
CallRouter		The process of receiving call-routing requests and determining the best destination for each call. It also collects information about the entire system.
Carrier		(1) An organization, typically an insurance company, that has a contract with the Health Care Financing Administration (HCFA) to administer claims processing and make Medicare payments to healthcare providers for most Medicare Part B benefits. (2) A private contractor that administers claims processing and payment for Medicare Part B services.

Term	Acronym	Definition
Case Management		Monitoring and coordination of health services for individual patients to enhance care and manage costs. Often used for patients with specific diagnoses or who require high-cost or extensive healthcare services.
Cell		The service area of RF coverage provided by a wireless access point. Also referred to as the Basic Service Area (BSA).
Centers for Medicare and Medicaid Services	CMS	The U.S. federal agency that administers Medicare, Medicaid, and the State Children's Health Insurance Program.
Centralized Automatic Message Accounting	CAMA	An analog phone trunk that connects directly to an E911 selective router, bypassing the PSTN.
Charges		The posted prices of provider services.
Cipher Block Chaining	CBC	Cipher block chaining (CBC) is a mode of operation for a block cipher (one in which a sequence of bits is encrypted as a single unit or block with a cipher key applied to the entire block).
Cisco CallManager Express	CCME	A Cisco service that provides call processing for Cisco IP phones.
Cisco Centralized Key Management	CCKM	This Cisco management service allows authenticated client devices to roam from one access point to another without any perceptible delay during re-association. The access point acts as a subnet context manager (SCM) and creates a cache of security credentials for CCKM-enabled client devices on the subnet.
Cisco Compatible Extensions	CCX	These Cisco extensions ensure the widespread availability of client devices that are interoperable with a Cisco Wireless LAN (WLAN) infrastructure and take advantage of Cisco innovations for enhanced security, mobility, quality of service, and network management.
Cisco Discovery Protocol	CDP	A Cisco protocol that runs over Layer 2 (the data link layer) on all Cisco routers, bridges, access servers, and switches. CDP allows network management applications to discover Cisco devices that are neighbors of already known devices—in particular, neighbors running lower-layer, transparent protocols.
Cisco Security Agent	CSA	Cisco software that protects server and desktop computing systems by identifying threats and preventing malicious behavior. It also mitigates new and evolving threats without requiring reconfigurations or emergency patch updates.
Cisco Trust Agent	CTA	Cisco's implementation of the posture agent. See Posture Agent.

Term	Acronym	Definition
Cisco Unified CallManager Express	CCME	Cisco IOS Software that provides call processing for Cisco Unified IP phones. It enables Cisco's access and Integrated Services Routers to deliver a set of features commonly used by businesses.
Cisco Unity Express	CUE	Cisco's voicemail and auto-attendant services for small and medium-sized businesses (SMBs) and branch offices.
Claim		The documentation of a medical service that is provided to a covered patient by a doctor, hospital, laboratory, diagnostic service, or other medical professional.
Class of Service	COS	A collection of permissions and restrictions assigned to each subscriber that control access and system usage.
Client		A wireless end-user device, such as a laptop computer, PDA, or wireless IP phone.
Clinical Context Object Workgroup	CCOW	An HL7 standard healthcare protocol designed to enable disparate applications to synchronize in real time, and at the user interface level. It is vendor independent and allows applications to present information at the desktop and/or portal level in a unified manner.
Clinical Information Systems	CIS	An application managing the acquisition, storage, manipulation, and distribution of clinical information throughout a healthcare organization.
Clinical Standards		The care guide used by health plans and providers in making decisions about medical necessity.
Clinician		A term that describes all types of medical professionals who care for patients, including doctor or physician, nurse, physician's assistant, therapist, and so forth.
Cluster		Integrates the resources of two or more computing devices (that could otherwise function separately) for a common purpose, such as a data center.
Coder-Decoder	Codec	A device that transforms analog voice into digital bitstream and vice versa.
Code Excited Linear Prediction	CELP	A speech-encoding algorithm where a limited set of pulses is distributed as excitation to a linear prediction filter.
Coding		A mechanism for identifying and defining physician services.
Collaboration Applications		Applications that Cisco and its partners offer to improve communication and collaboration, and optimize or establish business processes.
Common Intermediate Format	CIF	A standard video format used in videoconferencing. CIF formats are defined by resolution and standards both above and below the established original resolution. The original CIF also is known as Full CIF (FCIF). 4CIF (4 x CIF) resolution is 704 x 576. 16CIF (16 x CIF) resolution is 1408 x 1152.

Term	Acronym	Definition
Common Internet File System	CIFS	A platform-independent file-sharing system that provides users with network access to files, printers, and other machine resources.
Common Management Information Protocol	CMIP	An Open Systems Interconnection-based network management protocol that supports information exchange between network management applications and management agents.
Common Object Request Broker Architecture	CORBA	A communication pathway between disparate systems, CORBA is an architecture and specification for creating, distributing, and managing distributed program objects in a network. It allows programs at different locations, and developed by different vendors, to communicate in a network through an interface broker. CORBA was developed by a consortium of vendors through the Object Management Group (OMG). Both ISO and X/Open have sanctioned CORBA as the standard architecture for distributed objects (also known as components).
Complementary Code Keying	CCK	A modulation technique used by IEEE 802.11b-compliant WLANs for transmission at 5.5 and 11-Mbps.
Compression		The process of encoding information using fewer bits, or information units, with specific encoding schemes.
Compression Real-Time Protocol Header	cRTP	Header compression for real-time protocol traffic, cRTP is used to compress IP/UDP/RTP headers from 40 bytes to 2 to 4 bytes. cRTP reduces voice bandwidth requirements and minimizes serialization delay.
Compression Service Adapter	CSA	An adapter providing high-performance, hardware-based data-compression capabilities for routers.
Computerized Tomography	CT Scan	Computerized tomography, also known as a CT scan, is a diagnostic procedure that uses special X-ray equipment to obtain cross-sectional pictures of the body.
Computer Telephony Integration	CTI	(1) The technology that allows interactions on a telephone and a computer to be integrated or coordinated. (2) The software that integrates voice communications systems with computers for contact center and office automation applications.
Computerized Physician Order Entry	CPOE	A clinical information system that enables a patient's care provider to enter an order for a medication, clinical laboratory or radiology test, or procedure directly into a computer.

Term	Acronym	Definition
Computing Services		Services that connect and virtualize computing resources based on the application. Examples: low-latency fabric (Ethernet or InfiniBand); high-throughput capabilities; linkage of Inter-Process Communication among multiple hosts, such as Remote Direct Memory Access (RDMA); and the tools to manage resource pools in a demand-driven environment, such as VFrame.
Continuity of Care Record	CCR	A snapshot of a patient's care that can be downloaded into a small, portable memory storage device and brought by a patient to various healthcare facilities. It frequently includes history of present illness, current medical conditions, past medical history, allergies, and medications.
Continuous Data Protection	CDP	A storage system in which all the data in an enterprise is backed up whenever any change is made.
Convergence		The consolidation of all communications, voice, data (Internet, ATM, Frame Relay, and so forth), and video (broadcast TV and video on demand) onto a single network infrastructure.
Core		The network backbone. The core typically interconnects multiple lower-speed networks. This usually involves high-speed connections and geographically long links.
Coverage		Agreed-upon set of health services that a plan will pay for and/or provide.
Current Procedural Technology	CPT	A set of codes developed by the American Medical Association that describes medical procedures for billing. Each item submitted by a provider to an insurance company for payment must be listed by code on the bill.
Dark Fiber/Unlit Fiber		Fiber-optic cables that are yet to be used. Hence, they are not yet connected to any device and have been installed only for future usage.
Data Encryption Standard	DES	A standard used to encrypt packet data. DES implements the mandatory 56-bit DES cipher block chaining (CBC). CBC requires an initialization vector to start encryption. The initialization vector is explicitly given in the IP Security (IPsec) packet.
Data Gateway		A node on a network that acts as an entrance to another network and often serves to translate between different communications.
Data Rates		The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).

Term	Acronym	Definition
Database		A collection of interrelated data items organized by a consistent scheme that allows data items to be processed without regard to physical storage locations. A collection of easily accessed data residing on a computer.
Day-Zero or Zero-Day Attacks		Day Zero (or Zero Day) is the day that a virus attacks or other security compromise occurs.
Deductible		The amount paid by a patient for medical care prior to insurance covering the balance.
Demilitarized Zone	DMZ	A middle ground between a trusted internal network and an untrusted external network (for example, the Internet). The DMZ is a subnetwork (subnet) that may sit between firewalls or off one leg of a firewall.
Denial-of-Service Attack/ Oversubscription	DOS	Attacks in which hackers deliberately overload connectivity pipes to bring the network router to a standstill using a Trojan horse command.
Dense Wavelength Division Multiplexing	DWDM	A technology that increases the information-carrying capacity of existing fiber-optic infrastructure by transmitting and receiving data on different light wavelengths. Many of these wavelengths can be combined on a single strand of fiber.
Device Redundancy		The ability to have a secondary peripheral device that takes over when the primary unit fails.
Diagnosis-Related Groups	DRGs	(1) A system of classifying patients on the basis of diagnoses for purposes of payment to hospitals. (2) A system for determining case mix, used for payment under Medicare's PPS and by some other payers.
Dialed Number Identification Service	DNIS	A string (usually four, seven, or 10 characters long) indicating the number dialed by a caller and how the call should be handled by the ACD, PBX, or VRU. ICM software uses the DNIS and trunk group to indicate the destination for a call.
Dictionary Attack		Weak passwords can be cracked using standard dictionaries found easily in various Internet discussion forums and Websites. The success of this type of attack depends on the variation in user passwords, the attacker's experience in generating dictionaries, and the strength of the password.
Digital Certificate		A digital ID issued by a digital certificate authority that serves as an electronic identification document. It includes user information, serial numbers, public key information, and expiration dates.
Digital Hospital		A hospital with enterprisewide IT.

