Nepal GEA Infrastructure Architecture
Document History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>November, 2010</td>
<td>Draft</td>
<td>PwC India</td>
<td>Nepal GEA Infrastructure Architecture – Draft version</td>
</tr>
<tr>
<td>January, 2011</td>
<td>Final</td>
<td>PwC India</td>
<td>Nepal GEA Infrastructure Architecture – Final version</td>
</tr>
</tbody>
</table>

Distribution

<table>
<thead>
<tr>
<th>Title</th>
<th>No. of Copies</th>
</tr>
</thead>
<tbody>
<tr>
<td>HLCIT:</td>
<td></td>
</tr>
<tr>
<td>Primary: Mr. Juddha B. Gurung</td>
<td></td>
</tr>
<tr>
<td>Secondary: HLCIT to decide</td>
<td>1</td>
</tr>
</tbody>
</table>

# Table of Contents

1. Introduction ............................................................................................................. 8
   1.1 Executive Summary ......................................................................................... 8

2. Design Considerations .......................................................................................... 25
   2.1 Security ........................................................................................................... 25
      2.1.1 Shared Security Services ........................................................................ 25
      2.1.2 Shared Infrastructure Security Risks ....................................................... 26
      2.1.3 Network Security In a Secure Segment ................................................ 27

2.2 Availability ........................................................................................................... 30

2.3 Scalability ............................................................................................................ 31
      2.3.1 Network Virtualisation — Services Edge Design .................................. 31
      2.3.2 Integrating a Multi-VRF solution into the Data Center ......................... 34
      2.3.3 Shared Services Implementation in the Data Center ............................... 35
      2.3.4 Virtualised Internet Edge Design — Shared Internet Access ................ 38
      2.3.5 Firewall In Routed Mode ...................................................................... 42
      2.3.6 Firewall In Transparent Mode ................................................................ 42

2.4 Manageability ..................................................................................................... 43
      2.4.1 Overview and Goals ................................................................................ 43
3. State Wide Area Network ........................................................................................................51

3.1 Proposed Infrastructure .......................................................................................................51

3.1.1 NWAN Network Architecture and Topology: .................................................................52
3.1.2 Data Flow from PC to PC in NWAN: ..............................................................................53
3.1.3 Voice calls flow from NWAN phone to NWAN phone: ..................................................54
3.1.4 Video Call Flow: ..............................................................................................................54
3.1.5 Tier – 1: NITC NWAN Center Network ..........................................................................55
3.1.6 Mobility feature introduced into GSWAN: .................................................................55
3.1.7 WLAN for important other offices beyond reach of cable: ........................................55
3.1.8 Server farm: ....................................................................................................................55
3.1.9 Tier 2 – District Center – Generic Architecture.............................................................56

4. State Data Center ....................................................................................................................58

4.1 Data Center Architecture ....................................................................................................58

4.1.1 Description ......................................................................................................................58

4.2 Data Center Operations and System Management .............................................................59

4.2.1 Benefits of ITIL ................................................................................................................60
4.2.2 Improving Levels of Service .......................................................................................60
4.2.3 Reducing IT Costs .........................................................................................................60
4.2.4 Enforcing well-defined processes ..............................................................................60

4.3 Security Considerations for the Data Center ..................................................................60

4.4 Data Center Security Framework .......................................................................................62

4.4.1 Network security access and control ..........................................................................63
4.4.2 Common Service Network ............................................................................................63
4.4.3 User Authentication for Remote Access ..................................................................64
4.4.4 Virtual Private Network ...............................................................................................64
4.4.5 Intrusion Detections Systems (IDS) ...........................................................................64
4.4.6 Anti-Virus Protection .....................................................................................................64
4.4.7 System and Network Security Scanning ....................................................................64

4.5 Data-center Automation ......................................................................................................65

4.6 The business value of Data Center Automation ................................................................65

4.6.1 Basic benefits of IT - ....................................................................................................66
4.6.2 The Value of Data-center Automation ........................................................................66
4.7 Service Provider

4.7.1 Benefits of operating IT as a Service Provider

4.7.2 Implement the Service Provider Model

4.8 Configuration Management Database

4.8.1 The need for a CMDB

4.8.2 Benefits of using a CMDB

4.9 Service Level Agreements

4.9.1 Challenges related to IT Services Delivery

4.9.2 Defining Service Level Requirements -

4.10 IT Processes

4.10.1 The Benefits of Processes -

4.11 Policy Enforcement

4.11.1 Benefits of Policies

4.11.2 Types of Policies

4.11.3 Defining Policies

4.12 Business Processes

4.12.1 Benefits of Well Defined Processes

5. Infrastructure Roadmap

5.1 Roadmap – Shared Network Adoption

5.2 Roadmap – Data Center Consolidation

5.2.1 Phase 1 – IT Asset Inventory Baseline (Including Preliminary Assessment & Quick Wins)

5.2.2 Phase 2 – Application Mapping

5.2.3 Phase 3 – Analysis & Strategic Decisions

5.2.4 Phase 4 – Consolidation Design & Transition Plan

5.2.5 Phase 5 – Consolidation & Optimization Execution

5.2.6 Phase 6 – Ongoing Optimization Support

5.2.7 End Goal

6. Infrastructure Governance

6.1 Principles

6.1.1 Actively design governance

6.1.2 Know when to redesign

6.1.3 Involve senior managers

6.1.4 Make choices

6.1.5 Clarify the exception-handling process

6.1.6 Provide the right incentives

6.1.7 Assign ownership and accountability for IT governance
1. Introduction
# 1. Introduction

## 1.1 Executive Summary

People want a Government which meets their needs at an affordable cost, improves the quality of lives, which is available when they need it, and which delivers results to them. Physical separation between citizens and Government must not pose any limitation to the effective Governance.

Information Technology is a key enabler to the process of smart e-governance, offering access and delivery of services to the expectations of people:

- Horizontal and Vertical integration within the organization is essential for effective and efficient information exchange.
- This should be followed by authorizing public access to administration at various points in this Horizontal and Vertical information corridor.
- Standardizing, and transforming all citizens’ centric Government’s applications into electronic form for interactive public use is the last step in e-governances process.

To operationalize the goal for e-governance, a countrywide IT infrastructure deployment should be planned from two perspectives:

- shared and secured network, and
- shared data center services

To assist the Nepal government with the objective of improving interagency IT infrastructure sharing in we are assembling a set of best practices and design considerations that address:

- Shared Infrastructure
- Shared Data Center Services
- Shared Security Services
- Shared Infrastructure Management Services (Network and Datacenter)

## 1.2 Shared Infrastructure for the Government

A shared infrastructure can enable greater productivity, enhance collaboration, and improve service. By implementing a comprehensive architecture for shared network services, agencies can:

- Control and enhance network access for their employees, customers, partners, vendors, contractors, and guests
- Reduce IT support resources and expenses
- Keep the traffic of the various user groups securely separated from one another
- Have full auditing of network usage
The need for shared infrastructures has developed as the needs of operations support have evolved. At one time, it was sufficient to provide employees with a workspace, computer, and telephone. Today, agencies frequently have multiple, widely-dispersed offices, share vast amounts of data internally and externally with other agencies, and must be able to communicate quickly and reliably. Employees require full connectivity to a variety of public and private resources without compromising the security of the host network.

The main technical requirements for a complete shared infrastructure architecture are:

- Remote access from branch or home locations and the capability to establish a VPN connection to the network when traveling
- Logical isolation of traffic from the appropriate users
- Authentication and logging capabilities
- Accounting, filtering, content checking, and security
- Seamless support for both wired and wireless access

An example of a traditional architecture to connect branch offices to the headquarters leverages a privately-owned WAN, leased lines, ATM networks, and Frame Relay connections.

The requirement to reduce costs has, in recent years, led to the adoption of a new type of connectivity between branch locations and headquarters. In these deployments, VPN architectures (mostly IPSec) are implemented to leverage the public Internet. We have seen some adoption of these ideas within some ministries and departments within the Nepal government including the Nepal Police.
The goals of this architecture are to:

- Identify a user as a guest or employee and assign them to the appropriate segment
- Isolate the guest traffic from the rest of the network while providing Internet access
- Provide network services to enterprise visitors, including the following:
  1. Network services—DHCP, DNS, and Internet
  2. Security services—Firewalls, load balancers, intrusion detection systems (IDSs), accounting, and monitoring

The architectural framework is divided into three functional areas:

1. the access centers / the government offices and the citizens,
2. the connectivity / wide-area-network,
3. the data-center / computing resources

### 1.3 Shared and Secured Network Architecture

From a networking perspective, each of the above functional areas maps to one of the following objectives:

- Access control
- Path isolation
- Services edge

The goal is to provide a separate virtual environment for each group of users. For example, a guest user should be assigned to the guest virtual network, while an employee should be assigned to the internal virtual network or simply remain on the original enterprise network.

Because the various virtual networks are deployed on a common shared infrastructure, the physical access ports to the network are shared by the various groups. This implies that switch ports (for wired clients) and access points (for wireless clients) become shared network resources for internal employees and guests.

A dynamic mechanism is necessary to differentiate employees from guests and to assign their port the appropriate policy. This policy ensures that the users of one group can access only their own virtual network while the users of other groups are assigned to their respective segments. The policy can be as simple as the assignment of the port or access point association to a specific VLAN. This maps the user on that port to the virtual network. In the case of a guest, this means recognizing that a user is a guest and confining them to the guest segment of the network. Devices, for example, in the guest segment of the network can reach only the Internet and are subject to traffic accounting controls.

#### 1.3.1 Access Control

The access control functional area aims to identify the users or devices logging into the network so they can be successfully assigned to the corresponding groups. This process of identifying the users or devices is known as authentication.

When identified, the endpoints must be authorized onto the network. To achieve this, the port on which an endpoint connects is activated and configured with certain characteristics and policies. This process is known as authorization. Examples of authorization include the configuration of the VLAN membership of a port based on the results of an authentication process and the dynamic configuration of port access control lists (ACLs) based on the authentication.
For wireless access, the concept of a “port” is replaced by an “association” between client and access point. When authorizing a wireless device, the association is customized to reflect the policy for the user or device. This customization can take the form of the selection of a different wireless LAN (WLAN), VLAN, or mobility group, depending on the wireless technology employed.

When an endpoint is authorized on the network, it can be associated to a specific user group that usually corresponds to a separate virtual network in a segmented network architecture. Thus, it is the authorization method that ultimately determines the mapping of the endpoint to a virtual network. For example, when a VLAN is part of a virtual network, a user authorized onto that VLAN is therefore authorized onto the virtual network.

The main authentication scenarios for the enterprise are as follows:

- Client-based authentication for endpoints with client software
- Clientless authentication for endpoints with no client software

The current state of technology provides broad support for VLAN assignment as an authorization alternative. In the cases where policy changes based on authentication are required and only VLAN assignment authorization is available, a static assignment of a policy to a VLAN provides the required linkage between the user authorization and the necessary policy. In effect, the policy is applied to the VLAN because users are subject to the policy when authorized onto the VLAN.

1.3.2 Path Isolation

After the guests/customers are assigned to the appropriate segment, they should never have access to the internal agency resources. To achieve this, you can keep traffic logically isolated by using separate Layer 2 domains (VLANs or wireless domains) for guests, customers, and employees.

To preserve end-to-end separation, those Layer 2 domains must be extended across the entire network. Extending Layer 2 domains end-to-end negates all the scalability and modularity benefits achieved by a hierarchical network design. IP routing is at the heart of the hierarchical design because of its ability to limit the size of broadcast domains and to lessen the impact of failures and changes by providing a modular structure that is capable of preventing problems from propagating and affecting the entire network. A mechanism to provide network virtualization while preserving the scalability and modularity of the routed network is necessary.

When the Layer 2 domains at the edge are connected to the routed core of the hierarchical network, the logical isolation achieved at the edge by the Layer 2 domains is lost. A mechanism to give continuity to those segments over the routed core is needed.

The following alternatives are available to maintain this logical traffic separation in the Layer 3 domain of the enterprise network:

- Distributed ACLs—ACLs can be configured at the frontier points between the edge Layer 2 domains and the routed core. These ACLs should ensure that hosts in one group can access resources only in their own group. Thus, a user in group A should be able to reach addresses of users and resources only in group A. This policy can be enforced by means of an ACL, provided that the IP prefixes belonging to a group are well-known. Keeping track of the various combinations of IP addresses that belong to a group is a cumbersome task and can reach its scale limit relatively quickly, especially when peer-to-peer connectivity is required within the segments. For certain applications, such as guest access, the requirement is for many-to-one connectivity. In this case, the use of distributed ACLs might provide a manageable mechanism for restricting guests access to only the Internet edge. The ACL should simply deny access to any internal prefix and allow access to the Internet. This ACL is identical everywhere and is, therefore, relatively manageable.
Overlay of generic routing encapsulation (GRE) tunnels interconnecting VRFs (VPN Routing and Forwarding – a routing table instance)—Another mechanism to provide continuity over the routed network to the logical separation provided by VLANs at the edge is to use IP tunnel overlays. A tunnel overlay (either in a full or partial mesh) is created for each user group. Each tunnel overlay is mapped to the group VLANs at the various sites. For example, the traffic in a guest VLAN maps to the tunnel mesh created for guests, while all other traffic is treated normally (no tunnel overlay). Guest traffic being tunneled to specific places prevents the guests from reaching any enterprise resources not present in the guest segment. To associate the VLANs with the tunnel overlays, policy-based routing (PBR) can be used. However this requires the use of distributed ACLs and therefore provides little added value when compared to a pure ACL approach.