Term	Acronym	Definition
Digital Imaging and Communications in Medicine	DICOM	A standard developed by the American College of Radiology Manufacturers Association to define the connectivity and communication protocols of medical imaging devices.
Direct Inward Dial	DID	A telephone number obtained from a service provider that is used to dial in to a telephone network.
Distributed Denial of Service	DDoS	A denial-of-service attack against a site or server launched from multiple sources. This sometimes is carried out by concealed, exploiting servers to function as agents for transmitting the attacks. A distributed denial-of-service attack is more effective than a simple denial-of-service attack because the volume of traffic is considerably higher and is more difficult to prevent.
DivX		A video that is used to compress lengthy video segments into small sizes while maintaining relatively high visual quality.
Document Imaging		The process of creating a computer file from a paper document. Scanners record the paper image and change it into an electronic image (.tiff or .gif file) that is viewed and transmitted by a computer. Computer images are routed, indexed, and filed into appropriate files or programs.
Domain		A user-created logical partition of networks or subnets.
Domain Naming System	DNS	A mechanism used on the Internet and on private intranets for translating names of host computers into addresses. The DNS also allows host computers not directly on the Internet to have registered names in the same style.
DownSpeeding		The act of renegotiating the connection speed or bandwidth between two endpoints or terminals anytime there is a complete loss of channel synchronization within one or more channels in the connection.
DuoVideo		A mechanism that provides endpoint support when transmitting more than one video channel, providing the ability to view either people or presentation content.
Dynamic Host Configuration Protocol	DHCP	A communications protocol that lets network administrators centrally manage and automate the assignment of IP addresses in an organization's network. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.
E.164		An ITU Telecommunication Standardization Sector (ITU-T) recommendation for international telecommunication numbering, especially in ISDN, BISDN, and SMDS. An evolution of standard telephone numbers.

Term	Acronym	Definition
Ear and Mouth	E&M	The E&M interface provides voice signals from radio channels, which are then mapped to IP multicast or Unicast. The E&M interface provides the most common form of analog trunking.
Easy Virtual Private Networks	Ez VPN	A client feature that is configured to create IPsec VPN tunnels between a supported router and another Cisco router that supports this form of IPsec encryption/decryption.
Echo Cancellation	ECAN	A technique used in high-speed modems and voice circuits to isolate and filter out unwanted signal energy caused by echoes from the main transmitted signal.
Ecosystem Partner		A system whose members benefit from each other's participation via symbiotic relationships.
Edge Services Router	ESR	A router that aggregates traffic from thousands of low- and medium-bandwidth subscriber connections and routes it on a few high-bandwidth connections to the Internet core.
Electronic Business Card	vCard	A standard format for an electronic business card that includes fields for a phone number, text name, and e-mail address of the message sender.
Electronic Data Interchange	EDI	A standardized electronic format for business transactions sent from one computer to another computer system. EDI consists of strings of data in a pre-arranged, accepted format by both sending and receiving computer systems.
Electronic Data Interchange for Administration, Commerce, and Transport	EDIFACT	An ISO standard for electronic data interchanges (EDI) that was proposed to supersede both X12 and TRADACOMS as the worldwide standard.
Electronic Data Interchange X12	EDI X12	The electronic communication of business transactions, such as orders, confirmations, and invoices, between organizations. Third parties provide EDI services that enable organizations with different equipment to connect. Although interactive access may be a part of it, EDI implies direct computer-to-computer transactions into vendors' databases and ordering systems. X12 is a protocol from the American National Standards Institute (ANSI) for electronic data interchange.
Electronic Mail	E-mail	A method of composing, sending, storing, and receiving messages over electronic communication systems.
Electronic Medical Record	EMR	Electronic patient records that encompass a patient's diagnosis, treatments, and history.
Electronic Number	ENUM	A DNS-based method for mapping phone numbers to IP addresses.

Term	Acronym	Definition
Electronic Prescribing	eRx	The use of computing devices to write and transmit electronic prescriptions bidirectionally (office-to-pharmacy, pharmacy-to-office). Providers can access patient-specific drug histories, create or renew prescriptions electronically, send prescriptions to the pharmacy via fax or EDI, and print prescriptions to paper.
Emergency Care		The immediate care that is necessary due to a condition, illness, or injury that is life-threatening or would significantly impair a patient's health.
Encounter Data		A description of services and diagnoses that occur when a patient visits a healthcare provider under a managed care plan.
Encryption		A software coding procedure intended to prevent hacking or illegal access. Encryption converts plain text into a disguised file or message using a mathematical algorithm.
Endpoint		An H.323 terminal or gateway. An endpoint can call and be called, and generates and/or terminates the information stream.
Endpoint Device		Any host attempting to connect or use the resource of a network; for example, a personal computer, personal digital assistant (PDA), data server, or other network-attached device.
Enhanced 911	E-911	A more reliable extension of the basic 911 emergency call standard.
Enhanced Interior Gateway Routing Protocol	EIGRP	A distance vector routing protocol with optimizations to minimize both the routing instability incurred after topology changes, as well as the use of bandwidth and processing power in the router. It provides convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.
Enterprise Architecture		Specific enterprise implementations and recommended designs for integrated data center, campus, WAN/MAN, edge, branch, and teleworker locations (also referred to as "places in the network") that incorporate Cisco and partner solutions, services, and best practices.
Ethernet		A physical and data-link-layer technology for LANs. When first widely deployed in the 1980s, Ethernet supported a maximum theoretical data rate of 10 Mbps. Later, Fast Ethernet standards increased this maximum data rate to 100 Mbps. Today, Gigabit Ethernet technology further extends peak performance up to 1000 Mbps.
Ethernet over MPLS	EoMPLS	This service allows Layer 2 Ethernet frames to be transported across an MPLS core network.

Term	Acronym	Definition
European Telecommunications Standards Institute	ETSI	An independent, nonprofit organization whose mission is to produce telecommunications standards for today and for the future.
Evaluation and Management Service	EM Service	A nonprocedural service, such as a visit or consultation, provided by physicians to diagnose and treat diseases and counsel patients.
Explanation of Benefits	EOB	The statement from an insurance plan that itemizes the actions taken on submitted claims.
Extended Care Facility		A nursing facility that provides post-hospital services that are reimbursable by Medicare.
Extended Service Area		The area of RF coverage provided by multiple access points in a wireless LAN configuration.
Extended Video Graphics Array	XVGA	A display standard with a maximum resolution of 1024 by 768 pixels.
Extensible Authentication Protocol	EAP	The protocol for the optional IEEE 802.1X wireless LAN security feature. An access point that supports 802.1X and EAP acts as the interface between a wireless client and an authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network.
Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling	EAP-FAST	An 802.1X authentication type that is available for use with Windows 2000 and XP. Support for EAP-FAST is provided in the client adapter's firmware and the Cisco software that supports it, rather than in the operating system. With EAP-FAST, a username, password, and PAC are used by the client adapter to perform mutual authentication with the RADIUS server through an access point.
Extensible Markup Language	XML	A standard maintained by the World Wide Web Consortium (W3C) that defines syntax to create markup languages to specify information structures. Information structures define the type of information (for example, subscriber name or address), not how the information looks (bold, italic, and so on). External processes can manipulate these information structures and publish them in a variety of formats.
Fabric Shortest Path First	FSPF	The protocol currently standardized by the T11 committee for routing in Fibre Channel networks. The standard path selection protocol used by Fibre Channel fabrics.
Failover		A backup operation that automatically switches to a standby database, server, or network if the primary system fails or is temporarily shut down for servicing. Failover is an important fault tolerance function of mission-critical systems that rely on constant accessibility.

Term	Acronym	Definition
Fault		An abnormal condition that occurs when a system component exceeds a performance threshold or is not functioning properly.
Fault Tolerant		The ability of a system to respond to an unexpected hardware or software failure.
Fibre Channel ID	FC_ID	An ID assigned to worldwide port names (pWWNs), regardless of switch restarts and physical port.
Fibre CONnection	FICON	A bidirectional channel protocol used to connect mainframes directly to FICON control units, FICON directors, or ESCON aggregation switches (ESCON Directors with a bridge card).
Fibre Channel		A gigabit-speed network technology primarily used for storage networking, standardized by ANSI. Despite its name, Fibre Channel signals can run on both twisted-pair copper wire and fiber-optic cables.
Fibre Channel over Internet Protocol	FCIP	A network storage technology that combines the features of Fibre Channel and the Internet Protocol (IP) to connect distributed storage area networks (SANS) over large distances.
File Transfer Protocol	FTP	An application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.
Firewall	FW	Hardware or software that controls traffic between different zones of trust within the network to prevent communications forbidden by the security policy.
Fluhrer, Mantin, and Shamir Attacks	FMS Attacks	FMS attacks on the network have been known to uncover the WEP key after capturing just 1 million packets (about 17 minutes on a busy network).
Foreign Exchange Office	FXO	A trunk type that connects a call center with a central office in a remote exchange. This allows callers in that remote exchange to access the call center directly without using an interexchange carrier.
Foreign Exchange Station	FXS	An interface connecting directly to a standard telephone and supplying ring, voltage, and dial tone.
Frame Relay	FR	Commonly deployed WAN infrastructure, especially in Frame-to-Frame and Frame-to-ATM deployments (where remote Frame Relay is a service interworked to the hub site ATM within the network). Each end user has a private or leased line to a Frame Relay node. The Frame Relay network handles the transmission over a frequently changing path that is transparent to all end users.
G.711		The 64-kbps PCM voice coding technique. In G.711, encoded voice is in the correct format for digital voice delivery in the PSTN or through PBXs.

Term	Acronym	Definition
G.722.1		An international standard wideband audio compression algorithm. It provides high-quality audio at low bit rates, with low delay and very low complexity.
G.726		Describes Adaptive Differential Pulse Code Modulation (ADPCM) coding at 40, 32, 24, and 16 kbps. ADPCM-encoded voice can be interchanged between packet voice, PSTN, and PBX networks if the PBX networks are configured to support ADPCM.
G.729		Describes Code Excited Linear Prediction (CELP) compression where voice is coded into 8-kbps streams. The two variations of this standard (G.729 and G.729 Annex A) differ mainly in computational complexity; both provide speech quality similar to 32-kbps ADPCM.
Gatekeeper	GK	An application performing essential control, administrative, and managerial functions required to maintain the integrity of networks in both enterprise and carrier environments.
Gateway	GW	A device that connects two otherwise incompatible networks.
Gateway Load Balancing Protocol	GLBP	Protects data traffic from a failed router or circuit with participating routers and switches replying to ARP requests in a round-robin fashion, thereby guaranteeing that both devices are used.
General Packet Radio Service	GPRS	An ETSI standard that defines the implementation of packet data services on a GSM network.
Generalists		Physicians who do not limit their practice by health condition or organ system. Typically, these include family practitioners, general internists, and general pediatricians.
Generic Routing Encapsulation	GRE	A Cisco-developed tunneling protocol that encapsulates a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single protocol backbone environment, IP tunneling using GRE allows network expansion across a single protocol backbone environment.
Gigabit Ethernet	GiGE	A technology that extends Ethernet peak performance up to 1000 Mbps.
Gigahertz	GHz	A unit of measure for frequency. One billion cycles per second.
Global Load-balancing Protocol		A feature by which client connections are globally distributed evenly among multiple listeners, dispatchers, instances, and nodes so that no single component is overloaded.

Term	Acronym	Definition
Global System for Mobil Communication	GSM	A second-generation mobile wireless networking standard that uses time division multiple access (TDMA). GSM is widely deployed throughout the world.
Gratuitous Address Resolution Protocol	GARP	A gratuitous ARP message tells devices on a local network to associate a mobile node's IP address with a home agent's data-link-layer address. Gratuitous means the message isn't sent in order to perform an actual address resolution, but rather to cause caches to be updated. It may be sent more than once to ensure that every device gets the message.
H.225		A protocol that describes how audio, video, data, and control information on a packet-based network can be managed to provide conversational services in H.323 equipment. H.225 has two major parts: call signaling and RAS (registration, admission, and status).
H.245		A protocol for the transmission of call management and control signals in packet-based networks using H.323 equipment. The H.245 specification is used in audio, video, and data transmissions, as well as in voice over IP (VoIP).
H.263		A video codec used to provide IP video.
H.263 Annex F		Advance prediction mode.
H.263 Annex J		Deblocking filter mode.
H.263 Annex N		Reference picture selection mode.
H.323		Subset of standards from the International Telecommunications Union that defines real-time multimedia communications for packet-based networks.
H.323 Annex M.1		Describes the tunneling of QSIG signaling in H.323 networks.
HCFA Common Procedure Coding System	HCPCS	A Medicare coding system based on the American Medical Association's Current Procedural Terminology (CPT), expanded to accommodate additional services covered by Medicare.
Health Care Finance Administration 1500s	HCFA 1500	A universal form, developed by the government agency known as the Health Care Financing Administration (HCFA), for providers of services to bill professional fees to health carriers.
Healthcare Provider		An individual or institution that provides medical services (for example, a physician, hospital, or laboratory).
Health Information Exchange	HIE	The concept of an interoperable, secure health data exchange.
Health Insurance		Coverage that provides for the payments of benefits as a result of sickness or injury. This includes insurance for losses from accident, medical expense, disability, or accidental death and dismemberment.

Term	Acronym	Definition
Health Insurance Portability and Accountability Act of 1996	HIPAA	The Health Insurance Portability and Accountability Act is a set of security regulations that are a cornerstone in standards for the healthcare industry. Its main goals are 1) to improve healthcare by lowering costs while ensuring availability and 2) to protect the privacy of patient data by guaranteeing the safety of Electronic Protected Health Information (ePHI) and Individually Identifiable Health Information (IIHI). HIPAA was enacted on August 21, 1996 and its date of final implementation passed on April 20, 2005.
Health Level 7	HL7	ANSI-accredited standards for electronically defining clinical and administrative data in the healthcare industry. HL7 is one of several standards-development organizations in healthcare. It refers to application layer 7 in the OSI model, which is the highest level where programs talk to each other.
High Availability		High availability addresses congestion elimination, as well as single point of failure, by deploying redundant networks and data centers.
Host Bus Adapter	HBA	A part in an external network that constitutes the interface between the network itself and the PCI bus of the compute node.
Hot Standby Routing Protocol	HSRP	Provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from failures in network edge devices or access circuits.
Hypertext Markup Language	HTML	A simple hypertext document formatting language that uses tags to indicate how a given part of a document should be interpreted by a viewing application, such as a Web browser.
Hypertext Transfer Protocol	HTTP	A protocol used by browsers and Web servers to transfer files. Via HTTP, the browser can request and receive the files used by a Web page. HTTP transmissions are not encrypted.
Identity Services		Identity Services map resources and policies to the user and device, determine the identity of a user or device, grant access privileges, and enforce policy that governs interaction with applications. Examples: authentication and authorization services (RADIUS servers), NACv2 support, 802.1x capabilities, network-based application recognition (NBAR), and NetFlow are key identity services provided by the network that work with Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP).

Term	Acronym	Definition
Individual Practice Association	IPA	Networks of independent physicians that contract with MCOs and employers. IPAs may be organized as sole proprietorships, partnerships, or professional corporations.
InfiniBand		A high-performance, multipurpose network architecture based on a switched fabric. It is designed for use in I/O networks, such as storage area networks (SANs), or in cluster networks. InfiniBand supports network bandwidth between 2.5 Gbps and 30 Gbps.
Infrastructure		The wired Ethernet network.
Infrastructure Services Virtualization		Provides application flexibility, responsiveness, and compliancy by enabling networking services to handle loosely coupled resources as logical entities in an integrated network environment. Supports dynamic allocation of services functions, distributed capabilities, and centralized policy management of services.
Input		The labor, capital, and other resources hospitals use to produce goods and services.
Instant Messaging	IM	A service that allows online conversations to occur in real time.
Instrument Tracking		The inventory and maintenance of surgical instruments.
Integrated Delivery System	IDS	An entity that usually includes a hospital, a large medical group, and an insurance vehicle, such as an HMO or PPO. Typically, all provider revenues flow through the organization.
Integrated Dictation and Transcription	IDT	Technologies that help simplify the production and management of electronic patient information by capturing clinician diagnoses related to patient care and then translating these recordings into a format for integration into a patient's medical records.
Integrated Multiprotocol	IMP	A protocol that promotes centralization and SAN consolidation by allowing for multiple storage protocols (Fibre Channel, Small Computer System Interface over IP [iSCSI], Fibre Channel over IP [FCIP], and IBM Fiber Connection [FICON]) to run concurrently within the same platform without the need for any additional appliances or additional management software. This capability allows for centralized management of all protocols within a single management platform.
Integrated Services Digital Network	ISDN	A set of protocols for establishing and breaking circuit-switched connections and for advanced call features for the end user. Extensively used outside the United States.
Integrated Services Router	ISR	A router featuring conventional routing, firewalling, PoE switching, embedded VoIP call management, and voicemail.

Term	Acronym	Definition
Intelligent Contact Management	ICM	A Cisco system that implements enterprisewide call distribution across call centers. ICM software provides pre- and post-routing, along with performance-monitoring capabilities.
Intelligent Information Network	IIN	A strategy that addresses the evolving role of the network within a business and works to align IT resources with business priorities.
Inter-Access Point Protocol	IAPP	A Cisco proprietary protocol defined to support roaming. IAPP, however, does not address how the wireless system tracks users moving from one subnet to another.
Interactive Services Layer		Enables efficient allocation of resources to upper-layer applications and business processes delivered through the networked infrastructure. Cisco integrates a complete suite of services into intelligent systems that optimize business and collaboration applications for more predictable and reliable performance with lower operational costs.
Interactive Voice Response	IVR	A telecommunications computer that responds to caller-entered touch-tone digits. The IVR responds to caller-entered digits in much the same way a conventional computer responds to keystrokes or a mouse click. The IVR uses a digitized voice to read menu selections to the caller. The caller then enters the touch-tone digits that correspond to the desired menu selection. The caller-entered digits invoke options as varied as looking up account balances, moving the call within or to another ACD, or playing a pre-recorded announcement for the caller.
Interexchange Carrier	IXC	A long-distance telephone company.
Interface		(1) A network connection. (2) A connection between two systems or devices.
Interflow		The ability of a switch to forward calls to another location within the switch or to another switch. Interflow between switches requires a dedicated trunk line.
Interior Gateway Protocol	IGP	A protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include IGRP, OSPF, and RIP.
Interior Gateway Routing Protocol	IGRP	A protocol developed by Cisco to address the issues associated with routing in large, heterogeneous networks.

Term	Acronym	Definition
Intermediate Distribution Frame	IDF	A frame that cross-connects the user cable media to individual user line circuits. May serve as a distribution point for multi-pair cables from the main distribution frame (MDF) or combined distribution frame (CDF) to individual cables connected to equipment in areas remote from these frames.
International Classification of Diseases, 9th Revision	ICD-9	A listing of diagnoses and codes that are used by physicians to report on health plan enrollees. The coding and terminology provide a uniform language that can accurately designate primary and secondary diagnoses and provide reliable, consistent communication on claim forms.
International Telecommunications Union	ITU	An organization established by the United Nations to set international telecommunications standards and allocate frequencies for specific uses.
Internet Control Message Protocol	ICMP	A TCP/IP protocol used to send error and control messages. For example, a router uses ICMP to notify the sender that its destination mode is not available. A ping utility sends ICMP echo requests to verify the existence of an IP address.
Internet Engineering Task Force	IETF	The primary standards organization for the Internet. It is a large, open, international community of network designers, operators, vendors, and researchers concerned with identifying problems and opportunities in IP data networks and proposing technical solutions to the Internet community.
Internet Information Server	IIS	Microsoft's Web server that runs under Windows.
Internet Key Exchange	IKE	A method for establishing a security association that authenticates users, negotiates the encryption method, and exchanges a secret key.
Internet Operating System	IOS	The Cisco system software that allows centralized, integrated, and automated installation and management of internetworks while providing support for a variety of protocols, media, services, and platforms.
Internet Protocol	IP	A network layer protocol in the TCP/IP stack that offers a connectionless internetwork service. IP provides features for addressing, type of service specification, fragmentation and reassembly, and security.
Internet Protocol Contact Center	IPCC	A Cisco solution for VoIP-enabled call centers. This service is for enterprises wishing to reduce cost, optimize revenue per call, and increase overall customer satisfaction in call center environments.