By associating the VLAN interfaces and the tunnel interfaces in a group to a VRF, VLANs can be mapped to the required tunnel overlay. VRFs are considered virtual routers (although they are not strictly that) to which different interfaces can be assigned. Assigning VLAN interfaces and tunnel interfaces to these VRFs effectively creates a virtual network that has its own links and routed hops. Thus, a virtual network built this way consists of VLANs, VRFs, and GRE tunnels—all working together to form a separate overlay topology.

For the specific agency/department access scenario, there is an instance of an agency/department VLAN at every access point, an agency/department VRF at every distribution point, and an agency/department mesh of tunnels interconnecting the agency/department VRFs present at the distribution points. A routing protocol must run between the VRFs and over the tunnel mesh to provide the necessary reachability information. The underlying infrastructure is designed according to well-known hierarchical and high-resiliency principles. Hence the tunnel overlay enjoys these benefits.

- VRFs at every hop interconnected with VLAN (802.1q) trunks—This approach basically creates multiple parallel networks. Each group of users has a VRF at every hop, and all the VRFs for one group are interconnected. To keep traffic from the various groups separate as they travel from hop-to-hop, dot1q trunks are used to provide logical point-to-point connections between the VRFs. For each group, this provides an end-to-end virtual network in which each routed hop is represented by a VRF and each connection is represented by an 802.1q logical link. In a traditional network, each hop is a router and each connection is a physical wire. VRFs allow you to have separate logical routers and 802.1q allows you to interconnect these with separate logical wires. This requires a routing protocol to run at each VRF to convey the necessary network reachability information. This model maps directly to the hierarchical model of network design and therefore enjoys the same benefits of scalability and resiliency that have become required in any network design.

- MPLS/BGP VPNs (RFC2547)—This technique uses MPLS to dynamically create a tunnel mesh similar to the tunnel overlay created for the GRE-based architecture. These dynamic tunnels are better known as label switched paths (LSPs), which handle traffic forwarding, while Border Gateway Protocol (BGP) is used to carry routing information between the VRFs. The separation of the control plane and the data plane is the key to being able to create the LSPs dynamically. This is the most scalable technique of all the techniques described, but it is also the most demanding in terms of platform capabilities.

Some of these techniques apply exclusively to the campus and others are better suited for the aggregation of branches over the WAN. For example, a hop-to-hop VRF technique is better suited for the LAN than the WAN, primarily because of the requirement to control every hop in the network (including the core). A tunnel overlay architecture is better suited for the WAN, where the tunnels allow you to segment without having control of every hop in the core of the network. Usually these are service provider routers over which the customer has no control. Also the aggregation of branches over the WAN usually follows a hub-and-spoke logical topology, which is well-suited for the implementation of a static tunnel overlay.

Whichever technique is used, it can be overlaid onto the existing infrastructure. This means that the network continues to function as usual and only traffic that is steered into the created VPNs is isolated or segmented.
1.3.3 Services Edge

When the groups (agency/department and guest/customer in this scenario) have been separated, they need access to certain services. Some of these services are dedicated to each group, while others are shared among several groups. Agency/department requires access to its data centers, network services (e.g., DHCP servers, DNS servers), and many other resources including the Internet. Guests/customers require access to network services (e.g., DHCP, DNS, or Web authentication mechanisms), as well as the Internet. The Internet represents, in this case, a resource that is very likely to be shared between guests/customers and employees, while other services might be dedicated. The services edge provides the mechanisms necessary for users from different groups to access common services without compromising the security gained by isolating the groups from each other. The services edge also provides access to services that are dedicated to each specific group. To achieve this, it provides logical connectivity and security mechanisms over shared facilities, such as firewalls, load balancers, VPN concentrators, or even IDSs.

The virtualization of the enterprise network allows for the creation of a separate logical network that is placed on top of the physical infrastructure. The default state of these virtual networks (VPNs) is to be totally isolated from each other, in this way simulating separate physical networks.

The default behavior of a virtual network may be changed for the following reasons:

- allow inter-VPN communications; this must be done in a safe and controlled manner.
- To allow the various VPNs to share certain services; the most common is Internet access, but there are also network services, such as DHCP and DNS, and server farms.

To allow secure communication between each VPN and the Internet, it is necessary to create unique points of ingress and egress to each defined virtual network. This can be achieved by configuring the routing inside of each VPN to forward traffic destined outside the VPN to a specific gateway. When traffic reaches this gateway, it can be controlled by means of ACLs, firewalls, IDSs, or any other in-band security mechanisms that are considered necessary.

This is the equivalent of treating each VPN as if it were a physically separate network. Separate networks connecting to a common resource must have a security device headend to control access to the network.

The device typically used for this is a firewall. When accessing the Internet, the place in the network where such a firewall is deployed is known as the Internet edge. Figure illustrates a typical perimeter deployment for multiple VPNs accessing common services.

1.4 Shared Datacenter Services (Service Oriented Network Architecture – SONA)

Data centers are evolving and government agencies that focus on shared infrastructure architectures can benefit from this evolution. Data centers house many critical assets for government agencies, including data storage systems, applications, and servers that support day-to-day operations. Traditionally, these data centers housed mainframe computers, then client and server systems. Over several decades of build outs, data centers became overly complex, at times underused and exhausting physical resources such as heat, space, and power. However these expansions also provided for scalability, reliability, and availability. As the shared infrastructure architecture for data centers is designed, these shortcomings must be mitigated while preserving the positive critical attributes.

Cost is the most critical factor driving data center consolidation because as data centers expanded to meet agency requirements, with more and more servers, applications, and storage devices, they became increasingly expensive to support and maintain. Costs include the real estate required to store the equipment, some of which may only be operating at a fraction of its capacity, the power to run the equipment, and the maintenance of the devices. Hence while capital expenditures (CapEx) present the initial financial impact, recurring operating
expenses (OpEx) place a huge financial strain on government agencies, particularly when many government agencies maintain their own low-capacity, and inefficient, data centers.

In addition to the challenge of maintaining dedicated infrastructure, high operational expenses may cause agencies to sacrifice the technologies required to keep data centers secure, current with technology, and accessible. For example, in the above figure, the local Nepal Police services may not be able to centralize their data center. Its Kathmandu, Nepal location drives up bandwidth utilization at this site, which may at times overwhelm the last-mile connection and create unsatisfactory experiences for remote sites. Furthermore, this department may not have access to the technologies required to make the data center highly secure, which it could be if centralized and managed by a well-trained staff. In addition, many of the components are duplicated across agencies and may be operating at only a fraction of their capabilities.
A shared infrastructure architecture for data center consolidation drives down the cost while updating the technology, and hence becomes attractive on multiple levels. Agencies can reap huge financial benefits so they can redeploy funds to other projects instead of wasting it maintaining an inferior legacy operation.

In the shared data center approach of the shared infrastructure architecture, a center of excellence delivers to each agency a uniform set of data center services that are technologically current and much more cost-effective. To accomplish this, the next-generation shared data center must meet these requirements:

- Scalability, availability, and reliability—The consolidation of infrastructure into a shared LAN/WAN environment leads to higher-bandwidth 10 Gigabit Ethernet links in the access and aggregation network, while maintaining a high-availability design to ensure that the data centers are always accessible.

- Security—An ever-increasing factor in network design is security, requiring both products and a suite of security best practice designs to ensure that the critical assets of data centers can withstand known and day-zero threats.

- Segmentation—Consolidation of data centers translates to secure resource allocation and full utilization of the assets, thereby maximizing the capabilities of the equipment. In a shared environment,
segmentation allows multiple agencies to share assets that are partitioned to meet the requirements of each agency.

- **Virtualization**—With the capacity of the WAN, multiple sites for data centers and agencies can now virtualize more assets into the data center and offload the management of onsite gear. These assets can be located in multiple data centers to provide greater survivability in the event of unforeseen circumstances that might bring down a particular site.

- **Intelligence**—Different departments have different application requirements that can strain the data center. Intelligent service blades enable application acceleration, increased application security, and methods to simplify the application infrastructure to permit the faster deployment of new application servers.

- **Manageability**—This center of excellence approach simplifies the management of the data center. With infrastructure segmentation and virtualization bundled with management tools from major component OEMs and partners, the shared data center architecture drastically reduces agency overhead and streamlines operations.

A shared infrastructure architecture that meets these requirements helps drive down the total cost of ownership while enabling the data center to effectively meet the demands of multiple agencies. This can help address any regulatory or political roadblocks that a consolidation effort might face. Finally, the efficiencies gained not only reduce cost, but enable government agencies to more effectively develop tools to serve their constituents.

### 1.4.1 Data Center Network Architecture

The shared data center architecture of the shared infrastructure approach can be highly sophisticated. The components of the data center are simplified here to explore the specific requirements of a well-designed shared data center for multiple agencies.
Building blocks:

- Network areas—Core, aggregation, access, and DC interconnect
- Network DNA—Layer 2 and Layer 3 designs, high availability, and clustering
- Network virtualization and segmentation
- Network intelligence
- Network security

- Server fabric
- SAN fabric
1.5  **Data Center Architecture - Building Blocks**

1.5.1  **Network Areas**

The basis of the data center network can be compartmentalized into the access, aggregation, core, and DC interconnect network.

In the access network, a key question is whether to use a Layer 2 or Layer 3 design, as in figures below. Considerations include the availability requirements of the applications and server, sizing of the broadcast applications, the amount of over-subscription required for a multiple agency deployment, etc. The shared infrastructure architecture may support either a Layer 2 or Layer 3 implementation depending on the requirements and expertise of the staff.

In the aggregation network, several key architectural components are positioned. The aggregation network must also meet scalability demands by aggregating traffic into the DC core. To provide security and advanced application intelligence to each agency utilizing the shared infrastructure, the aggregation layer has built-in security capabilities using distributed-denial-of-service (DDoS) blades, application intelligence with the ACE product, and additional Layer 4-7 services such as firewall, session load balancing, Secure Sockets Layer (SSL), and IDS. These powerful capabilities at the aggregation layer enable agencies without the expertise to design and operate these advanced services to still benefit from them through the shared data center approach.

In the DC core network, connectivity to the enterprise is provided to multiple sites and multiple agencies. The DC core is built to be very highly scalable with 10 Gigabit Ethernet links and redundancy that provides the capability to isolate failure domains and ensure connectivity between critical assets.

For widely dispersed agencies, such as country wide, that require connectivity, it is critical to ensure site survivability and geographic diversity of the data centers. To meet this demand, multiple data centers have various options to deliver on DC interconnect, ranging from a self-managed or service provider-managed WAN that can be supported over Metro Ethernet networks, traditional SONET/SDH networks, or dense wavelength-division multiplexing (DWDM) networks. These connectivity options maintain carrier-class attributes for communication between multiple data centers.

1.5.2  **Network DNA**

Meeting the traditionally expected requirements for data centers, such as scalability, availability, and reliability, is central to a shared data center network.
In a Layer 2 network, Rapid Per-VLAN Spanning Tree (PVST+) or PVST+ is used on the switches to provide fast convergence of STP. For even faster convergence times, with zero seconds of packet loss, Layer 3 fast-convergence techniques with Open Shortest Path First (OSPF) protocol and Enhanced Interior Gateway Routing Protocol (EIGRP) can help ensure that applications, servers, and storage units are not affected in case of a failure.

An important capability to protect data center servers is network interface card (NIC) teaming and clustering. Clustering exists when multiple servers for a specific agency are clustered together to behave as a single device—a common method for ensuring high availability and load balancing for servers. Two servers in a cluster may even be across different switches supported by extended VLANs and STP diameter. The servers communicate at Layer 2 to exchange state, session, and other information. With NIC teaming, it is common for servers to be dual connected for high availability. If a NIC loses connectivity, the other NIC inherits the properties of the failed NIC. Therefore the server is always reachable by the same IP address. To support this, both NICs must belong to the same broadcast domain and the access switches must provide Layer 2 adjacency between the two NICs.

1.5.3 Network Virtualization and Segmentation

As next-generation data centers are designed, virtualization and segmentation of network assets enables increased flexibility and cost savings to government agencies building shared infrastructures. Virtualization allows the vast numbers of servers and high storage volume to be centralized into redundant data centers, allowing devices to be centrally managed and maximally utilized. Segmentation takes the virtualization of the data center one step further, allowing the same infrastructure to be shared among multiple agencies. To support segmentation, the critical attribute is that the physical resource is virtually distinct and separate. For the government, this allows a converged network to deploy common and sustainable services to a building that supports multiple agencies which want to offload services to a shared network infrastructure serviced by the data centers. The common network infrastructure securely provides segmentation of traffic between the multiple agencies. Segmentation could also provide departmental isolation within a specific agency if that is a requirement. Common methods of isolation include:

- Guest access
- Closed user groups
- Application-access rights
- Departments and divisions such as finance, engineering, and administrative

This model provides greater flexibility for the placement of the equipment in the network, the packaging of the system, and the capacity it can support. The agencies incur lower CapEx for equipment and lower OpEx because of the resulting efficiencies and the capability to enable newer services, faster deployments, and simplification of network operations. Note that although the focus in this section is on the shared data center, segmentation and virtualization must also be designed across the end-to-end network.
To achieve the segmentation and virtualization requirements, some foundational steps must be implemented across the entire network, which require that branch and campus locations be designed with proper security, segmentation, and QoS. The WAN connection that connects these dispersed sites must also support VRFs to isolate traffic as shown in the above diagram. Inside the data center, access to storage and servers is preserved through the traffic separation. As we design the virtualization and segmentation, we must also pay attention to the fundamental elements of access control, path isolation, and the services edge.

<table>
<thead>
<tr>
<th>Role</th>
<th>Function</th>
</tr>
</thead>
</table>
| Access Control        | Authenticate client (user, device, application) attempting to gain network access  
|                       | Authorize client into a partition (VLAN, ACL)                              
|                       | Deny access to unauthenticated clients                                    |
| Path Isolation        | Maintain traffic partitioned over Layer 3 infrastructure                   
|                       | Transport traffic over isolated Layer 3 partitions                        
|                       | Map Layer 3 isolated path to VLANs in access and services edge            |
| Services Edge         | Provide access to services described through the intelligence layer       
|                       | Make decision on shared versus dedicated resource                         
|                       | Apply policy per partition                                                
|                       | Isolate application environments if necessary                             |

Other issues to consider when designing a shared data center include:

- Components of the network infrastructure should all be VRF-aware. VRF is critical to enable the isolation of virtual traffic flows across a shared physical infrastructure.
- Determine if the service modules providing the services edge are able to support multiple and isolated user bases. Products such as the Cisco ACE blade support this scenario.
- Define each functional domain clearly and independently while establishing a clear hand-off between each domain across the end-to-end network.
- Ensure that self-defending network principles are implemented throughout the network including the
data center.

1.5.4 Network Intelligence

Network intelligence in the data center and across the network enables agencies to maximize the efficiency of data center consolidation. The aggregation layer services provided through intelligent service blades enables enhanced functionality. For example, in a shared environment, some important decisions must be made regarding resource management and application acceleration of the assets in the data center, so that each agency receives the service-level agreements (SLAs) they expect. The capability to allocate resources or optimize TCP traffic flows delivers network traffic efficiencies and allows servers to spend more processing time on applications. Another critical factor in network intelligence is delivering secure operations to data and server access.

The table below lists capabilities to consider regarding network intelligence.

<table>
<thead>
<tr>
<th>Role</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stateful firewalls</td>
<td>The firewall service modules (FWSM) can support the firewall services for multiple agencies in a scalable and efficient manner. The blade provides for Layer 4-7 defense methods and secures IP service integration. The blade tracks the status of all network communication and prevents unauthorized access.</td>
</tr>
<tr>
<td>Content caching</td>
<td>The content switch services (CSS) and content switch module (CSM) provide efficiencies for content management for dedicated agencies</td>
</tr>
<tr>
<td>Intrusion detection</td>
<td>The IDSM-2 blade is highly scalable and helps provide business continuity for the shared data center against intrusion-based threats. The blade integrates with Trend Micro outbreak prevention services</td>
</tr>
<tr>
<td>Server load balancing and Secure Socket Layer (SSL)</td>
<td>The ACE module provides functions for server load balancing (SLB), SSL offload, and some native security functions to consolidate functions into a single blade to serve multiple agencies</td>
</tr>
<tr>
<td>DDoS protection</td>
<td>The traffic anomaly detector service module monitors traffic flows to detect abnormal behavior due to DoS attacks. It works in conjunction with the anomaly guard service module to mitigate DoS attacks by filtering the abnormal behavior traffic while allowing normal traffic to continue to the shared data center. These service modules provide a vital resource to all agencies of the shared data center into protecting against attacking traffic toward the data center</td>
</tr>
<tr>
<td>Application acceleration</td>
<td>The main goal of the following service blades is to make applications and servers more scalable by providing greater control, increasing performance, adding additional layers of security, and simplifying the infrastructure. ACE offers a truly virtualized service blade to support multiple agencies. Application velocity system (AVS) is offered for dedicated agencies through an appliance. AVS provides:</td>
</tr>
<tr>
<td></td>
<td>• Performance and latency reduction for WAN deployments of Web applications to improve user response times</td>
</tr>
<tr>
<td></td>
<td>• Optimization of data communication to help reduce bandwidth of Web applications and assist the server by offloading low-level communications like TCP and SSL transactions</td>
</tr>
<tr>
<td></td>
<td>• Security strength adding to the Cisco Self-Defending Network framework through SSL encryption and decryption, directional deep inspection, white-</td>
</tr>
</tbody>
</table>
### Detailed network traffic analysis

The network analysis module (NAM) gives agencies enhanced visibility into traffic flows to a data center. This correlative data provides tools to proactively resolve problems and manage valuable network resources. For real-time applications such as voice and video supported by the servers in the data center, the NAM blade provides real-time and historical data to help with fault isolation and measurements for response times to critical servers. For a shared infrastructure, this visibility enables data center operations to function with optimal performance.

### 1.5.5 Network Security

Security threats must be taken very seriously when network assets are concentrated in a data center. From an attacker perspective, the data center is an attractive target since the damage has a broad impact. However layers of defense in the data center and across the end-to-end network can detect attacks, rapidly report them, and mitigate them without any impact to operations.

Security components that provide layers of defense to enable the mandatory protection for a shared data center include:

- Inherent network security features built into products at both the hardware and software level that help ensure component reliability when under attack. For example, Cisco NetFlow is built into many Cisco products and provides detailed data about network traffic flows that can be used for statistical profiling, even for day-zero attacks.

- A general approach should factor in methods to:
  - Secure the router and router services
  - Secure the control plane
  - Secure the data plane
  - Define a logical methodology to handle and mitigate known threat types

- Security Monitoring, Analysis, and Response System appliances combine network intelligence, context correlation, vector analysis, anomaly detection, hotspot identification, and automated mitigation capabilities allowing managers to accurately identify, manage, and eliminate network attacks and maintain compliance with policies. These appliances also help track a broad array of security measures by monitoring operations and managing security information. These appliances centrally aggregate logs and events from a variety of devices, including routers and switches, security devices and applications, hosts, and network traffic. They capture thousands of events, efficiently classify incidents using data reduction techniques, and compresses the information for archiving. A key source of data is the NetFlow information from routers and switches in the network.

- Access control should be provided:
  - A “Security Agent” to check the operation of the application against the application’s security policy, making a real-time allow-deny decision on its continuation and determining if logging the request is appropriate.
  - A Network Admission Control (NAC) to ensure every device connected to a port adheres to the
established policies before it is allowed to connect to the network.

- The aggregation layer should provide an intelligent layer of defense. They should be capable to enable firewall, IDS, URL filtering, and DDoS protection services to the agencies supported by the data center. This capability provides virtualization and segmentation of services to the agencies.

- Isolation of traffic specific to an agency is an important tool to compartmentalize any agency-specific security threats to only that agency. Traffic separation ensures that other agencies of a shared infrastructure are unaffected. The tools of the targeted agency deployed by the shared infrastructure provide the necessary mitigation schemes to handle the localized threat.

### 1.5.6 Server Fabric

The server fabric provides the performance and control necessary to access the applications and servers in a shared data center. From a shared infrastructure perspective, the server fabric virtualizes physical components such as I/O and CPU and provides policy-based dynamic resource allocation to the assets.

For management of the policies used by the server switch, VFrame director or third-party software provides the rules. Based on the rules assembled, the virtual server then acts upon policies such as:

- Selecting server(s) that meet minimum criteria (e.g., CPU, memory)
- Booting server(s) over the network with appropriate application or operating software image
- Creating virtual IPs in servers and maps to VLANs for client access
- Creating virtual host bus adapters (HBAs) in servers and maps to zones, logical unit numbers (LUNs), and worldwide node names (WWNNs) for storage access

The blade servers that operate on the server fabric greatly benefit server consolidation. Servers that may be dispersed across multiple locations and at hard-to-manage locations can now be centrally placed in the blade servers. A well-designed shared data center architecture is critical to server consolidation, which translates to reduced management, reduced infrastructure for space and power, and maximum utilization of the active servers.

### 1.5.7 SAN Fabric

The SAN fabric handles the connectivity in the data center from the network to the storage farms. Many of these networks were designed around an inefficient full mesh network, yielding poor effectiveness on port count and thereby driving up the total cost. A more structured design using a traditional core/edge design or collapsed core design that combines the core and edge layers helps reduce the complexities and drive more effective use of the ports.

From a shared infrastructure perspective, the use of a VSAN provides a mechanism to allocate ports within a physical fabric to create virtual fabrics. Conceptually, the VSAN model is analogous to VLANs in an Ethernet. The virtual segments are isolated to provide secure access to the storage data. To enhance the isolation, events that are generated in the fabric are segmented per VSAN, so statistics can be gathered on individual VSANs, which can help identify failure scenarios. With hardware-based capabilities, membership in the VSAN can be explicitly tagged on interswitch links. The cost of a physical redundant fabric can drive up costs. By providing virtual allocation to these resources, wasted ports are reduced.
2. Design Considerations
2. Design Considerations

Networks today are global and critical to the core operations of business and society. As such, it is important that their characteristics be understood by the network administrators. It takes many providers, partners, and vendors to establish and maintain the global network ecosystem we all depend on daily. Therefore it is critical that all participants in the network know and understand their role and expectations as it relates to network characteristics. It is also important that the networks be actively managed to assure network availability, reliability, and performance.

2.1 Security

Security can no longer be treated as an afterthought when it comes to network and datacenter design. Trial-and-error networking is not an option, as a single vulnerability could compromise the organisations’ lifeblood, the network. There are challenges in offering encryption, certification, directory, network, and other security components that enable what one would consider a 100 percent secure network. While industry struggles with developing the technology to provide these protective components, the IT manager must still cope on a daily basis to reduce the network's imminent risk.

A complete network security solution includes

- authentication,
- authorization,
- data privacy,
- and perimeter security.

Perimeter security is traditionally provided by a firewall, which inspects packets and sessions to determine if they should be transmitted or dropped. In effect, firewalls have become a single point of network access where traffic can be analyzed and controlled according to parameters such as application, address, and user for both incoming traffic from remote users, and outgoing traffic to the Internet.

In general, firewalls are intended to protect resources from several kinds of attacks such as passive eavesdropping/packet sniffing, IP address spoofing, port scans, denial-of-service (DoS) attacks such as SYNchronize-ACKnowledge attack (SYN flooding), packet injection, and application-layer attack.

The best practices checklist section ensures that security considerations are effectively incorporated within the network design.

2.1.1 Shared Security Services

Security is a process, not a product. Security should be built into the overall architecture from the beginning. After you determine the appropriate security measures required to secure assets, you should continuously monitor and re-evaluate to ensure that new threats are addressed. The Security Wheel, illustrates this continuous process based on a foundational security policy and incremental improvement.
Managing security risk and compliance audit requirements requires a system-based best-practice approach to controls. The network itself plays a fundamentally important role in achieving these objectives because it touches every aspect of the IT infrastructure. The point-product architectural model has become inadequate for managing today’s network security risk, compliance, and audit requirements. An end-to-end, systems-based approach aligned with industry frameworks and best practices is required. It should be integrated, collaborative, and adaptive—an approach that helps administrators better manage network security risk while enabling auditors to satisfy internal and external compliance requirements. A “Self-Defending Network Definition” provides an approach, managing network security risk and supporting industry control frameworks such as Control Objectives for Information and related Technology (COBIT) and ISO 17799 best practices. This approach helps an organization better manage its network security risk while readying it to meet regulatory compliance.

2.1.2 Shared Infrastructure Security Risks

The vast majority of today’s government agencies are increasingly dependent on automated business processes. Information systems and the networks that support them are now viewed as strategic assets based on their ability to contribute to the overall strategy and objectives of the business, the level of investment and resources committed, and new security risks that must be managed.
As a result, network and security administrators must find new ways to protect networks—and the data and applications they carry—from attacks that are faster, more complex, and more dangerous than ever before. But the historical point-product approach makes it difficult to acquire, deploy, and operationalize the security controls necessary to protect the enterprise infrastructure. As a result, trade-offs must often be made and organizations are forced to tolerate unacceptable levels of risk.

All organizations now face growing compliance demands, as regulations and public insistence require that appropriate steps be taken to ensure the proper use and protection of government, corporate, and personal information.

Historically, the approach to managing network security risk and compliance audit requirements has been fragmented across organizational divisions and departments, resulting in a duplication of effort and technology. Inevitably these different approaches are inconsistent and control systems overlap, contradict, or undermine one another. Measurement and reporting are equally fragmented, resulting in administrators not knowing whether they are efficiently and effectively managing network risk, including emerging compliance requirements (http://www.itcinstitute.com/display.aspx?id=465). Not surprisingly, according to Forrester Research, businesses now seek a formalized, consistent approach to managing information risk and compliance requirements across the entire organization (Forrester, Trends 2005: Risk and Compliance Management, October 25, 2004).

In a shared service and/or network infrastructure environment, security does not have to be minimized to offer such services. Each tenant on the network, whether a department, subagency, customer, or guest, has specific security requirements that can be met in a shared environment.

To enhance the overall network security, the service provider, the GIDC in this case, could offer a service to the tenants that updates the virus protection software on the computers prior to allowing access to the network. By sharing a network infrastructure and services with other departments and agencies, the GIDC could improve the security of the information while providing timely access and improved collaboration.