Term	Acronym	Definition
Internet Protocol Security	IPsec	A set of protocols developed to support secure exchange of packets at the IP layer. IPsec is widely deployed to implement virtual private networks (VPNs).
Internet Service Node	ISN	A switch that allows calls to be routed and transferred through an IP network under complete customer control. ISN components can be deployed at the edge of an IP network, providing local IVR, queuing, and switching services without consuming expensive bandwidth on a core IP backbone. The Cisco ISN enables calls to be offloaded from traditional telephony networks to an IP environment, reducing toll-free phone costs.
Internet Small Computer System Interface	iSCSI	An IP-based standard for linking data storage devices over a network and transferring data by carrying SCSI commands over IP networks. SCSI is a parallel interface standard used by Apple Macintosh computers, PCs, and many UNIX systems for attaching peripheral devices to computers.
Internet/Portal		A framework for integrating information, applications, and processes across organizational boundaries.
Internet Protocol Device Control	IPDC	A specification for controlling hardware devices. It provides management and system integration between switches.
Internetwork Performance Monitor	IPM	A Cisco workstation-based network management product that provides data about response times between devices.
Interoperability		The ability of different information technology systems and software applications to communicate; to exchange data accurately, effectively, and consistently; and to use the information that has been exchanged.
Inter-Process Communication	IPC	A capability that allows one process to communicate with another. The processes can be running on the same computer or on different computers connected through a network. IPC enables one application to control another application and for several applications to share the same data without interfering with one another.
Inter-switch Link	ISL	The use of an external, or two-level, packet tagging scheme to multiplex VLANs across a single physical link while maintaining strict adherence to the individual VLAN domains. With ISL, all packets must be tagged on a physical link.

Term	Acronym	Definition
Inter-VSAN Routing	IVR	A routing capability allowing Fibre Channel resources across different virtual SANs (VSANs) to be zoned together without compromising other VSAN benefits. Resources are easily shared across VSANs without merging the virtual fabrics.
Intrusion Detection System	IDS	A system that provides security across a distributed network.
Intrusion Prevention System	IPS	Cisco IOS software's deep packet inspection-based solution that helps mitigate a wide range of network attacks without compromising router performance in branch installations. While it is common practice to defend against attacks by inspecting traffic and installing firewalls, Cisco IOS IPS at the branch enables gateways to drop traffic, send an alarm, or reset the connection as needed to stop attacking traffic at the point of origination and remove unwanted traffic from the network.
IP Access Control Lists	IP ACL	A list that is used to control the transmissions of packets on an Ethernet interface whether it is an interface to manage a switch, or Fibre Channel over IP (FCIP), or small computer system over IP (iSCSI) communication. IP ACLs restrict IP-related traffic based on configured IP filters.
IP Address		The Internet Protocol (IP) address of a station.
IP Multicasting	IPmc	IP Multicasting allows a source to send a single packet into the IP network and have it duplicated and sent to many listeners by the other routers within the network
IP over Fibre Channel	IPFC	An Internet Protocol-based storage networking technology developed by the Internet Engineering Task Force (IETF). IPFC mechanisms enable the transmission of Fibre Channel information by tunneling data between storage area network (SAN) facilities over IP networks. This capacity facilitates data sharing over a geographically distributed enterprise. One of two main approaches to storage data transmission over IP networks, IPFC is among the key technologies expected to help bring about rapid development of the storage area network market by increasing the capabilities and performance of storage data.
IP Subnet Mask		The number used to identify the IP subnetwork, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway. This number is expressed in a form similar to an IP address, as in 255.255.255.0.
Java Telephony Application Programming Interface	JTAPI	An extensible API that supports telephony call control. It is designed to scale for use in a range of domains, from first-party call control in a consumer device to third-party call control in large, distributed call centers.

Term	Acronym	Definition
Jitter		A variation in timing, or time of arrival, of a received signal.
Jitter Control		Healthcare networks must provide secure, predictable, and measurable service. MGN QoS features manage delay variation (jitter) by appropriately addressing and prioritizing voice and video packets.
kbps		Kilobits per second (thousands of bits per second). A measure of bandwidth on a data transmission medium.
Laboratory Information System	LIS	The laboratory software that receives orders, manages lab test data throughout the processing cycle, and generates and distributes result reports. An LIS also may be used to place orders to, and receive result reports from, other labs.
Latency		The time information takes to move across a network. For voice networks, latency is the delay from when a word is spoken to the time it is heard by the listener. Low latency is usually highly desirable for real-time applications, such as voice and video.
Layer 2		The Ethernet layer of the Open Systems Interconnection (OSI) model, which defines internetworking in terms of a vertical stack of seven layers. The upper layers of the OSI model represent software that implements network services, such as encryption and connection management. The lower layers of the OSI model implement more primitive, hardware-oriented functions like routing, addressing, and flow control.
Layer 2 Tunneling Protocol version 3	L2TPv3	Extends the usability of IP networks by enabling the transport of Layer 2 frames over an IP infrastructure. L2TPv3 is required for supporting legacy services over IP infrastructures and for supporting several new connectivity options, including Layer 2 VPNs and Layer 2 virtual leased lines.
Layer 3		The Internet protocol network layer of the OSI model.
LEAP		An 802.1x authentication type for WLANs that supports strong mutual authentication between the client and a RADIUS server using a logon password as the shared secret. It provides dynamic per-user, per-session encryption keys.
Legacy System		An older software system based on mainframe computer or older programming languages.
Lifetime Maximum		The total amount an insurance policy will pay for medical care during the lifetime of the insured person.
Lightweight Access Point Protocol	LWAPP	The control and data tunneling protocol between access points and wireless LAN controllers.

Term	Acronym	Definition
Lightweight Directory Access Protocol	LDAP	A software protocol for enabling anyone to locate organizations, individuals, and other resources, such as files and devices, in a network, whether on the Internet or on a corporate intranet. LDAP is a lightweight (smaller amount of code) version of the Directory Access Protocol, which is part of X.500, a standard for directory services in a network.
Link Layer Discovery Protocol	LLDP	Derived from Cisco Discovery Protocol, LLDP provides some of the capabilities offered by Cisco Discovery Protocol. Through the LLDP encoding mechanism, called Type Length Value, all the features of both Cisco Discovery Protocol and standard LLDP are available to Cisco users.
Load Balancing		The capability of a router to distribute traffic over all its network ports that are the same distance from the destination address. Good load-balancing algorithms use both line speed and reliability information. Load balancing increases the use of network segments, thus increasing effective network bandwidth.
Logical Unit Number	LUN	A small computer system interface identifier within a target is assigned to each Fibre Channel- accessible disk so that the host can address and access the data on those devices.
MAC Address		A standardized data-link-layer address that is required for each port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are six bytes long and are controlled by the IEEE. Also known as a hardware address, MAC-layer address, or physical address.
Magnetic Resource Imaging	MRI	A method of creating images of the inside of opaque organs in living organisms as well as detecting the amount of bound water in geological structures. It is a commonly used form of medical imaging.
Main Distribution Frame	MDF	A termination point within a local exchange. All exchange equipment and any terminations to the local loop appear at the MDF.
Malware		A program designed to infiltrate or damage a computer system.
Mammography		The process of using low dose X-rays to examine the human breast. It is used to look for different types of tumors and cysts.

Term	Acronym	Definition
Managed Care		(1) An integrated system of health insurance, financing, and service delivery functions involving risk sharing for the delivery of health services and defined networks of providers. (2) Any system of health payment or delivery arrangements where the health plan attempts to control or coordinate use of health services by its enrolled members in order to contain health expenditures, improve quality, or both. Arrangements often involve a defined delivery system of providers with some form of contractual arrangement with the plan. (3) Approaches to health services delivery and benefit design that integrate management and coordination of services with financing to influence usage, cost, quality, and outcomes.
Managed Care Organization	MCO	Integration (to varying degrees) of the financing and delivery of healthcare services.
Management Information Base	MIB	A database of network management information that is used and maintained by a network management protocol, such as SNMP or CMIP. The value of an MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.
Man-in-the-middle Attack		A hacker attack that takes place when the attacker inserts himself in the middle of an authentication sequence and attempts to obtain security credentials or a security key by intercepting credentials.
Material Management		The analysis and management of medical equipment, which focuses on cost-effective purchases, supply usage, equipment, and resources.
Maximum Allowable Cost, or Charge		This term often is used in pharmaceutical contracting and refers to the maximum that a vendor may charge for something.
Media Access Control	MAC	A unique 48-bit number used in Ethernet data packets to identify an Ethernet device, such as an access point or a client adapter.
Media Gateway Control Protocol	MGCP	A protocol that helps bridge the gap between circuit-switched and IP networks. A combination of Internet Protocol Device Control (IPDC) and Simple Gateway Control Protocol (SGCP). MGCP allows external control and management of data communications devices or media gateways at the edge of multiservice packet networks by software programs.

Term	Acronym	Definition
Media Gateway Controller	MGP	A device that provides control of media and signaling gateways.
Medical-Grade Network	MGN	An information framework defined to meet key technology requirements for the healthcare industry. The MGN defines network strategies and policies using an industry-specific framework. It maps clinical and business needs to technology solutions.
Medical Technology		Includes drugs, devices, techniques, and procedures used in delivering medical care and the support systems for that care.
Message Handling		The lower-level protocols that transfer data over a network that assembles and disassembles the data into the appropriate codes for transmission.
Message Integrity Check	MIC	An implementation that prevents attacks on encrypted packets. MIC, implemented on both the access point and all associated client devices, adds bytes to each packet to make the packets tamperproof.
Message Waiting Indicator	MWI	A phone system device (lamp, distinctive dial tone, or LCD display) that alerts a subscriber to the arrival of new messages.
Metropolitan Area Network	MAN	A network that covers an area larger than a LAN, usually a metropolitan area. MANs exist between, and interconnect, the long-haul and access segments of the global network.
Microsoft Media Streaming	MMS	A sequence of moving images that are sent in compressed form over the Internet and displayed by the viewer as they arrive. Streaming media is streaming video with sound. With streaming video or streaming media, a Web user does not have to wait to download a large file before seeing the video or hearing the sound. Instead, the media is sent in a continuous stream and is played as it arrives.
Microwave Networks		Microwaves are electromagnetic waves with wavelengths longer than those of infrared light but shorter than those of radio waves. The IEEE 802.11g and b specifications use microwaves in the 2.4-GHz ISM band, although 802.11a uses an ISM band in the 5-GHz range. Licensed long-range (up to about 25 km) wireless Internet access services can be found in many countries (but not the U.S.) in the 3.5- to 4.0-GHz range.
Mobile IP	MoIP	Mobile IP is an open standard, defined by the IETF, which allows users to keep the same IP address, stay connected, and maintain ongoing applications while roaming between IP networks. Mobile IP is scalable for the Internet because it is based on IP. Any media that can support IP can support Mobile IP.