This is a brief overview of the current security environment. By leveraging common shared services, it allows a more comprehensive security plan to be implemented and maintained by the line of business best equipped to manage it. Many of the same policies and requirements can be implemented on a customer-by-customer basis, which gives individual customers the autonomy to implement additional security measures if required.

2.1.3 Network Security In a Secure Segment

In a shared infrastructure, you do not have to sacrifice control of your security policies and requirements. From the provider’s view, once your traffic is segmented, you have a secured network since your traffic is being transported virtually separate from other network traffic. If you want to increase security, consider that the implementation of some security techniques may prevent the implementation of other traffic management techniques discussed in this chapter. If additional security is required, the network provider should be consulted, as it may affect how your network is designed and implemented. It may also affect what shared services are available.

For example, if the GIDC is providing a network (SWAN), it may create a VPN or provision a circuit-based link through its network for a sub agency. In doing so, it secured the sub agency’s traffic from everyone else’s traffic. However, the sub agency can implement IPSec to further encrypt network traffic. This allows every sub agency packet transiting the GIDC’s network to be encrypted to the sub-agency’s standards. This is relevant since we have national security and police department as possible customers.

Routers can combine security and network functions in a single device, independently delivering VPN, stateful firewall, intrusion protection, and URL filtering in addition to full-featured IP routing. Depending on budget constraints, traffic load, security requirements, and service load, this may or may not be a desirable feature.
Careful consideration should be given when deploying services. Each service feature will require processing power that could have a negative effect on performance if traffic loads are heavy.

<table>
<thead>
<tr>
<th>Context</th>
<th>Feature / Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Services</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **Stateful Firewall**    | • Stateful firewall engine—Performs deep packet inspection maintaining state information per application  
                              • Threat detection and prevention—Denial-of-service detection and prevention, Java blocking, Simple Mail Transfer Protocol (SMTP) attack detection, IP fragmentation defense  
                              • URL filtering support—Web browsing control and auditing through URL filters, including Content Engine Network Module, N2H2, and WebSense  
                              • Voice traversal—Firewall recognizes and secures multiple voice protocol traffic, including H.323, and Session Initiation Protocol (SIP)  
                              • Multimedia application—VDO Live, RealAudio, Internet Video Phone (H.323), NetMeeting (H.323), NetShow, CuSeeMe, Streamworks  
                              • Advanced applications—SQLNet, RPC, BSD R-cmds, ICMP, FTP, TFTP, SMTP, and common TCP/UDP Internet services  
                              • AAA integration—Supports separate security policies per user, interface, or sub-interface |
| **Intrusion Protection** | • Matches network traffic against malicious patterns  
                              • Enhanced performance—Combines with stateful firewall to perform deep packet inspection with a single lookup  
                              • Inline operation (shunning)— Resets connections with malicious code attacks, providing protection to end users  
                              • Alarm management  
                              • Authentication, authorization, and accounting (AAA) support—Authenticates and authorizes end users through an AAA server  
                              • Worm blocking—Rules-based pattern matching provides preliminary inspection of known malicious code with the ability to reset connections  
                              • Anti-virus proxy—Complements anti-virus software by caching the cleaned objects and using them in subsequent hits, thereby increasing anti-virus performance |
| **URL Filtering**        | • Integrated SmartFilter URL filtering provides web surfing control and auditing, protecting against legal liabilities, preserving network bandwidth, and improving productivity  
                              • Interoperability with N2H2 and WebSense URL filters |
| **Trust and Identity**   | • CNS bootstrap call home—Forces newly-provisioned remote routers to “call home” to management server, greatly simplifying large-scale deployments  
                              • Public key infrastructure (PKI) support—Digital certificates that can be used to authenticate routers, providing greater scalability and security  
                              • Management tunnel—Allows periodic audit checks to ensure configurations have not been tampered with. Allows for a clean separation and outsourcing of management function  
                              • Secure RSA private key—Guards against router being stolen or misused; private key is erased if password recover attempted  
                              • PKI and AAA integration—Credentials stored centrally on an AAA server, allowing quick addition and deletion of devices with a single entry.  
                              • DNS secured IP address assignment—Device-level protection against IP address hijacking |
<table>
<thead>
<tr>
<th>Feature / Benefit</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Integration</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Voice and Video Enabled Virtual Private Network</strong></td>
<td></td>
</tr>
<tr>
<td>Multi-service-centric quality of service (QoS)—Delivering toll-quality voice and video services requires QoS that addresses end-to-end transport quality. Low-latency queuing provides a foundation for prioritizing multiservice traffic and delivering specific bandwidth and latency guarantees. Relevant devices should provide comprehensive low-latency queuing capabilities, including features specific to encrypted voice and video traversing the VPN. Furthermore, features like traffic shaping to ensure quality on asymmetric link speeks and link fragmentation and interleaving (LFI) to control jitter in the presence of large packet transmissions like FTP are critical and desirable to ensuring voice and video quality on the VPN.</td>
<td></td>
</tr>
<tr>
<td>• Support for diverse traffic types—IP video traffic and voice traffic like hoot and holler and music on hold require support for multicast traffic across the VPN.</td>
<td></td>
</tr>
<tr>
<td>• Support for multiservice network topologies—Because multiservice traffic is latency sensitive, network topologies must often be adapted to reduce network hops and minimize latency. Furthermore, VPN routers should offer embedded software features such as Dynamic Multi-Point VPN that provide automated, dynamic provisioning of meshed networks for ease of deployment.</td>
<td></td>
</tr>
<tr>
<td>• Enhanced network failover capabilities—Should provide comprehensive resiliency, addressing both VPN network transport and the IP telephony network. Should have full Layer 3 routing and stateful VPN failover capabilities. This eliminates network black holes. Survivable Remote Site Telephony (SRST) features for remote offices provide telephony-specific resiliency to ensure the voice network continues operating in the event of lost connectivity to the headquarters site are also desirable.</td>
<td></td>
</tr>
<tr>
<td><strong>Dynamic Multi-Point VPN (DMVPN)</strong></td>
<td></td>
</tr>
<tr>
<td>Virtual full mesh—Allows IPSec with routing protocols to be dynamically configured</td>
<td></td>
</tr>
<tr>
<td>On-demand spoke-to-spoke tunnels—This capability optimizes performance and reduces latency for real-time traffic</td>
<td></td>
</tr>
<tr>
<td>Dynamic discovery of spoke-to-hub tunnels—Minimizes hub configuration and ongoing updates when new spokes are added</td>
<td></td>
</tr>
<tr>
<td>QoS, multicast support—Required for latency-sensitive applications such as voice and video</td>
<td></td>
</tr>
<tr>
<td>Tiered DMVPN—Allows preferential treatment of users and simplifies configuration</td>
<td></td>
</tr>
<tr>
<td>Enhanced scalability—Load balancing doubles the performance compared to passive failover. Single hop to go from spoke to spoke reduces overhead on the system; tiered DMVPN extends scalability.</td>
<td></td>
</tr>
<tr>
<td><strong>IPSec-to-MPLS integration</strong></td>
<td></td>
</tr>
<tr>
<td>VRF-aware IPSec—Terminates multiple customer edge IPSec tunnels onto a single provider edge VRF interface, reducing CapEx</td>
<td></td>
</tr>
<tr>
<td><strong>IPSec NAT Transparency</strong></td>
<td></td>
</tr>
<tr>
<td>Allows encrypted IPSec traffic to traverse Network Address Translation (NAT) or Port Address Translation (PAT) devices by wrapping IPSec within User Datagram Protocol (UDP), simplifying VPN design and deployment</td>
<td></td>
</tr>
<tr>
<td><strong>High Availability</strong></td>
<td></td>
</tr>
<tr>
<td>IPSec stateful failover—Provides subsecond failover that provides reliability for mission critical application such as Systems Network Architecture (SNA), voice, and databases. Scales to thousands of remotes. Fewer help desk calls from end users in the event of a head-end failure.</td>
<td></td>
</tr>
</tbody>
</table>
### Context

<table>
<thead>
<tr>
<th>Feature / Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>- DMVPN load balancing and self-healing—Doubles the performances compared to passive failover while providing resiliency. Reroutes around link failures and maximizes up time.</td>
</tr>
<tr>
<td>- Easy VPN failover—Ability to failover to multiple backup peers successively</td>
</tr>
</tbody>
</table>

### Management

**IP Solution Center**
- Policy-based management; should scale to large number of devices
- Multiple VPN deployments—Site-to-site VPN, remote access VPN, DMVPN, Easy VPN
- PKI-based end-to-end authentication and audit checks
- Device abstraction layer—Should allows policy rules to be created independent of devices and later pushed to different device implementations, such as the Cisco IOS firewall
- Bootstrap call home—Should force newly-provisioned routers to call home to management server, get authenticated, and receive their digital certificates and policies
- Hub-and-spoke, full and partial mesh topologies
- Design and deploy complex firewall rules
- Should provide provisioning and tuning of network devices
- Integrated routing—Open Shortest Path First (OSPF), Enhance Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP)
- Automate provisioning of failover and load balancing
- QoS provisioning
- Should provide for massive NAT configuration deployment
- Service provisioning—Network-based IPSec, MPLS, managed firewall, and managed IDS

**Security Management System**
- Policy-based management
- Should combine Web-based tools for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network- and host-based IDS
- Device hierarchy and policy inheritance
- Should allows a large number of firewalls to pull security configurations and update themselves easily and quickly
- Centralized role-based access control enables different groups to have different access rights across different devices and applications
- Integrated monitoring of network device syslogs and events from network- and host-based IDS, along with event correlation

### 2.2 Availability

Availability is generally ensured by the overall network design and implemented in several ways.

First, networks are designed with steps to minimize the occurrence of service problems and the time to recover from problems (such as backup recovery policies).
Second, high availability must be considered at each layer of the Open Systems interconnection (OSI) reference model, with redundancy and failover provisions made at the physical, data link (for example, Ethernet), network (for example, IP), and application layers.

The most effective solutions are those with consistent engineering considerations tightly integrated throughout the data center, rather than those approached with a series of “point-solution” products and techniques.

### 2.3 Scalability

Scalability must be provided in every data center. Server load balancing is the norm, and techniques such as reverse proxy caching are often used to offload servers. Server load balancing, like other aspects of data center design, must also be content-aware, preferably using delayed binding, full URL and cookie inspection, and “sticky (server) connections” as part of the logic of choosing a server for each user request.

Specific content may be in high demand and considered “hot.” Because this content may not be known in advance (such as breaking news stories), advanced data centers should also have the ability to automatically and immediately identify and replicate hot content to overflow or backup servers or cache to ensure the ability to support the increased demand without compromising performance.

#### 2.3.1 Network Virtualisation – Services Edge Design

The centralization of access to shared services provides a common point of policy enforcement and control for all VPNs. This is referred to as the services edge functional area. Services edge has more of a logical than a physical meaning. In a specific network design, the point of policy enforcement can be physically located in a specific area of the network, but in certain cases, it might also be spread around the network.

The term network virtualization refers to the creation of logical isolated network partitions overlaid on top of a common enterprise physical network infrastructure, as shown in figure below.

Each partition is logically isolated from the others and must provide the same services that would be available in a traditional dedicated enterprise network. This essentially means that the experience of the end user is that
of being connected to a dedicated network that provides privacy, security, an independent set of policies, service level, and even routing decisions.

At the same time, the network administrator can easily create and modify virtual work environments for the various groups of users, and adapt to changing business requirements in a much easier way. The latter derives from the ability to create security zones that are governed by policies enforced centrally. Because policies are centrally enforced, adding users and services to or removing them from a VPN requires no policy reconfiguration. Meanwhile, new policies affecting an entire group can be deployed centrally at the VPN perimeter. Thus, virtualizing the enterprise network infrastructure provides the benefits of leveraging multiple networks but not the associated costs, because operationally they should behave like one network (reducing the relative operating expenses).

Network virtualization responds to both simple and complex business drivers. As an example of a simple scenario, an enterprise wants to provide Internet access to visitors (guest access). The stringent requirement in this case is to allow visitors external Internet access while preventing any possibility of connection to the enterprise internal resources and services. This can be achieved by dedicating a logical “virtual network” to handle the entire guest communications. A similar case is where Internet access can be combined with connectivity to a subset of the enterprise internal resources, as is typical in partner access deployments.

Another simple scenario is the creation of a logical partition to be dedicated to the machines that have been quarantined as a result of a Network Access Control (NAC) posture validation. In this case, it is essential to guarantee isolation of these devices in a remediation segment of the network, where only access to remediation servers is possible until the process of cleaning and patching the machine is successfully completed.

As an example of a more complex scenario, an enterprise IT department starts functioning as a service provider, offering access to the enterprise network to a variety of “customers” that need to be kept logically isolated from each other. Users belonging to each logical partition can communicate with each other and can access dedicated network resources, but inter-communication between groups is prohibited.

The architecture of an end-to-end network virtualization solution that is targeted to satisfy the requirements listed above can be separated in three logical functional areas:

- Access control
- Path isolation
- Services edge

Each area performs several functions and interfaces with the other functional areas to provide a complete integrated end-to-end solution.

The virtualization of the enterprise network allows for the creation of a separate logical network that is placed on top of the physical infrastructure. The default state of these virtual networks (VPNs) is to be totally isolated from each other, in this way simulating separate physical networks.