Term	Acronym	Definition
Mobility Services		Services that allow users to access network resources, regardless of their physical location. Examples: location-based services with RFID for asset tracking and tagging, E911 and 802.11 voice routing, 802.11 mesh networks, classic VPN, and guest access to technology.
Monitoring		The collection, transmission, and interpretation of patient data.
Monitoring, Analysis, and Response System	MARS	A Cisco system that recognizes and correlates network attacks and defines how to stop them.
Motion JPEG	MJPEG	A video codec where each video field is separately compressed into a JPEG image.
Multiprotocol Label Switching	MPLS	A switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on pre-established IP routing information.
Multicast		A routing technique that allows IP traffic to be sent from one or multiple sources and delivered to multiple destinations. Instead of sending individual packets to each destination, a single packet is sent to a group of destinations known as a multicast group, which is identified by a single IP destination group address. Multicast addressing supports the transmission of a single IP datagram to multiple hosts.
Multicast Packet		A single data message (packet) sent to multiple addresses.
Multicast Routing Monitor	MRM	A management diagnostic tool that provides network fault detection and isolation in a large multicast routing infrastructure. It is designed to notify a network administrator of multicast routing problems in near real time.
Multiple Broadcast SSID	MBSSID	An access point that appears to be several distinct, co-located access points. It transmits a beacon for each broadcast SSID, allowing all of the SSIDs to be visible for passive scanning.
Multiple Spanning Tree		An advanced network protocol and algorithm that provides a loop-free topology for any LAN or bridged network.
Multipoint Control Unit	MCU	An H.323 endpoint that provides the capability for three or more terminals and gateways to participate in multipoint conferences.
Multiprotocol Extensions for Border Gateway Protocol	MP-BGP	Capabilities are added to BGP to enable multicast or other routing policies throughout the Internet.

Term	Acronym	Definition
Multiprotocol Label Switching VPN	MPLS VPN	An emerging technology with healthcare organizations, largely due to its segmentation capabilities and cost effectiveness. It provides high-performance switching for networks with existing native IP or ATM architectures or a mixture of other Layer-2 technologies. A chief advantage of MPLS is that it provides the scalability to support both small and large VPN deployments—up to tens of thousands of VPNs on the same network core. Other benefits include end-to-end QoS, rapid fault correction of link and node failure, bandwidth protection, and a foundation for deploying value-added services.
Multipurpose Internet Mail Extensions	MIME	An industry-standard specification for formatting non-ASCII messages so they can be sent over the Internet. Many e-mail clients now support MIME, which enables them to send and receive graphics, audio, and video files via the Internet mail system.
Music on Hold	MOH	The ability to provide real-time or recorded sound to callers while they are on hold. MOH can be provided from an audio file or from a live feed from an external source.
National Council for Prescription Drug Programs	NCPDP	An ANSI-accredited group that maintains a number of standard formats for use by the retail pharmacy industry, some of which are included in the HIPAA mandates.
National Health Information Network	NHIN	(1) An initiative to develop an architecture and network for secure information sharing among healthcare providers. This effort will ensure that information can be exchanged seamlessly between regional healthcare markets, thus establishing an infrastructure for the sharing of electronic health information and enabling each U.S. citizen to establish a personal health record. (2) A network promoting the seamless movement of secure healthcare data.
NetFlow		A technology that provides the metering base for a set of applications, including network traffic accounting, usage-based network billing, network planning, network monitoring, outbound marketing, and data-mining capabilities for both service provider and enterprise customers. Cisco provides a set of NetFlow applications to collect NetFlow export data, perform data volume reduction and post-processing, and provide end-user applications with access to this data.
Network		A group of physicians, hospitals, and other healthcare providers working with a health plan to offer care at negotiated rates.

Term	Acronym	Definition
Network Access Device	NAD	A device that enforces network access control privileges by controlling which endpoint devices have access to network destinations and services reachable through that NAD.
Network Address Translation	NAT	Allows IP networks to maintain public IP addresses separately from private IP addresses. NAT is a popular technology for Internet connection sharing. It also sometimes is used in server load-balancing applications on corporate networks.
Network Address Translator	NAT	See Network Address Translation.
Network Admission Control	NAC	Performs posture validation at the Layer 2 network edge for hosts with or without 802.1x enabled. Vulnerable and noncompliant hosts can be isolated, given reduced network access, or directed to remediation servers based on organizational policy. By deploying the NAC Framework on Cisco Catalyst switches, users can restrict noncompliant endpoints that may be vulnerable or infected with worms, viruses, or spyware before they have a chance to enter the LAN.
Network Entity Title	NET	A network service access point where the last byte is always zero.
Network File System	NFS	A client/server application that lets a user view, optionally store, and update files on a remote computer as though they were on his or her own computer.
Network Infrastructure Virtualization		A common technology employed in many of the interactive services supported across the networked infrastructure, virtualization has the ability to make many resources look like one (or one to look like many) and to deal with resources on a logical, rather than physical, basis.
Network Infrastructure Virtualization		Improves the convergence, usability, and flexibility of network infrastructure components and functions. It is available through network infrastructure capabilities, such as routing, switching, and basic network fabric functions.
Network-based Application Recognition	NBAR	A classification engine that recognizes and classifies a wide variety of protocols and applications.
Networked Infrastructure Layer		The network foundation on which all IT resources are interconnected. Includes servers, storage devices, and clients (users or devices, such as routers and switches) interconnected across distributed places in the network (such as campus, branch, and data center). Validated Cisco Enterprise Architectures for these places in the network provide complete design guidance for a fully integrated, end-to-end system across the customer's enterprise.

Term	Acronym	Definition
Node		A device on a network with its own unique network address and name.
Non-stop Forwarding	NSF	NSF enables routers continuously to forward IP packets following a route processor takeover or switchover to another route processor. NSF maintains and updates Layer 3 routing and forwarding information in the backup route processor.
Nurse Call		Solutions increasingly mandated by hospitals to provide automated patient call routing and forwarding, code blue reporting, and patient transfer, so that patients can have immediate contact with a nurse at all times.
Nursing Facility		An institution that provides skilled nursing care and rehabilitation services to injured, functionally disabled, or sick persons.
Open Shortest Path First	OSPF	A link state, hierarchical Interior IGP routing protocol. The well-known Dijkstra's algorithm is used to calculate the shortest path tree. It uses cost as its routing metric. OSPF is, perhaps, the most widely used IGP in large networks.
Open Systems Interconnection Model	OSI Model	The OSI model defines internetworking in terms of a vertical stack of seven layers. The upper layers of the OSI model represent software that implements network services like encryption and connection management. The lower layers of the OSI model implement more infrastructure-oriented functions, such as routing, addressing, and flow control. IP corresponds to the network layer, Layer 3. TCP and UDP correspond to OSI model Layer 4, the Transport layer. Lower layers of the OSI model are represented by technologies such as Ethernet. Higher layers of the OSI model are represented by application protocols, such as TCP and UDP.
Optimized Edge Routing	OER	Cisco's intelligent network traffic load distribution and dynamic failure detection of data paths at the WAN edge (multi-homing to the Internet or intranet connectivity).
Out of Area		Beyond or outside the geographical area served by a network plan.
Outcome		The consequence of medical intervention on behalf of a patient.
Out of Plan Services		The services furnished to patients by providers who are not members of the patient's managed care network.
Out-of-Pocket Costs		The health expenses that a patient must pay, including deductibles, co-payments, and charges not covered by a health plan.
Packet		A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error-detection information.

Term	Acronym	Definition
Packet Over SONET	POS	A high-speed means of transmitting data over a SONET fiber-optic transmission system through a direct fiber connection to a data switch or router. POS is a point-to-point dedicated leased line approach intended purely for high-speed data applications. POS allows a user organization to pass data in its native format, without the addition of any significant level of overhead in the form of signaling and control information.
Participating Provider		A physician who signs a contract with a PPO and agrees to accept the plan's allowable charges.
Passive Attack		An attack that involves an unauthorized user gaining access to the network but not modifying any network resources.
Patient Tracking		An application that delivers an information exchange used to provide patient care as a patient enters admission through discharge.
Pay for Performance	P4P	A strategy being used to increase and drive innovation and technology adoption in healthcare delivery systems.
Payer		A person or organization responsible for paying the amount stated on the face of a negotiable instrument.
Private Branch Exchange	PBX	A private phone switch that serves a particular business or organization.
Peer-to-Peer	P2P	A computer network that relies primarily on the computing power and bandwidth of the participants in the network rather than concentrating it in a relatively low number of servers.
Performance Measure		A specific measure of how well a health plan does in providing health services to its enrolled population.
Protocol Independent Multicast-Sparse Mode	PIM-SM	One of the two PIM operational modes. PIM sparse mode tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the rendezvous point. In sparse mode, receivers are widely distributed and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them.
Personal Health Record	PHR	A portable device or service that holds digital health data. It allows different physicians to view patient data, as well as to make additions.
Per-VLAN Spanning Tree	PVST	In Ethernet switched environments where multiple VLANs exist, spanning tree can be deployed per VLAN. Cisco refers to this as Per VLAN Spanning Tree (PVST and PVST+ are the default protocols used by Cisco switches).

Term	Acronym	Definition
Pharmacy Benefit Management	PBM	A company under contract with managed care organizations, self-insured companies, government programs for pharmacy network management, drug utilization review, outcomes management, and disease management.
Physician/Hospital Organization	PHO	(1) A structure in which a hospital and physicians (both in individual and group practices) negotiate as an entity directly with insurers. (2) An organization that contracts with payers on behalf of one or more hospitals and affiliated physicians.
Picture Archiving and Communication System	PACS	Networks or standalone systems dedicated to the storage, retrieval, distribution, and presentation of images. Full PACS handle images from various modalities, such as ultrasonography, magnetic resonance imaging, positron emission tomography, computer tomography, and radiography (plain X-rays).
Ping of Death		A hacker attack that involves sending IP packets of an illegal size (greater than 65,535 bytes) to the target system.
Plain Old Telephone Service	POTS	A basic telephone service supplying standard single-line telephones, telephone lines, and access to the public switched telephone network (PSTN).
Point-to-Multipoint	P2MP	Communication between a series of receivers and transmitters to a central location. Cisco P2MP typically is set up in three segments to enable frequency re-use.
Point-to-Point	P2P	Communication between one receiver and one location. With less overhead to manage the data paths, and only one receiver per transmitter, P2P has a higher bandwidth than P2MP.
Port		(1) An interface on an internetworking device (such as a router); a physical entity. (2) In IP terminology, an upper-layer process that receives information from lower layers. Ports are numbered and each numbered port is associated with a specific process.
Port Access Control List	PACL	An access list that is mapped to a physical port. This list provides extra granularity to filter traffic on a specific physical port.
Positron Emission Tomography	PET	A nuclear medicine medical imaging technique that produces a three-dimensional image or map of functional processes in the body.
Post Office Protocol	POP	A protocol that client e-mail applications use to retrieve mail from a mail server.
Posture Agent		The host agent software that serves as a broker on the host for aggregating credentials from potentially multiple posture plug-ins and communicating with the network.

Term	Acronym	Definition
Posture Credentials		The credentials that describe the state of an application and/or operating system that is running on an endpoint device at the time a Layer 2 or Layer 3 challenge response is issued by a NAD.
Power over Ethernet	PoE	The 48-volt DC power provided over standard Ethernet unshielded twisted-pair cable. Instead of using wall power, IP phones and other inline-powered devices can receive power provided by inline-power-capable Ethernet switches or other inline power source equipment (PSE).
Pre-authorization		An approval from an insurance plan that must be obtained before specialty services are provided or the service will not be reimbursed.
Preferred Provider Organization	PPO	A managed care plan in which a group of providers contracts with an insurer and agrees to provide services at pre-negotiated fees. Members are given incentives to use providers within the organization but may use providers outside the plan and pay greater out-of pocket costs.
Premium		The charge (not including any required deductibles or co-payments) paid to the insurer for health coverage. This may be paid weekly, monthly, quarterly, or annually.
Presence		A Cisco server that collects information about a user's availability status and communications capabilities.
Preventive Care		Medical services that try to reduce the chances of illness, injury, or other conditions. This contrasts with acute care, which is given after the condition has occurred.
Primary Care		Routine medical care usually provided in a doctor's office or clinic.
Primary Care Provider		A healthcare professional capable of providing a wide variety of basic health services. Primary care providers include practitioners of family, general, or internal medicine; pediatricians and obstetricians; nurse practitioners; midwives; and physician's assistants in general or family practice.
Primary Rate Interface	PRI	An ISDN interface to primary rate access. Primary rate access consists of a single, 64-kbps D channel plus 23 T1 or 30 E1 B channels for voice or data.
Private Virtual Local Access Network	PVLAN	A group of devices on one or more private LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire when, in fact, they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

Term	Acronym	Definition
Proactive Key Caching	PKC	Cisco's extension to the 802.11i standard and precursor to the 802.11r standard that facilitates secure roaming with AES encryption and RADIUS authentication.
Protected Extensible Authentication Protocol	PEAP	A method of securely transmitting authentication information, including passwords, over wireless networks. It was developed jointly by Microsoft, RSA Security, and Cisco. It is an IETF open standard.
Protocol Data Unit	PDU	A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error-detection information.
Protocol Independent Multicast	PIM	A multicast routing architecture defined by the IETF that enables IP multicast routing on existing IP networks. Its key point is its independence from any underlying unicast protocol, such as OSPF or BGP.
Provider		A hospital, skilled nursing facility, outpatient surgical facility, physician, practitioner, or other individual or organization that is licensed to provide medical or surgical services, therapy, or treatment.
Proxy		An entity that, in the interest of efficiency, essentially stands in for another entity.
Public Key Infrastructure	PKI	A system of digital certificates, certificate authorities, and other registration authorities that verifies and authenticates the validity of each party involved in an Internet transaction.
Public Switched Telephone Network	PSTN	A general term referring to the variety of telephone networks and services in place worldwide.
Pulse Code modulation	PCM	A form of modulation in which information signals are sampled at regular intervals and a series of pulses in coded form is transmitted representing the amplitude of the information signal at that time.
Q Signaling	QSIG	An ISDN-based protocol developed for networking different enterprise switching systems together and providing additional supplementary services for feature transparency.
Quality of Service	QoS	The ability of the network to provide better service to select network traffic over various network technologies. QoS allows network managers to establish service-level agreements (SLAs) with network users, enables network resources to be shared more efficiently, expedites the handling of mission-critical applications, and prioritizes time- sensitive multimedia and voice application traffic. With QoS, bandwidth can be managed more efficiently across LANs and WANs.

Term	Acronym	Definition
Quality Assurance	QA	A formal, systematic process to improve quality of care that includes monitoring quality, identifying inadequacies in delivery of care, and correcting those inadequacies.
Radiation Oncology		A series of treatments—including specialized technologies—related to cancer.
Radio Frequency Identification	RFID	A technology that uses radio frequency waves to transfer data between a movable item and reader to identify, track, or locate that item.
Radiology Information System	RIS	A system that supports the medical and administrative functions of a radiology department; computerized systems for tracking patients and the diagnostic imaging (DI) procedures they receive, along with scheduling, reporting, and billing.
Rapid Spanning Tree Protocol	RSTP	In 1998, the IEEE introduced an evolution of the Spanning Tree Protocol: Rapid Spanning Tree Protocol (RSTP), or 802.1w. In the 2004 edition of 802.1D, Spanning Tree Protocol is superseded by Rapid Spanning Tree Protocol (RSTP).
Real Time Streaming Protocol	RTSP	A protocol enabling the controlled delivery of real-time data, such as audio and video. RTSP is designed to work with established protocols, such as RTP and HTTP.
Real Time Transfer Protocol/RTP Control Protocol	RTP/RTCP	It is defined in RFC 3550 (which obsoletes RFC 1889). RTCP provides out-of-band control information for an RTP flow. It partners RTP in the delivery and packaging of multimedia data, but does not transport any data itself. It is used periodically to transmit control packets to participants in a streaming multimedia session. The primary function of RTCP is to provide feedback on the quality of service being provided by RTP.
Real Time Transport Protocol	RTP	An IPv6 protocol designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over Multicast or Unicast network services. RTP provides services such as payload type identification, sequence numbering, time stamping, and delivery monitoring to real-time applications.
Record Locator Service	RLS	A service that holds information authorized by the patient about where authorized information can be found, but not the actual information the records may contain.
Redundancy		The characteristic of having a secondary peripheral computer system or network device that takes over if the primary unit fails.

Term	Acronym	Definition
Redundant Array of Inexpensive Disks	RAID	A storage device that provides fault tolerance through redundant physical disks. A RAID system is an alternative to mirrored disks.
Referral		A formal process by which a patient is authorized to receive care from a specialist, therapist, or hospital.
Reflexive Access Control List	RACL	A list that contains condition statements (entries) that define criteria for permitting IP packets. These entries are evaluated in order and, when a match occurs, no more entries are evaluated.
Regional Health Information Network	RHIN	An Internet-based, privacy-protected, secure network where health information is shared.
Regional Health Information Organization	RHIO	An organization made up of regional hospitals that share information and resources. RHIOs, in turn, form the foundation of the National Health Information Network (NHIN).
Registration, Admission, and Status		Registration, admission, and status is a management protocol between endpoints. RAS is used for registration, admission controls, and status between devices and gatekeepers.
Remote Authentication Dial In User Service	RADIUS	The industry-accepted standard protocol for authentication servers (AAA servers). RADIUS uses a challenge and response method for authentication purposes. It is commonly used for embedded network devices such as routers, modem servers, and switches.
Remote Direct Memory Access	RDMA	An extension of hardware-based Direct Memory Access (DMA) capabilities that allow the CPU to delegate data movement within the computer to the DMA hardware.
Remote FrameBuffer	RFB	Protocol used by virtual network computing (VNC) for exporting mouse, keyboard, and display functions over an IP network.
Remote Monitoring	RMON	An MIB agent specification described in RFC 1271 that defines functions for the remote monitoring of networked devices. The RMON specification provides numerous monitoring, problem-detection, and reporting capabilities.
Remote Switched Port Analyzer	PSPAN	A capability that helps an administrator remotely monitor traffic for one or more SPAN sources distributed across one or more source switches in a Fibre Channel, Fibre Channel over IP (FCIP), or Small Computer System Interface over IP (iSCSI) fabric.
Remote-Edge Access Point	REAP	An access point that enables a Lightweight Access Point (LAP) to reside across a WAN link and still have the ability to communicate and provide the functionality of a regular LAP.