This default behavior may need to be changed when the various VPNs need to share certain services, such as Internet access as well as network services such as DHCP and DNS, and server farms.

This section presents alternative ways to accomplish this sharing of resources between various VPNs. The services that need to be shared are discussed, as well as the distinction between protected and unprotected services. This section broadly categorizes services that are shared by many VPNs as either protected or unprotected, depending on how they are accessed.
Various technologies are discussed that achieve the sharing of resources between different network partitions.

**Services Edge – Scope of Information**

The services edge portion of the overall network virtualization process is where a large part of policy enforcement and traffic manipulation is done. Before the services edge is implemented, it is important to thoroughly understand which methodology is to be deployed and what the trade-offs are for selecting the methods described in this section. It is also important for customers to understand their applications and their associated traffic flows to help in the overall network optimization process.

This guide accomplishes the following:

- Provides guidelines on how to accomplish the integration of multi-VPN Routing and Forwarding (VRF) solutions into the data center core layer while using the core nodes as provider edge (PE) routers.
- Presents implementation options for providing shared services in a multi-VRF environment
- Distinguishes between protected and unprotected services, and discusses the design of the services edge to allow shared access to the most typical shared resource, which is the Internet.
- Describes the use of web authentication appliances to authenticate and authorize users before permitting Internet access. This is a common requirement in the enterprise arena when providing guest access services to visitors, but can also be leveraged in various contexts.

Although this guide addresses many technical areas, it does not address during this phase of the network virtualization project the following areas:

- Placing of voice services or multicast services into a VRF.
• Use of overlapping IP addresses in the VRFs. IP address overlap may be addressed in the future; the major reason for not addressing it in this guide is because of the operational impacts that this causes to customer networks in the operations and management aspects of the network infrastructure.

**Unprotected Services**

An unprotected service is a service that can be accessed openly without subjecting the traffic to any type of security check. An unprotected service is reachable from one or more VPNs without having a policy enforcement point between the service and the requesting host. The best path routes to reach an unprotected service can be present in the various VPNs that can access the service.

In general, this type of access is used to provide shared DHCP or DNS services to the various VPNs without adding an unnecessary load to the firewalls that are being used to control access to other shared services that must be protected.

**Protected Services**

Protected services must be accessible from the VPNs, but only after specific security policies are enforced. To be able to enforce the necessary security policies in a manageable way, access to the services must go through a policy enforcement point. Thus, all traffic reaching the services must be routed through a common point of policy enforcement. As a result, the routing between a requesting host and a service can potentially be less than optimal. However, this is true only in very specific scenarios, such as when the shared services themselves are part of a VPN. In general, shared services that are to be protected are centrally located for optimal accessibility.

Examples of protected services include server farms and the Internet. When accessing the Internet, not only is it necessary to control access to the service from the VPNs, but it is also critical to control any access initiated from the service area towards the VPNs. Ideally, none of the VPNs should be accessed from the Internet; thus access into the VPNs from the services area is generally prohibited.

In cases where VPNs must communicate with each other in a controlled manner, the policies at the VPN perimeter can be changed to provide such access. In this particular inter-VPN connectivity application, the policies must be open to allow externally-initiated communication into the VPNs.

**2.3.2 Integrating a Multi-VRF solution into the Data Center**

One of the most common implementations of a multi-VRF solution is in data center consolidation, which allows multiple applications to reside in one central facility and to share a common WAN infrastructure that services more than one customer segment.

Benefits of this solution include the ability to consolidate data centers during a merger or acquisition, or the ability to offer tenant-type services for various locations. This solution allows the common WAN infrastructure to be virtualized across multiple departments or customers, and allows them to maintain separation from their data center resources all the way to their branch locations.

The actual implementation of this solution requires that the core nodes be treated as the PE routers if you are using a Multiprotocol Label Switching (MPLS) network. The reasons for not extending the core routing further into the data center are that doing so introduces core routing into the facility, and thus reduces convergence times in the event of a physical link problem in the data center. It also mandates the use of a larger memory pool to support the data center Interior Gateway Protocol (IGP), Border Gateway Protocol (BGP) for MPLS reachability, and then the actual VRF route tables. This can limit platform selection by the customer and also affect services deployment in the data center.

Terminating the VRFs on the PE routers in the core maintains a clean separation of the WAN/data center. (See figure below) This eliminates the need for appliances or services modules to become VRF-aware, which can potentially impact the data center design as it scales to support a larger server install base as servers are consolidated. This is because many services appliances and services modules are not currently MPLS VRF-aware.
Sub-interfaces are used for the VRFs because it is assumed that the global table will be the existing network for a customer seeking to deploy a virtualized network. Creating the virtualized network out of sub-interfaces avoids the need to make changes to this table, and there is no impact to the global table as you migrate to this new environment.

2.3.3 Shared Services Implementation in the Data Center

Implementation of shared services in the data center treats the services to be shared no differently than any other VLAN or VPN defined, with the exception that this VPN exports its routes to most if not all of the other VPNs that exist in the network. The shared services VRF also needs to statically route into the global table until software support allows for importing and exporting of routes from the global table into a VRF. Using import and export commands allows the data center to act as the central policy enforcement area and to create a high capacity exchange framework between all VPNs, whether or not they need to reach services. The idea here is to use access control lists (ACLs) to act as a first line of policy enforcement to allow VPNs to communicate to each other. Then within each VPN or VLAN, you can use the FWSM and ACE and their individual context capability to further manipulate traffic.
Careful consideration must be made in the distribution layer in the allocation of VLAN assignments and the termination of the VRFs. It is important to understand the service chaining needed for each customer environment and whether policies can be shared. If transparent operation mode is to be implemented, you must ensure that Bridge Protocol Data Unit (BPDU) forwarding is enabled in both the FWSM and the ACE module. The next consideration is how to allow the shared services to be used by users in the global route table, and then the individual Customer VRFs.

The simplest method for doing this is to use simple static routing into the global table.
After the services are working with the global table, the next area to address is sharing services between the VRFs. Again, this is accomplished through the use of export and import commands on the individual VRFs. The important thing to consider here is what are the application interdependencies, and whether any unique traffic patterns might dictate using shared versus non-shared resources. Before doing this, thoroughly examine the customer application environment to ensure that resources are positioned correctly for application optimization.

As an example, assume a customer has a home-grown application that relies heavily on DNS and Layer 2 communications between several organizations servers. It would not be advisable to insert Layer 3 boundaries into this environment until you can determine what the impact would be to the application.

The other method of allowing communication between the VPNs is to implement a data center fusion VRF to allow for shared Internet access.
This method has the advantages of allowing every VRF that would need access to the shared services to have their own service chain created and thus their own shared services policy implemented. Depending on the services contained in the shared services VRF, this can be either advantageous or unnecessary.

### 2.3.4 Virtualised Internet Edge Design – Shared Internet Access

To allow secured communication between each VPN and the Internet, it is necessary to create unique points of ingress and egress to each defined virtual network. This can be achieved by configuring the routing inside each VPN to forward traffic destined outside the VPN to a specific gateway. When traffic reaches this gateway, it can...
be controlled by means of ACLs, firewalls, intrusion detection systems, or any other in-band security mechanisms that are considered necessary.

This is the equivalent of treating each VPN as if it were a physically separate network. Separate networks connecting to a common resource must have a security device head-end to control access to the network. The device typically used for this is a firewall. When accessing the Internet, the place in the network where such a firewall is deployed is known as the Internet edge. The figure below illustrates a typical perimeter deployment for multiple VPNs accessing common services.

In the above network diagram, it is assumed that a separate VRF instance for each VPN is defined on the PE device in the Internet edge. However, a similar design where distributed ACLs are the mechanism deployed for path isolation can also be used in the scenario. In that case, no VRFs are defined and the traffic might be steered to a separate firewall by using policy-based routing (PBR).

As seen in the above figure, each VPN is head-ended by a dedicated firewall. This allows for the creation of security policies that are specific to each VPN, independent of each other. To access the shared services, all firewalls are connected to a fusion router. The fusion router can provide the VPNs with connectivity to the Internet or inter-VPN connectivity. Separate load balancers can also be deployed per VPN to create a complete service chain on a per-VPN basis (this is more relevant when deploying this model for accessing shared resources located in a data center).

The use of a fusion router raises two main concerns: the potential for traffic leaking between VPNs, and the risk of routes from one VPN being announced to another VPN. Having dedicated per-VPN firewalls prevents the leaking of traffic between VPNs through the fusion router by allowing only established connections to return through the VPN perimeter. It is important to configure the routing on the fusion device so that it does not advertise the routes from one VPN to another VPN.

The additional firewall shown in the above figure, separating the fusion area from the Internet, is optional, and is used to keep common services or transit traffic in the fusion area protected from the Internet.

The information in the following section, even though largely focused on providing Internet access, can be generalized to provide access to any resource external for a VPN. An external resource can also include resources in other VPNs; thus a resource in VPN A is considered an external resource for VPN B and it is therefore accessed through the secure VPN perimeter. This scenario is illustrated in following Figure.
The use of service chaining allows for each VPN to have its own internal policy domain. This same service chaining can easily be applied to the fusion VRF to allow for a common policy to be applied to all users going to the Internet. This in effect simplifies the internal VPN policies because you can layer security and load balancing solutions instead of having to create a new policy for each VPN.

As the number of VPNs increases, head-ending each VPN onto its own firewall can become expensive and hard to manage. Firewalls can be virtualized, and therefore offer a separate context for each VPN on the same physical appliance. The resulting topology is shown in the Figure below. Note that a single physical firewall provides a dedicated logical firewall to each VPN.
The concept of virtual firewalls or firewall contexts has been implemented on Cisco firewall appliances, as well as in the integrated FWSM for the Cisco Catalyst 6500. The integration of the firewall functionality onto the PE platform allows the topology shown to be consolidated onto a single physical device, as shown in the below figure. The logical topology remains unchanged. The firewall functionality is carried out by an FWSM within the PE, and the fusion router is implemented by the creation of a VRF inside the same PE. Also note, how the fusion VRF acts as a separate router.

To provide a resilient solution, we recommend deploying a redundant pair of PE devices in the Internet edge, and equipping each one with its own firewall module.

The routing between the fusion router, the various contexts, and the VPNs must be configured with care. Because of its place in the topology, the fusion router has the potential to mix the routes from the various VPNs when exchanging routes dynamically with the various VPNs. The following two scenarios to prevent this can be considered, depending on the mode of operation of the firewall:
- Firewall in routed mode
- Firewall in transparent mode

It is recommended to deploy the Internet edge separately from the data center shared services design. In effect, this creates two separate policy domains that can be layered together to create a stronger overall security posture. Inter-VPN traffic should be handled as outlined previously concerning how to share traffic between VPNs, and Internet edge traffic should be handled as a separate use case.

2.3.5 Firewall In Routed Mode

When configured for multiple contexts, the firewall in routed mode supports only static routing, so the mixing of VPN routes is not a concern. Connectivity between VPNs is achieved by the sole configuration of the fusion router. However, the firewalls are configured to allow only established connections (only connections that are initiated from inside of the firewall). Thus, all VPNs can reach the fusion router, and the fusion router can return traffic to all the VPNs. However, the VPNs are unable to communicate with each other through the fusion router unless very specific policies are set on the various firewall contexts to allow inter-VPN communication through the VPN perimeter gateway.

The static routing configuration for the perimeter gateway is illustrated in the figure below. Details are provided for one VPN only; other VPNs require similar configuration. Note that Network Address Translation (NAT) can be used in this configuration because the firewalls are in routed mode, and this allows support for overlapping IP addresses in various VPNs.

2.3.6 Firewall In Transparent Mode

Deploying the firewalls in transparent mode simplifies the routing, and allows the complete functionality to be achieved by IGPs, as shown in the figure below.
The fusion router adds a default route into the IGP that is enabled in the context of each VRF. Because of the bridged nature of the firewalls, it is possible to establish the peering between the VRFs and the fusion router directly with an IGP. It is not possible to use the firewalls for NAT, so all VRFs must use valid and unique IP address spaces (no support for overlapping IP addresses).

This configuration is very simple and consists of the following steps. This is a standard Internet edge configuration and it must be done for each VPN.

### 2.4 Manageability

Manageability means much more than simply knowing if a server or other network element is “up or down.” Especially in service provider data centers supporting multiple customers (which in this case would be the different government departments), the ability to assess service levels on a per-customer basis is essential to the offering and administration of service-level agreements (SLAs). Managing IP address assignments, keeping track of network configurations, and not losing site of trouble tickets and alarms often requires use of a mechanized network operations center (NOC) support system.

Good manageability tools and qualified personnel supporting the infrastructure translate into lower operations costs, since time is not wasted trying to resolve indications from conflicting management systems and higher customer satisfaction.

#### 2.4.1 Overview and Goals

Network management is an important component of overall network reliability and includes several categories:

- **Configuration management**—Process by which device configurations are standardized and centrally administered.

- **Security management**—Process by which the security policies are implemented, tested, and re-evaluated to ensure the overall network is secure based on agency policy. Policy management is also enforced within the security management framework.

- **Event management**—Process by which individual network elements send status updates (traps) to a management system that then can correlate the alarms and take action based on the policy set for a single event or series of events. Actions such as blinking lights, sounding alarms, sending pages, re-routing traffic, collecting network data, etc. can all be triggered based on how reactive or proactive network management functions are performed.

- **Address management**—Process to manage the IP address space. Policies should be set forth to properly
categorize IP address space by whatever means administration deems effective, such as ensuring subnet masks are correct on the WAN link to ensure there are no wasted addresses or placing various departments in their own subnetworks.

- Application management—Process to ensure the IT department knows what software is resides on the network devices. This helps give technical support a standard frame of reference with regard to release numbers and patch applications.
- Asset management—Process to account for the network assets. There are a variety of means to collect information depending on network element capability.

Each of these processes fosters management of the infrastructure. Proactive management facilitates other processes such as trending, budgeting, support, and configuration. Each one plays a specific role and may interrelate to other management processes to achieve higher reliability and customer satisfaction.

Network management is an art based on science. It relies on individual network characteristics that make up network performance, error, efficiency, and trending analysis. Turning this data into actionable information for managing an agency requires proper monitoring and reporting of data relevant to a specific network. For example, an error report may reveal that network errors occurred during specific times of the day and hence may be related to specific events.

This section describes an option for a robust management infrastructure based on time-proven techniques and operations.

2.4.2 Demarcation Point

This is the physical point where the service provider hands off control/responsibility of the network to the customer. In many cases, customers can choose the demarcation point, allowing them to control as much or as little as they wish. The provider takes measures to ensure that customer changes to equipment cannot affect the operation of the provider’s network. The customer should also ensure that appropriate measures are taken to prevent provider changes from having unexpected adverse effects on the customer’s network operations and administration.

2.4.3 Administration

The provider may or may not allow various levels of administration to the network service equipment based on purchased service capability. In some cases, partial administration may be allowed for customer services.

2.4.4 Service-Level Agreements

A service-level agreement (SLA) is a contract between a service provider (in this case GIDC) and a customer (in this case a ministry or a government department) that defines the terms of responsibility of the provider and consequences if those responsibilities are not met.

Why Are SLAs Important?

SLAs define the attributes for the portions of a network that are not controlled by the customer. This allows the customer to establish expectations for the network such as:

- Availability
- Delay
- Throughput
- Costs
Reliability

Each of these attributes plays a critical role. Providers must engineer their networks to meet SLAs, so as not to incur penalties for network outages or performance issues. It is essential that the different departments using the GIDC services understand all the parameters of the SLA to minimize unexpected problems. For example, it is important to understand if network services can be pre-empted or denied and under what criteria this can occur.

Compliance

Customers must monitor their networks over time to determine whether SLAs are being met. Many performance tools are available for this purpose. Customers must also be aware of where these measurements are taken. It is imperative that performance measurements be taken end-to-end utilizing several performance parameters. Applications today use many protocols and each should be tested and monitored if it is deemed critical to business operations, particularly since not all protocols perform identically across the network or in each segment of the network. Once these parameters are established, the network can be engineered to meet applications’ performance requirements. Note that customers should have a clear understanding of the process to follow when SLAs are not met, as well as the remediation of the non-compliance infraction.

2.4.5 Network Management Architecture

Network management is typically implemented in one of two ways:

- In-band using the data path, as in enterprise/commercial networks
- Out-of-band using a separate network management infrastructure, often found in service provider networks

While in-band network management using Simple Network Management Protocol (SNMP) is very effective for commercial networks, it poses potential security risks in that access passwords are sent in the clear. SNMPv3 attempts to address this vulnerability, however DES or Message Digest Algorithm 5 (MD5) hash does not meet the stringent security requirements of governments.

To meet the security requirements inherent in classified networks, and the security requirements intrinsic to the devices themselves, a dedicated management network, typically referred to as a data communications network (DCN), might be considered for the provider. This can be accomplished by a physically separate link or a VPN tunnel.

A DCN has the ability to provide various levels of security, including physical separation of data and encryption, depending on the sensitivity and location of critical network elements.

What is a DCN?

A Data Communications Network (DCN) is the out-of-band management network that customers’ IT organizations use to provide operations connectivity between the element management systems (EMSs) and network management systems/operations support systems (NMSs/OSSs) systems within a network operations center (NOC) and the respective network elements that they manage. These systems support OAM&P (Operations, Administration, Maintenance, and Provisioning) functions, including network surveillance, provisioning, service restoration, key management, etc. Network elements comprising the provisioned services infrastructure include SDH/SONET add-drop multiplexers (ADMs) and optical repeaters, xWDM optical equipment, voice switches, digital cross-connect systems, Frame Relay or ATM switches, routers, DSL access multiplexers (DSLAMs), digital loop transmission systems, etc.
Building a Foundation for an Optical Transport Network with DCN

The DCN architecture provides out-of-band connectivity between optical network elements and their respective management systems. In addition, the DCN architecture can provide cost-effective connectivity between non-optical network elements and their respective management systems by sharing the same connectivity network with optical. This end-to-end architecture enables NOCs to utilize one operations network (DCN) to connect large numbers of optical and legacy network elements (up to the tens of thousands) to their centralized network operations center housing multiple management systems (CTM is one on them). Virtually all protocol types for both new and legacy technologies are supported, including IP (UDP, TCP), OSI (CLNS, IS-IS, ES-IS, TARP), X.25 (PVC, SVC), BX.25, asynchronous, and discrete alarms. By simplifying the operations network connectivity through consolidation, users can greatly reduce costs of DCN equipment, training, and maintenance while ensuring faster delivery of new services on their network infrastructures.
A proposed DCN diagram using Cisco network components is shown below, however, equivalent components from other manufacturers can also be used.

The traffic that resides on a DCN is very low as it includes only element provisioning, network traffic statistics, SNMP (if desired), key management (if desired), network monitoring (Remote Monitoring, etc.), and real-time element management such as port activation/deactivation, key activation/deactivation, traffic trending, and anomaly detection and reporting, etc. Since this network is considered to be a “closed” network, practically any network element management traffic that the user considers necessary can be placed on the DCN with little risk of security threats.

If desired, additional appliances can be added to enhance the network’s security level, such as encryption. As described, a DCN is nothing more than a traditional out-of-band LAN/WAN network that is used for the sole purpose of managing the network elements of the infrastructure. Unlike in-band management, where network
element traffic coexists with user traffic, network operations has a dedicated link to critical network elements while maintaining the highest level of security required by operational parameters. This also allows for more robust management of the infrastructure since the management has no effect on user application performance.

The proposed DCN architecture is based on a three-tiered architecture consisting of backbone, distribution, and access elements. As illustrated below, the backbone contains WAN switches that form a core or transport function. The second tier consists of switching centers or distribution routers located around the backbone to provide symmetric connectivity to main offices. The third tier is made up of access routers at each office that provide connectivity to their respective switching/distribution centers. The focus of the proposed DCN architecture is within the access tier, providing configurations for small, medium, and large central offices.

This architecture supports asynchronous, X.25, and IP connectivity to existing OSSs with X.25 and IP interfaces and network elements. With regard to Cisco products the architecture supports early-generation SONET equipment, transmission multiplexers, early-generation digital cross-connect switches, and T1 channel banks. Also included is transport support for legacy protocols such as BX.25, providing connectivity for voice switches and billing data collection devices.

The diagram below shows a typical architecture using Cisco components. However, equivalent components from other vendors maybe used to implement the same architecture.
This type of management implementation may be useful in our Agriculture Department example. The IT department of the Agriculture Department would connect a management port (VLAN) of every network appliance it owned and managed into the management VLAN (DCN). This segments all user traffic. It also prevents unauthorized users from accessing any network device that is maintained by the provider because there is no physical or logical path to the management ports of these devices.

This does not prevent each department or agency from using the network to manage their network devices. Their traffic and management functions can be completely independent from the network provider’s management systems. This allows the user to make changes to their network without affecting the larger provider network.
3. State Wide Area Network
3. **State Wide Area Network**

3.1 **Proposed Infrastructure**

The government of Nepal should create a state – of – the – art network infrastructure under Nepal Wide Area Network Project (NWAN) with the following goals:

1. establish a reliable horizontal and vertical communication corridor for within the state administration to make government more productive and compatible for electronic transactions;
2. achieve e-governance commitment and bring governance closer to public;
3. strengthen disaster management response capacity;

We recommend that this state owned ICT network infrastructure (Nepal Wide Area Network – NWAN) be setup to provide:

1. Voice, Video and Data – all services on IP,
2. connect the 14 zones and 75 district offices in the network capable of handling high volume, high speed data and video conference
3. connect subsequently, strategically selected villages numbering more than 1000
4. One robust campus area network at Singh Durbar (SDAN) connected with NWAN enabling connectivity upto the District level access for all officers at secretariat and vice versa,
5. Satellite interconnect with NWAN Hub to make all services of the network omni present in the state/country at the village level, through VSAT or Local Wireless as infrastructure permits terminal.
At a very high level we recommend the following connectivity:

**Singh Durbar** – Secure Fibre Optic connectivity between all departments within the Singh Durbar having 15 MBps bandwidth network with redundancy.

**Kathmandu** – All departments within Kathmandu should connect to the Singh Durbar on Fiber Optic connectivity 5 MBps bandwidth network with redundancy.

**Zones** – Zonal offices should be connected with 2 Mbps broadband to Kathmandu and Singh Durbar offices having 15 MBps bandwidth network with redundancy.

**Districts** – The district offices should be connected to the zonal and Singh Durbar offices with at least 256 Kbps broadband having 1 MBps bandwidth network with redundancy.

**Villages** – The villages can be connected to the district offices using wireless or other connectivity on at least 256Kbps bandwidth network with redundancy.

### 3.1.1 NWAN Network Architecture and Topology:

We recommend that the NWAN be based on a “hub-and-spoke” design, with 3 tiers:

**Tier 1** – NITC at Singha Durbar, Secretariat offices within Singha Durbar and the Metropolitan and Secretariat offices within Kathmandu where the highest offices of the government functions should be connected horizontally through a Durbar Campus Area Network (DCAN). The district centers (DCs) would be connected vertically with this Campus Area Network.

**Tier 2** – The District and Zonal Offices for the various Secretariats would be connected horizontally to a District Center (DC).

**Tier 3** – The local village offices where applicable would be connected horizontally to a Village Center (VC) which in turn would be vertically connected to the district center (DC).
The NITC is the network HUB. The Durbar Campus Area Network (DCAN) integrates with NWAN at NITC (as shown in the figure below)

The recommended design for NWAN is that of a total IP network. In such a scenario, Data, Voice and video travels as IP packets in the network, with a total convergence.

An attempt is made to explain the data flow taking place in the network for Data, voice, and video services, as given below -

3.1.2 Data Flow from PC to PC in NWAN:

- Application on computer encapsulates the data in Layer 7-Layer 5 headers
- Network driver on PC then includes Layer 4 and Layer 3 information, packetization, and encapsulation in IP. This includes source and destination IP address, TCP port, etc.
- NIC encapsulates IP data within Layer 2 MAC header, and sends it out over the LAN.
- If the destination IP address is not on the LAN, the frame reaches the router. Router strips off layer 2 MAC header, and looks at the destination IP address.
- Router does a lookup in the routing table, finds appropriate interface to send the packet out of. If this is a WAN interface, then a Layer 2 PPP header is appended to the packet, and it is queued on the interface. At this time, appropriate QoS/Queueing mechanisms are applied to the packet, based on the configuration done on the router, and the information available in the IP header.
- Once the packet reaches the remote router, the remote router strips off the Layer 2 PPP header and looks at the destination IP address. This destination IP address will typically be on the local LAN.
- Then, the router encapsulates the IP packet into a MAC header and puts it on to the LAN interface. The packet now has the destination MAC address of the PC that the data is destined to.
3.1.3 Voice calls flow from NWAN phone to NWAN phone:

- User picks up NWAN phone, dials access code for trunk line ("0" or "9").
- The PBX understands that this call is destined to another location, and therefore passes on the call to the router over the TDM link (E1 – 2Mbps leased line). Here, all digits are passed on to the router, one 64-kbps timeslot on the E1 is allocated to that call.
- The router receives the call on its voice interface. It understands the TDM signalling (E1 CAS), and converts it into H.323 standard for IP calls. It does a lookup and converts the destination phone number into the IP address of the remote router to which the destination user is connected.
- The remote router receives the H.323 call from the source router. It places that call on to the TDM link to the destination PBX. It also converts the H.323 signalling back to E1-CAS, which the PBX can understand. A 64-kbps slot on the E1 is allotted for this call.
- The remote phone starts ringing. Once the phone is answered, an RTP (real-time protocol) stream is set up between the two routers for transport of VoIP packets.
- At the source router, the digitized voice call travels from the PBX to the router. The router packages and compresses the voice from 64kbps to 8kbps (G.729a standard) using on-board DSP resources.
- IP and RTP headers are added to the compressed and packetized voice. The destination IP address in the IP header is of the remote router. This brings up the bandwidth per call to approximately 12kbps.
- The router identifies the voice traffic as high priority and puts it before the data traffic on the interface. If there are some large packets in the queue, they are broken up into smaller packets, and voice packets are then queued in between these. This ensures that voice does not face undue latency because of large data packets. This technique is known as Link Fragmentation and Interleaving.
- IP routing ensures that the VoIP packets traverse the WAN to the remote router.
- Once the voice packets reach the remote router, the reverse process is done – strip IP and RTP headers, decompress the voice, and put it on the designated 64kbps E1 link to the PBX.
- The PBX then switches the voice to the destination phone using TDM switching technology.