Term	Acronym	Definition
Reverse Route Injection	RRI	A feature designed to simplify network design for VPNs in which there is a requirement for redundancy or load balancing.
RFC 854		Defines the TELNET protocol.
RFC 1350		Defines TFTP.
Role-based Access Control	RBAC	A form of identity-based access control where the system entities that are identified and controlled are functional positions in an organization or process.
Role-based CLI Access		Allows the network administrator to define a view, a set of operational commands, and configuration functions that provide selective or partial access to the Cisco IOS executive and configuration mode commands. Views restrict user access to Cisco IOS CLI and configuration information; that is, a view can define which commands are accepted and which configuration information is visible.
Router		A physical device that joins multiple wired or wireless networks together. Technically, a wired or wireless router is a Layer 3 gateway, meaning that the wired/wireless router connects networks (as gateways do) and that the router operates at Layer 3.
Routing		A process of finding a path to a destination host. Routing is very complex in large networks because of the many potential intermediate destinations a packet might traverse before reaching its destination host.
Routing Information Protocol	RIP	RIP is a legacy routing protocol that uses hop count as a routing metric.
Scalability		The ability to increase workloads or the number of users, ports, or capabilities without making major changes to systems or software, and without affecting network performance. Scalability especially is important for rapidly growing enterprises and networks.
Secure FTP	SFTP	The process of tunneling a normal FTP session over a Secure Shell (SSH) Protocol connection.
Secure Shell	SSH	A set of standards and an associated network protocol that allow a secure channel to be established between a local and a remote computer. It uses public key cryptography to authenticate the remote computer and, optionally, to allow the remote computer to authenticate the user.
Secure Sockets Layer	SSL	A cryptographic protocol that provides secure communications over the Internet. SSL uses two keys to encrypt data: a public key known to everyone and a private or secret key known only to the recipient of a message. SSL commonly is used to transport HTTP (Web) traffic securely.

Term	Acronym	Definition
Secure Sockets Layer (SSL) VPN	SSL VPN	SSL VPN provides endpoint authentication for VPNs that provide remote access. In typical use, only the server is authenticated (for example, its identity is ensured) while the client remains unauthenticated; mutual authentication requires PKI deployment to clients. The protocols allow client/server applications to communicate in a way that prevents eavesdropping, tampering, and message forgery. SSL involves peer negotiation for algorithm support, public key encryption-based key exchange and certificate-based authentication, and symmetric cipher-based traffic encryption.
Security Services		Services that ensure security in all aspects of the network—from devices connecting to the network, to secured transport, to data theft prevention.
Segmentation		The ability to segment the network allows enterprises to secure sections from each other while continuing to run them on the same backbone. This technology provides consistent network segmentation of departments, business functions, and user groups, and is most appropriate for a large enterprise with an IT staff that is comfortable with greater technical complexity.
Self-defending		A strategy designed to protect an organization's business processes by identifying, preventing, and adapting to threats from internal and external sources.
Server Farm		A group of real servers in a cluster of network servers. See Cluster.
Service Connection Manager	SCM	A device providing simple configuration of Layer 2 and Layer 3 services for aggregation of IP and DSL traffic. SCM provides service management, process automation, provisioning, fault detection, configuration, and statistic tracking.
Service Limits		The number of times a health service may be used during a specific time period.
Service Set Identifier	SSID	A unique radio-network identifier used to identify a radio network that stations must use to communicate with each other or to an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.
Service-Oriented Architecture	SOA	An architecture that integrates applications by assembling a series of services to act as a business process. The services can be used to extend the outputs of traditional integration.
Service-Oriented Network Architecture	SONA	The Service-Oriented Network Architecture (SONA) is Cisco's architectural framework designed around the benefits of its intelligent information networks.

Term	Acronym	Definition
Session Initialization Protocol	SIP	A signaling protocol used to create, manage, and terminate sessions in an IP-based network. SIP enables two-way voice calls, as well as collaborative multimedia conference sessions. It opens up a world of innovative services, such as video communication and Web page click-to-dial. SIP offers many of the same architectural features as H.323 but relies on IP-specific technologies, such as DNS. It also incorporates the concept of fixed port numbers for all devices and allows for the use of proxy servers.
Signaling Connection Control Part/Skinny Client Control Protocol	SCCP	A protocol that provides additional functionality to the SS7 Message Transfer Part to support connectionless and connection-oriented network services Global Title Translation. SCCP also serves as the transport layer for Transaction Capabilities Application Part.
Simple Gateway Control Protocol	SGCP	SGCP was designed to be compatible with SIP, enabling the call agent to relay calls between a VoIP network using SIP and a traditional telephone network. The SGCP commands are encoded with syntax somewhat comparable to the SIP or HTTP headers. They carry a payload describing the VoIP media stream. This payload is encoded using the same SDP as SIP.
Simple Mail Transfer Protocol	SMTP	An Internet protocol providing e-mail services.
Simple Network Management Protocol	SNMP	A network management protocol that defines the transfer of LAN operational data between MIBs.
Simple Object Access Protocol	SOAP	A lightweight protocol for exchange of information in a decentralized, distributed environment. SOAP is an XML-based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it; a set of encoding rules for expressing instances of application-defined data types; and a convention for representing remote procedure calls and responses.
Simplified Message Desk Interface	SMDI	An interface that defines a way for a phone system to provide voicemail systems with the information needed to process incoming calls intelligently. Each time the phone system routes a call, it sends an EIA/TIA-232 message to the voicemail system that tells it the line it is using, the type of call it is forwarding, and information about the source and destination of the call.
Single Sign On	SSO	A specialized form of software authentication that enables a user to authenticate once and gain access to the resources of multiple software systems.

Term	Acronym	Definition
Single Specialty Hospital	SSH	A hospital that provides treatment relating to a single specialty, such as cardiac or orthopedic services.
Small Computer System Interface	SCSI	SCSI (pronounced "skuzzy") is a hardware interface that allows for the connection of up to 15 peripheral devices to a single PCI board called a SCSI host adapter, which plugs into the motherboard. SCSI uses a bus structure and functions like a mini-LAN connecting 16 devices, but the host adapter counts as one device. SCSI allows any two devices to communicate at one time (host-to-peripheral, peripheral-to-peripheral).
Sniffer		Software program that examines network traffic, making a copy of the data without redirecting or altering it. Some sniffers work only with TCP/IP packets, but the more sophisticated tools can work with many other protocols and at lower levels, including Ethernet frames.
SoftPhone		A communications application for use with a PC desktop.
Sonography (ultrasonography)		A diagnostic medical procedure that uses high-frequency sound waves (ultrasound) to produce dynamic visual images of organs, tissues, or blood flow inside the body.
Spanning Tree Protocol	STP	The Spanning Tree Protocol provides a loop-free topology for any bridge LAN. The Spanning Tree Protocol is defined in the IEEE 802.1d standard and calculates the shortest route by which data can reach its destination.
Sparse Mode PIM		See Peripheral Interface Manager-Sparse Mode.
Standards		The accepted measures of comparison having quantitative or qualitative value.
State Synchronization Protocol	SSP	A protocol developed to transfer state information between the active and standby routers.
Stateful Packet Filters		A firewall filtering service that protects voice communications.
Stateful Switchover	SSO	A process that transfers the state of the original router to a standby router during a router switchover. SSO provides protection for network edge devices with dual route processors that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.
Storage Area Network	SAN	High-performance local area networks designed for server clusters. A typical application of SAN is network data storage. This type of SAN supports transfers of large quantities of data to and from multiple disk arrays.
Storage Services		Services that provide distributed and virtual storage across the infrastructure. For example, synchronous and asynchronous replication, serverless backup, point-in-time copy, data migration, write acceleration, and remote backup.

Term	Acronym	Definition
Structured Query Language	SQL	A standard database query language in which the user can formulate statements that will manipulate data in a database.
Structured Wireless-aware Network		Cisco's framework for delivering integrated wired and wireless LAN networks.
Super Video Graphics Array	SVGA	An extension to the original VGA standard that allows resolutions of 800x600.
Survivable Remote Site Telephony	SRST	A mechanism providing backup to a proxy server by providing basic registrar and redirect server or back-to-back user agent services.
Switch Control Module	SCM	A module providing master control that is responsible for the following functions: system power-up and boot control, centralized routing table management, systemwide connection management, and interfaces to an external network management station.
Switch Fabric		The foundation of a router, interconnecting incoming data from ingress (input) ports to egress (output) ports. There are multiple switch fabric architectures with differing strengths in terms of bandwidth, throughput, and delay.
Switch Port Analyzer	SPAN	A feature that allows troubleshooting of a SAN/LAN by letting an administrator collect protocol-level data without any interruption to production traffic.
Synchronous Digital Hierarchy	SDH	A European standard that defines a set of rate and format standards that are transmitted using optical signals over fiber. SDH is similar to SONET, with a basic rate of 155.52 Mbps, designated as STM-1. See Synchronous Optical Network.
Synchronous Optical Network	SONET	A high-speed synchronous network specification developed by Bellcore and designed to run on optical fiber. See Synchronous Digital Hierarchy.
Syslog		A logging feature that tracks all fabric events occurring with hardware or software. Events may include connect or disconnect activity, power or fan outages, changes to configuration, environmental changes, and any proactive or reactive fabric changes. The Syslog service indicates what the event is, when it occurred, where the issue may be within the fabric, and the level of criticality.
Systematized Nomenclature of Human and Veterinary Medicine	SNOMED	A standardized vocabulary system for medical databases. Current modules contain more than 144,000 terms and are available in at least 12 languages. SNOMED has potential to become the standard vocabulary for speech recognition systems and computer-based patient records.

Term	Acronym	Definition
T1		A digital WAN carrier facility, T1 transmits DS1-formatted data at 1.544 Mbps through the telephone switching network.
Telemedicine		The use of electronic communication and information technologies to provide or support clinical care at a distance.
Teleradiology		The process of sending radiology images from one location to another.
Telnet		A protocol providing standard terminal emulation in the TCP/IP protocol stack. Telnet is used for remote terminal connections, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.
Temporal Key Integrity Protocol-Per-Packet Keying	TKIP-PPK	A protocol that provides initialization vector hashing and an MIC to ensure data integrity.
Time Division Multiple Access	TDMA	A satellite and cellular phone technology that combines multiple digital signals onto a single, high-speed channel. For cellular, TDMA triples the capacity of the original analog method (FDMA). It divides each channel into three subchannels, providing service to three users instead of one.
Time Division Multiplexing	TDM	A type of digital multiplexing in which two or more apparently simultaneous channels are derived from a given frequency spectrum (for example, bitstream) by interleaving pulses representing bits from different channels. In some TDM systems, successive pulses represent bits from successive channels (for example, voice channels in a T1 system). In other systems, different channels take turns using the channels for a group of successive pulse times (a time slot).
Total Cost of Ownership	TCO	The cost of owning and operating a business network.
Transcoder		A technology for converting between different codecs. Transcoding is needed when the calling and called parties cannot use the same codec type.
Transmission Control Protocol	TCP	A connection-based Internet protocol that is responsible for packaging data into packets for transmission over the network by the IP protocol. TCP provides a reliable flow-control mechanism for data in a network.