3.1.4 Video Call Flow:

- User at Polycom end station dials the H.323 prefix (phone number of remote device). This may be for another end station in a point-to-point scenario, or may be an MCU.
- Polycom talks to the Gatekeeper in the network, and gets the IP address corresponding to that specific prefix. Once found, a call setup message is initiated over H.323 to the remote device.
- Once call setup is complete, a call is established. The Polycom digitizes and packetises voice and video from the camera and microphone and puts it onto the LAN port.
- While doing this, it classifies the traffic as high-priority, so that the router can identify it and give it the requisite treatment for QoS.
- Once the IP Packets are on the LAN, they are then routed to the destination device using normal IP routing, just like VoIP or data traffic.
3.1.5 Tier – 1: NITC NWAN Center Network

As shown in the above diagram, the network in the NITC NWAN center comprises all the components of a central hub site.

Existing data connections (5000 – 10000 estimated) on the DCAN should be interconnected to NWAN. All Government offices and each of the (5000 – 10000 estimated) users at Secretariat, in the capital city, should be capable of doing video conferencing (VC) to any one or all Master Control Units (MCU) in the network anywhere in the state.

3.1.6 Mobility feature introduced into GSWAN:

An extended c-band VSAT station (need to get some second opinion on this recommendation) should be interfaced on to the LAN at NITC, to enable NWAN connection with the portable VSAT mobile working at a distant remote location. This will enable wide area network services to locations where there is a total telecom black out. The events taking place at remote locations are covered and connected to NWAN through portable VSAT terminal. This will give tremendous flexibility to the state administration in reaching to the public in remote areas during any emergency.

3.1.7 WLAN for important other offices beyond reach of cable:

A Wireless LAN can be commissioned, to connect to the DCAN in case they are not on the Ethernet backbone of the campus network.

3.1.8 Server farm:

Multiple Servers can be commissioned in server farm at the State Datacenter in GIDC. All common IT services, viz. internet, web hosting and maintenance, data base storage and maintain, mail services, etc., can be managed from the server farm facility center, interfaced with NWAN and DCAN.
3.1.9 Tier 2 – District Center – Generic Architecture

The District Center NWAN node should have all – voice, video and data communication faculties available.

The districts in each zone should have a District NWAN Center (DC) and be connected horizontally at the zone office in addition to all Village NWAN Nodes (VC) stations falling under its jurisdiction. Offices authorized by the Government should be able to enter into the network through dialup access. Remote Access Server (RAS) at each DC should have 10 dialup PSTN lines enabling access to those who are not directly connected with NWAN.
4. State Data Center
4. State Data Center

4.1 Data Center Architecture

4.1.1 Description

1. The router can be of SWAN or connected to SWAN depending on case-to-case scenario

2. It should be also noted that, SWAN would also be carrier for CSC information or dataflow between the Citizens / Users (Departments/ Offices) and the DC. This Router would be bridge between the intranet i.e. SWAN users and DC environment

3. The router would also have capability to handle the data traffic and multiple SSL/VPN encapsulations
for secured data transfer between SWAN/CSC/Internet and DC

4. Intrusion Detection & prevention system should detect malicious traffic and further protect the DC environment

5. Intrusion system would also detect (and prevent) any intrusion from Internet/extranet network

6. Firewalls would provide next layer of protection between the extranets (SWAN/ CSC/ Internet) and DMZ (which has hosted the application server)

7. The Application servers would be accessing the database from the backend in order to process the user / citizens queries/requests

8. The Database servers (RDBMS) are further hosted in higher security layer, comprising of components such as Firewall and Intrusion Prevention system

9. The DC provides Infrastructure Services such as Firewall Service, Directory Service, Web Service, Database Service, messaging, Backup services and data storage services etc. which would be shared among all the applications / departments participating in the DC. Using these services, the DC ensures centralized delivery of citizen / departmental services. The DC services would be deployed as components and therefore will have a potential for re-use in launching future services, without disturbing the existing architecture

10. For Securing the DC, the Intrusion prevention systems shall carry out state-full inspection and multiple layers of Firewalls shall manage the access control. At the same time more specific content level scanning products like Anti-Spam, network anti-virus gateways should be provisioned at appropriate points to ensure content level scanning, blocking and access

11. In this secure infrastructure it has to be ensured that the security devices in the network such as Firewalls, Anti-Spam Filters, proxy servers, anti-virus gateways are in high-availability mode, and these devices should be even distributed to optimize performance

12. Another key consideration should be done for hosting the Legacy applications. State Govt/Department has to migrate / port the applications to n tier architecture, which would be provided using DC

13. Web servers facing external world should be placed in DMZ internet zone in load balanced mode using external load balancer

14. Web Interface of the portal should be in a DMZ (Internet zone) & should be configured in active-standby mode using external load balancer

15. Staging servers are used for development, testing and pre-production activities should be located in separate test and development zone

16. State Government intends to host all state government applications pertaining to various divisions and departments in a single location with commitment of better service and availability to end users, it is imperative that availability of the proposed solution should be high by design

4.2 *Data Center Operations and System Management*

The information technology infrastructure library (ITIL) is the de facto best practices guide to data center operations and systems management.
4.2.1 Benefits of ITIL

Many IT organizations tend to operate in an ad-hoc and reactive fashion. They often respond to issues after they occur, leading to problems such as downtime and lower quality of service (QoS). In many cases, this scenario is understandable as IT organizations are often faced with providing increased levels of service with insufficient staff and minimal budgets. Many organizations either cannot afford to provide additional resources to IT departments or cannot justify the reasons to increase investments.

On the surface, this problem might seem very difficult to solve. However, one approach — increasing overall efficiency — can improve IT service delivery without requiring significant expenditures. It is in this arena where the implementation of IT management best practices comes in.

4.2.2 Improving Levels of Service

The quality of an IT organization is often measured by its ability to respond to business-related change requests and to provide reliability, availability, and performance. Many IT organizations do not have an organized process for responding to new issues and requests, and often several of the requests “fall through the cracks.” ITIL prescribes ways in which organizations can improve the reporting and management of problems and incidents. It helps IT organizations define how particular problems should be addressed and how to communicate with end users. By better managing these aspects of service delivery, IT departments can often identify potential areas for improvement.

4.2.3 Reducing IT Costs

Many IT departments suffer from inefficiencies that lead to increased costs. Problems caused by lack of communication, poor issue tracking, and ad-hoc changes can add up quickly. Often, IT managers are unaware of the true costs of purchasing capital assets, configuring and deploying new equipment, and maintaining this equipment. ITIL best practices include methods for calculating true costs and for translating this information into business-related terms. This information can then be used to make a strong case for investments in automation and other labor-saving technologies.

4.2.4 Enforcing well-defined processes

Policies and processes are crucial to a well-managed environment. When policies are implemented and enforced, IT management can ensure that issues are dealt with consistently and completely. ITIL recommendations provide suggestions for designing and implementing successful processes.

Often, it seems that no matter how quickly responses are handled, users’ expectations are higher. Through the use of SLAs, IT departments can communicate to users the type of response they should expect for various problems. Developing an SLA is easier when service delivery is managed through clearly defined processes.

4.3 Security Considerations for the Data Center

Data centers have evolved significantly as organizations consolidate servers, applications, and other resources, and as they adopt new technologies as a means to reduce costs and increase efficiency. Technologies such as server virtualization, distributed application tools, and IP-based storage are helping organizations maximize their data center resources, while at the same time making it more difficult to protect these critical assets.

In addition to cyber theft and increasing levels of malware, organizations must guard against new vulnerabilities introduced by data center technologies themselves. To date, security in the data center has been applied primarily at the perimeter and server levels. However, this approach isn’t comprehensive enough to protect information and resources in new system architectures.

To effectively manage the new risks, organizations should re-evaluate their data center security practices and implement new network-centric capabilities to ensure the integrity of their services. Because the network
 touches every device in the data center, it is an ideal location for security. A network-centric approach to providing security in the data center delivers benefits such as scalability, unified security policy definition and enforcement, visibility into application traffic, and reduced operations overhead.

Data centers are evolving quickly in response to operational pressures and technology innovations. To reduce costs and gain flexibility, organizations are consolidating data centers and adopting new technologies ranging from virtualization to new application architectures and cloud computing.

The current economic environment is accelerating these trends. With data center consolidation, organizations can achieve efficiencies by moving “high touch” systems from satellite offices to either central data centers or third-party cloud providers. Consolidating servers, applications, and other resources leads to higher utilization of these resources and eliminates the need for IT staff in many locations.

At the same time, new collaboration tools, including telephony presence, instant messaging, wikis, blogs, and social networking, are bringing employees closer despite physical distance. In addition, use of service-oriented architecture (SOA) and other distributed approaches to application development are resulting in highly distributed applications.

These trends are having a major impact on data center architectures and the problems that need to be addressed to provide adequate security for data and systems residing in them. In traditional data center models, applications, compute resources, and networks have been tightly coupled, with all communications gated by security devices at key choke points. However, technologies such as server virtualization and Web services eliminate this coupling and create a mesh of interactions between systems that create subtle and significant new security risks.

To secure modern data center applications, organizations need comprehensive, scalable and elastic security tools in the network that combine application fluency and identity-based controls with centralized policy and compliance management. Understanding these new security challenges is key to implementing appropriate security solutions for the virtualized, cloud-ready environment.
### 4.4 Data Center Security Framework

<table>
<thead>
<tr>
<th>Physical Security</th>
<th>High Availability</th>
<th>Backup / Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Load Balancing</td>
<td>VPN, IP SEC, PKI, SSH</td>
</tr>
<tr>
<td>Firewall</td>
<td></td>
<td><strong>AVAILABILITY, CONFIDENTIALITY / INTEGRITY</strong></td>
</tr>
<tr>
<td>Antivirus</td>
<td>PKI Smart Card</td>
<td></td>
</tr>
<tr>
<td>Secured Web Server</td>
<td>Token Card</td>
<td>Access Control</td>
</tr>
<tr>
<td>Border Router</td>
<td>Remote Access</td>
<td>Single Sign-on</td>
</tr>
<tr>
<td>Auditing</td>
<td>Access Control</td>
<td><strong>AUTHENTICATION, AUTHORISATION</strong></td>
</tr>
</tbody>
</table>

**PROTECTION**

**MONITORING**

- Intrusion Detection
- Enterprise Security
- Vulnerability Scanning
- Intrusion Alerts
- Resource Management

- Assessment
- Vulnerability Analysis
- Ethical hacking

**RISK MANAGEMENT**

- Policy | Procedures | Organisation

**STRATEGY**

The security model should be designed to provide the data center with the necessary infrastructure to support the defined services description for the customers. For example, security requirement is different for co-location and web hosting services. Also, the security design must meet the requirement of the technical/administration teams for the data-center operation.

The major focus in initial stage for the development of security architecture requires the following -

1. Identifying the services to be supported
2. Identifying the technology that addresses the security requirements
3. Identifying the connectivity requirements
4. Understanding the information to be protected
5. Provision of secure management and administration environment
6. Security management

The key components of the security architecture -

1. Network security access and control
2. Common service network
3. User authentication
4. Virtual Private Network (VPN)
5. Intrusion Detection (IDS)
6. Anti-Virus Protection
7. System and Network security scanning

4.4.1 Network security access and control

1. Border Router
   - The routers must block unnecessary network traffic such as ICMP to thwart obvious attacks
   - The routers should be configured to provide high resilience using the hot standby routing protocol (HSRP) technology
2. Content Switches
   - A clustered content switch is used to load balance incoming web-based traffic to the backend servers to improve performance (ex. For the firewall traffic flowing in and out)
3. Firewall
   - A firewall is a system that is placed between two networks that controls what traffic is allowed between those networks
   - These firewalls can be clustered to provide high resilience
4. Private VLAN
   - In order to protect servers (in co-location and dedicated web-hosting) against each others, the Private Virtual LAN (PVLAN) technology is adopted to isolate servers and provide privacy among servers
   - Preventing the possibility of one customer tampering another customer’s server via the VLAN switch. Customers owning more than one server will be configured in a community allowing communication between the servers
5. Backup Segment
   - A dedicated LAN segment for the purpose of data backup and restore
   - Each of these servers will be equipped with an additional network interface card so that data backup can be transmitted via this dedicated LAN segment, rather than competing with the core backbone traffic. PVLAN is used to isolate servers.

4.4.2 Common Service Network

- A DMZ between the border router that connects to the Internet and the Firewall
- It is created to host some important servers, these hosts will directly interact with the external world
  - The virus filtering mail relay for Internet Mail
  - External Domain Name Server (DNS)
  - Web Server or Proxy Server
4.4.3 **User Authentication for Remote Access**

- The Internet Data Center may require a dialup solution for customers to dial into the remote access network to perform content or server management of their own dedicated web servers.

- An integrated strong authentication solution enables dialup access server to authenticate these customers by means of SecureID tokens. The traditional weak authentication of using username and password pair can be replaced by strong two factor authentication (one-time password).

4.4.4 **Virtual Private Network**

- The VPN technology provides the IDC's customers a secured tunnel to communicate with their hosts from public networks (dialup or internet), and perform their own web server's content management or server management.

- For security reasons, the customer may be asked to re-authenticate using the strong two factor authentication mechanism during the VPN tunnel establishment.

4.4.5 **Intrusion Detection Systems (IDS)**

- Intrusion detection is a security technology that attempts to identify and isolate “intrusions” against computer systems.