Term	Acronym	Definition
Transmission Control Protocol/Internet Protocol	TCP/IP	The Internet suite of protocols used to connect a worldwide internetwork of universities, organizations, and corporations. TCP/IP is the protocol used to communicate between the Central Controller and devices in the Cisco ICM software system. TCP/IP is based primarily on a connection-oriented transport service, the Transmission Control Protocol (TCP), and a connectionless-mode network service, the Internet Protocol (IP). TCP/IP provides standards for how computers and networks with different technologies communicate with each other.
Transport Layer Security	TLS	A protocol that provides data integrity and privacy on a communications link over the Internet. It allows client/server applications to communicate and is designed to prevent eavesdropping, message forgery, and interference.
Triple DES	3DES	A data encryption standard. It offers a stronger form of encryption than DES, providing 168-bit encryption keys that allow transmission of sensitive information over untrusted networks. 3DES provides security for in-flight data packets on iSCSI or FCIP. 3DES is more secure than DES but requires more processing for encryption and decryption.
Trivial File Transfer Protocol	TFTP	A simple protocol used to transfer files. It runs on UDP and is explained in depth in RFC 1350.
Trunk		A telephone line connected to a call center and used for incoming or outgoing calls.
Unicast Packet		A single data message (packet) sent to a specific IP address.
Unicast Reverse Path Forwarding	uRPF	A feature that helps mitigate problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address.
Unified Messaging		A messaging system in which all types of messages can be managed from the same inbox.
Uniform Bill 92	UB92	The common claim form used by hospitals to bill for services. Some managed care plans demand greater detail than is available on the UB92, requiring hospitals to send additional, itemized bills.
User Datagram Protocol	UDP	A communications protocol that offers a limited amount of service when messages are exchanged on an IP network. UDP is an alternative to TCP. Together with IP, it sometimes is referred to as UDP/IP. Like TCP, UDP uses IP to transport a data unit, called a datagram. UDP, however, does not provide the service of dividing a message into packets and reassembling it at the other end.

Term	Acronym	Definition
Usual, Customary, and Reasonable	UCR	A fee-controlling system to determine the value of physician reimbursement based on the physician's usual charge for a given procedure, the amount customarily charged for the service by other physicians in the area, and the reasonable cost of services for a given patient after medical review of the case.
Utilization Review		A series of processes that ensures medically necessary acute inpatient and outpatient care has been provided in the most appropriate and cost-effective settings.
Variable Size Frame	VFrame	A service providing the virtualization, orchestration, and provisioning services to address data center resources, including switching, data network, load balancing, and security products.
Video Codec		A video codec is a device that enables video compression or decompression for digital video. Digital video codecs are found in emerging satellite and terrestrial broadcast systems and on the Internet. Video codecs allow delivery of live, high-quality streaming video using network-efficient multicast technology.
Videoconferencing		A technology that allows interactive communications between two or more people who are geographically distant, providing video and audio elements.
Video Graphics Array	VGA	A video standard that allows for resolutions up to 640x480 with up to 16 colors at a time or 320x200 resolution with 256 colors.
Video on Demand	VoD	A system that allows users to select and watch video content over a network as part of an interactive television system.
Video Terminal Adapter	VTA	A self-contained video interface that connects one H.320 system to an IP network.
Virtual Local Access Network	VLAN	A virtual LAN, commonly known as a VLAN, is a logically independent network. Several VLANs can coexist on a single physical switch.
Virtual Network Computing	VNC	A desktop sharing system that uses the remote framebuffer (RFB) protocol to remotely control another computer.
Virtual Private Network	VPN	An overlay network that links to users via secure Internet connections, causing it to behave as a private network although it sits on top of the public Internet. VPNs provide networking organizations with all the advantages of a private network at the much lower cost of a public one.

Term	Acronym	Definition
Virtual Router Redundancy Protocol	VRRP	Provides default gateway redundancy, where the backup members of the peer relationship are idle, waiting for a failure event to occur. Only one device responds to an ARP request; the other waits until there is a failure.
Virtual Storage Area Network	VSAN	VSANs allow administrators to divide a switch or group of switches logically into separate, isolated fabrics.
Virus		Pieces of malicious code that attach themselves to a host file or message and are physically propagated by users sending or sharing them through e-mail or by loading disks.
VLAN Load Balancing		A network design in which the HSRP and Spanning Tree root alternate between distribution node peers with the even VLANs homed on one peer and the odd VLANs homed on the alternate peer.
Voice Activity Detection	VAD	A service that, when enabled on a voice port or a dial peer, does not allow silence to be transmitted over the network, only audible speech. When VAD is enabled, the sound quality is slightly degraded but the connection monopolizes much less bandwidth.
Voice and Collaboration Services		Services that carry voice across the network. Examples are security, multicast, QoS, PoE, integrated call managers, distributed call manager clusters, integrated gateway and gatekeeper functions, and voice gateways.
Voice over IP	VoIP	VoIP is a technology that allows telephone calls to be made over the Internet by converting analog voice signals into digital data packets. VoIP offers substantial cost savings over traditional long-distance telephone calls. Many VoIP implementations are based on the H.323 technology standard.
Voice Recognition		The ability for a computer system to recognize spoken words.
Voice Response Unit	VRU	See IVR.
VPN Routing/Forwarding Instance	VRF	An instance consisting of an IP routing table, a derived forwarding table, a set of interfaces that uses the forwarding table, and a set of rules and routing protocols that determines what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a router.
War Driving		A method used to hack into and capture the access point's beacons for SSID, radio MAC address, WEP protocol status, and other information.
Wavelength Selective Switch	WSS	A switch that directs each wavelength from a common input port to any of multiple output ports.

Term	Acronym	Definition
Web Cache Communication Protocol	WCCP	A protocol for communication between routers and Web caches. Two versions exist: WCCP Version 1 (WCCPv1) and WCCP Version 2 (WCCPv2). The two versions are incompatible. Cisco IOS images can support either or both.
Webconferencing		A communications medium used to hold group meetings or live presentations over the Internet.
Web Services Description Language	WDSL	The XML-based language that is used to describe a Web service.
Wide Area File Services	WAFS	Software that overcomes WAN latency and bandwidth limitations with optimization technologies, offering branch office users a LAN-like experience when accessing the centralized files over the WAN.
Wide Area Network	WAN	A network connecting local area networks. Typical WAN interfaces include plain old telephone service (POTS) lines, digital subscriber lines (DSL), cable, T1/T3, and ISDN.
Wi-Fi		The industry name for wireless LAN (WLAN) communications technology related to the IEEE 802.11 family of wireless networking standards. Today, however, Wi-Fi can refer to any of the three established standards: 802.11a, 802.11b, and 802.11g. The Wi-Fi Alliance certifies vendor products to ensure 802.11 products on the market follow the various 802.11 specifications.
Wi-Fi Protected Access	WPA	Wireless network architecture that addresses most known WLAN encryption threats. WPA uses EAP for transport of authentication information between client and authentication server.
Wi-Fi Protected Access 2	WPA2	An enhanced version of WPA. It is the official 802.11i standard that was ratified by the IEEE in June 2004. It uses AES instead of TKIP. AES supports 128-bit, 192-bit, and 256-bit keys.
Windows Media Video	WMV	A generic name for the set of video codec technologies developed by Microsoft.
Wired Equivalent Privacy	WEP	WEP is an encryption protocol that adds security to WLANs based on the 802.11 Wi-Fi standard. WEP is an OSI Data Link layer (Layer 2) security technology that can be turned on or off. It was designed to give wireless networks a level of privacy protection equivalent to a wired network. It is based on a security scheme called RC4 that uses a combination of secret user keys and system-generated values. When communicating over the wire, wireless network equipment uses WEP keys to encrypt the data stream.

Term	Acronym	Definition
Wireless Application Protocol	WAP	A language used for writing Web pages that uses far less overhead, which makes it more preferable for wireless access to the Internet.
Wireless Control System	WCS	A platform for wireless LAN planning, configuration, and management. A foundation allowing IT managers to design, control, and monitor enterprise wireless networks from a centralized location. This optional network component works in conjunction with Cisco Lightweight Access Points, Cisco wireless LAN controllers, and the Cisco Wireless Location Appliance.
Wireless Domain Services	WDS	An access point providing WDS on a wireless LAN maintains a cache of credentials for CCKM-capable client devices on the wireless LAN. When a CCKM-capable client roams from one access point to another, the WDS access point forwards the client's credentials to the new access point with the multicast key. Only two packets pass between the client and the new access point, thereby shortening re-association time.
Wireless LAN	WLAN	In a typical WLAN configuration, clients communicate through an access point where wireless clients access the network. The access point provides connectivity to other clients associated with itself or to the wired LAN.
Wireless LAN Solutions Engine	WLSE	A specialized appliance designed to manage WLAN infrastructures. It centrally identifies and configures access points in customer-defined groups and reports on throughput and client associations.
Workstation		A computing device with an installed client adapter.
Worm		A subclass of viruses that does not need a host. They are free-standing applications that duplicate themselves and use system resources, such as tapping into an address list and sending undesired e-mails to members of this address list.
Zigbee		A low-data-rate, two-way standard for home automation and data networks.

Acknowledgements

The authors of this paper would like to thank all the participants for their teamwork and cooperation. Special thanks to Matt Mandrgoc and Terry McMann for their contributions in developing and reviewing all of the materials. Other significant contributors included Tony Anderson, Nick Augustinos, Michael Boland, Dave Evans, Carla Gallegos, Kamal Hyder, May Konfong, Bob Meindl, and Terri Quinn-Andry.

More Information

The Cisco Internet Business Solutions Group (IBSG), the global strategic consulting arm of Cisco, helps Global Fortune 500 companies and public organizations transform the way they do business—first by designing innovative business processes, and then by integrating advanced technologies into visionary roadmaps that improve customer experience and revenue growth.

For further information about IBSG, visit http://www.cisco.com/go/ibsg

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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

C11-404465-01 02/08