- IDS automatically monitors user and system activity to detect patterns of misuse that may correspond to security violations.

- An IDS can monitor a server machine (Host-based IDS), a whole network (Network-based IDS), or even an application (such as a database or web server, Application-based IDS).
  - Host based IDS monitors the malicious activities within a host.
  - Network-based IDS focuses on monitoring malicious network traffic within a network segment.

4.4.6 **Anti-Virus Protection**

- On each dedicated web hosting server, an anti-virus agent should be installed to scan against known virus patterns. The mail relay in the Common Service Network should be able to scan incoming and outgoing email messages for viruses by means of a virus scanner.

- A centralized virus control system is used to control and manage all anti-virus agents and mail relay including latest virus pattern update. The virus wall behind the firewall filter out the malicious program.

4.4.7 **System and Network Security Scanning**

We suggest the data center to acquire vulnerability scanning tools so that the data center can use them to check against system and network vulnerabilities.

- A network vulnerability scanning solution checks all network-accessible entities (such as firewall, router) on a network for vulnerability to attack.

- A host-based vulnerability scanning solution checks network servers for vulnerabilities from the operating system perspective, such as file permissions, login permissions, user and group passwords, and a wide variety of other configuration settings that can affect the security profile of network servers.
4.5 **Data-center Automation**

Over time, organizations have placed increasingly heavy demands on their IT departments. Although budgets are limited, end users and other areas of the business rely increasingly on computing resources and services to get their jobs done. This situation raises the important issue of how IT staff can meet these demands in the best possible way. Despite the importance of IT in strategic and tactical operations, many technical departments are run in an ad-hoc and reactive way. Often, issues are only addressed after they have ballooned into major problems and support-related costs can be tremendous. From the end-user standpoint, IT departments can never react quickly enough to the need for new applications or changing requirements. Clearly, there is room for improvement.

This document explores data-center automation - methods through which hardware, software, and processes can work together to streamline IT operations. Modern data center challenges include increasing demands from business units with only limited resources to address those demands and covers the following areas -

1. **Business processes and frameworks** — The fundamental purpose of IT is to support business operations and to enable end users and other departments to perform their functions as efficiently as possible. IT departments face many common challenges, and various best practices have been developed to provide real-world recommendations for ways to manage IT infrastructures. From a business standpoint, the specifics include establishing policies and processes and implementing the tools and technology required to support them.

2. **IT as a service provider** — The perceived role of IT can vary dramatically among organizations. One approach that helps IT managers better meet the needs of users is to view IT as a service provider. In this approach, the “customers” are end users that rely upon IT infrastructure to accomplish their tasks. This method can help in the development of Service Level Agreements (SLAs) and IT processes and better communicate the business value that IT organizations provide.

3. **Agile management** — Modern IT environments are forced to constantly change in reaction to new business requirements. In the early days of IT, it was quite common for network administrators, server administrators, and application administrators to work in isolated groups that had little interaction. These boundaries have largely blurred due to increasing inter-dependencies of modern applications. With this convergence of servers and networks comes new management challenges that require all areas of a technical environment to work in concert.

4. **Network and server automation** — The building blocks of IT infrastructure are servers and network devices. In an ideal world, all these complex resources would manage themselves. In the real world, significant time and effort is spent in provisioning and deploying resources, managing configurations, monitoring performance, and reacting to changes. All these operations are excellent opportunities for labor-reducing automation.

4.6 **The business value of Data Center Automation**

Over time, modern businesses have grown increasingly reliant on their IT departments. Networked machines, multi-tier applications, and Internet access are all absolute requirements in order to complete mission-critical work. However, in many organizations, the clear business value of IT is difficult to estimate. Unlike departments such as sales and marketing, there are often few metrics available for quantifying how IT benefits the bottom line. Part of the reason for this disparity is that IT departments have evolved based out of necessity and have a history of filling a utilitarian role. Instead of presenting clear business value propositions, they tend to grow as needed and react to changing business requirements as quickly as possible. In many cases, this situation has caused IT budgets to shrink even while organizations are placing a greater burden on IT staff.

Furthermore, business units often see IT as out of touch with the rest of the business. To ensure success for modern companies, it’s critical that all areas of the business recognize common goals and that all contribute toward achieving them. It’s difficult to deny the basic business value of IT departments, but the quandary that...
emerges revolves around how to measure, quantify, and communicate those benefits to business decision makers. This document looks at the specific business benefits of IT, including details related to measuring benefits and costs. It then explores how data center automation can help increase the overall value that IT departments provide to their organizations.

4.6.1 Basic benefits of IT -

Practically everything that a business does relies upon the business’ underlying computing infrastructure. Accordingly, IT departments’ internal “customers” expect a certain level of service. They depend upon IT to perform various functions, including:

1. Maintaining the infrastructure — If asked what their IT departments do, many end users would point to the computing infrastructure: setting up workstations and servers, keeping systems up-to-date, and installing and managing software. Reliable and high-performance Internet connectivity has become almost as vital as electricity; without the Internet, many business functions would cease. IT is responsible for implementing and maintaining an efficient infrastructure that supports these requirements.

2. Reacting to business changes — New business initiatives often place new (or at least different) requirements on the computing infrastructure. For example, a new marketing campaign might require new applications to be deployed and additional capacity to be added. Alternatively, an engineering group might require a new test environment in order to support the development of a new product. Usually, there is an organized process to be followed whenever an employee starts or leaves the company. These changes often need to be made as quickly as possible and in a cost-efficient manner.

3. Troubleshooting — From the Help desk to critical network and server support, the service desk is often the first point of contact with IT for users that are not able to do their jobs. Users rely on these resources to quickly and efficiently resolve any issues that arise.

These benefits of IT generally point to tactical operations — performing maintenance-related operations. When enumerating the benefits of IT, often the first metrics that come to mind are those involving reliability, availability, and performance. Although these are certainly important considerations, they do not necessarily demonstrate the strategic advantage of how IT initiatives and projects can contribute to the bottom line. Consequently, it’s easy to simply look at IT as just a cost center. Regardless of whether end users realize it, IT departments do much to help their organizations.

4.6.2 The Value of Data-center Automation

So far, we’ve seen how a major component of overall IT costs and overall service levels relate to labour. It takes time and effort to maintain even small IT environments, and these factors can clearly affect the bottom line. One initiative that can provide clear benefits and a quick return on investment is data center automation. Data center automation solutions can dramatically reduce charges for one of the most expensive resources — labour. Tools and features that allow for automated deployment, provisioning, change management, and configuration tracking provide an excellent payoff.

For example, a common challenge for most IT environments is that of keeping systems up to date. Managing security patches and other software changes can easily use up large amounts of time. Furthermore, the process tends to be error-prone: It’s easy for systems administrators to accidentally overlook one or a few systems. Through the use of data center automation, the same tasks can be performed in much less time with far less involvement from IT staff. This provides numerous benefits, including freeing systems administrators to work on other tasks. Often, automation increases the server-to-administrator ratio and reduces the amount of time required to perform operations. Other benefits include improved consistency, the enforcement of policies and processes, and improved security. Additionally, by implementing best practices (such as those provided with the ITIL), efficiency and operational reliability can improve.
The bottom line is that data center automation can significantly improve the business value of IT. By reducing costs and removing data center-related bottlenecks, data center automation enables IT and business leaders to focus on more important tasks. The entire organization will be able to react more quickly and surely to changes, providing both strategic and tactical advantages to the entire enterprise.

4.7 Service Provider

Modern organizations often rely upon many vendors and outside resources to meet business objectives. For example, a marketing group might recruit outside talent to develop a Web site or to work on creative aspects of a new campaign. Alternatively, engineering groups might rely on outsourcing to contractors or consultants to build a portion of a product. IT departments, however, are often seen as cost centers that provide only basic infrastructure services. By treating IT departments as service providers, however, a strategic relationship can be established, and IT can be seen as a business partner.

4.7.1 Benefits of operating IT as a Service Provider

The value of a service provider is often measured by its abilities to help its customers reach their goals. In this arena, customer service is most important. By having IT departments serve its customers in this arrangement, both can work together to ensure that the best projects and solutions — those that provide the most value to the individual business units — are delivered.

When IT works as a service provider, it should act like an independent business. Its “customers” are the end users and departments that it serves, and its “products” are the services and technology solutions that are provided for use by the customers. Although this concept might at first seem like a strange approach for an internal department, there are many potential benefits.

First, IT services are better communicated so that end users know what to expect (and what to do if expected service levels are not met). Second, all areas of the business can see how IT operations are helping them achieve their objectives.

4.7.2 Implement the Service Provider Model

There are several aspects that must be taken into consideration before an internal IT department can be seen as a business partner.

1. Identifying the customer’s needs - For IT as a service provider, this process can start with meetings with individual department leaders as well as end users that might have specific requirements. The overall goal for the service provider is to focus on the business goals of the customer, and not on technology itself. The first step is to identify the primary purpose of the department. This includes details related to how success is measured and approaches to achieving the success. The details will likely differ dramatically between, for example, sales and engineering organizations. Next, it is important to identify current “pain points”—problems or limitations that are reducing the level of success. Based on this input, IT service providers can develop proposed solutions that address those issues.

2. Identifying the Service Delivery Details - Once a customer has agreed to purchase a specific product or service from the IT department, it’s time to look into the implementation details. It’s important to identify the key stakeholders and to establish points of contact on the IT side and on the customer side. The goal should be to identify who is responsible for which actions. Milestones should be designed and mutually agreed upon before moving forward. Also, processes for managing changing requirements will help eliminate any surprises during the implementation of the solution. For larger projects, a change management process should be created, complete with approval authority from the customer and the service provider.

3. Measuring Service Levels - An IT service provider can create products of various types. Some might be closed-ended initiatives, such as the installation of a Customer Relationship Management (CRM)
solution, or the expansion of a development test lab. In those cases, service levels can be measured based on milestones and the quality of the implementation. Stakeholders can sign off on project completion just as they would with external vendors. Other products might involve expected levels of service. For example, when new servers and workstations are added, customers should know what type of response to expect when problems occur. Service Level Agreements (SLAs) can be instrumental in developing mutually agreed upon expectations. For less-critical systems, longer turnaround times might be acceptable. For mission-critical components, greater uptime and quicker response might be justified. Of course, those services will likely come at a higher cost because they will involve additional staff allocation, the purchase of high-availability solutions, and other features.

4.8 **Configuration Management Database**

To make better business and technical decisions, all members of the IT staff need to have a way of getting a single, unified view of “everything” that is running their environments. A Configuration Management Database (CMDB) is a central information repository that stores details related to an IT environment. It contains data about hardware and software deployments and allows users to collect and report on the details of their environments.

The CMDB contains information related to workstations, servers, network devices, and software. Various tools and data entry methods are available for populating the database, and most solutions provide numerous configurable reports that can be run on-demand. The database itself can be used to track and report on the relationships between various components of the IT infrastructure, and it can serve as a centralized record of current configurations.

The below illustrated Figure shows an overview of how a CMDB works with other IT automation tools. Various data center automation tools can store information in the CMDB, and users can access the information using an intranet server. The goal of using a CMDB is to provide IT staff with a way to centrally collect, store, and manage network- and server-related configuration data.

4.8.1 **The need for a CMDB**

Most IT organizations track information in a variety of different formats and locations. For example, network administrators might use spreadsheets to store IP address allocation details. Server administrators might store profiles in separate documents or perhaps in a simple custom developed database solution. Other important details might be stored on paper documents. Each of these methods has weaknesses, including problems with collecting the information, keeping it up-to-date, and making it accessible to others throughout the organization.

The end result is that many IT environments do not do an adequate job of tracking configuration related information. When asked about the network configuration of a particular device, for example, a network administrator might prefer to connect directly to that device over the network rather than refer to a spreadsheet that is usually out-of-date. Similarly, server administrators might choose to undergo the tedious process of logging into various computers over the network to determine the types and versions of applications that are installed instead of relying on older documentation. If the same staff has to perform this task a few months later, they will likely choose to do so manually again. It doesn’t take much imagination to recognize that there is room for improvement in this process.

4.8.2 **Benefits of using a CMDB**

A CMDB brings all the information tracked by IT organizations into a single centralized database. The database stores details about various devices such as workstations, servers, and network devices. It also maintains details related to how these items are configured and how they participate in the infrastructure of the IT department. Although the specific details of what is stored might vary by device type, all the data is stored within the centralized database solution. The implementation of a CMDB can help make IT-related information much easier to collect, track, and report on. Among the many benefits of using a CMDB are the following:
1. Configuration Auditing - IT environments tend to be complex, and there are often hundreds of different settings that can have an impact on overall operations. Through the use of a CMDB, IT staff can compare the expected settings of their computers with the actual ones. Additionally, the CMDB solution can create and maintain an audit trail of which users made which changes and when. These features can be instrumental in demonstrating compliance with regulatory standards such as the Health Insurance Portability and Accountability Act (HIPAA) or the Sarbanes-Oxley Act.

2. Centralized Reporting - As all configuration-related information is stored in a central place, through the use of a CMDB, various reporting tools can be used to retrieve information about the entire network environment. In addition to running pre-packaged tools, developers can generate database queries to obtain a wide variety of custom information. Many CMDB reporting solutions provide users with the ability to automatically schedule and generate reports. The reports can be stored for later analysis via a Web site or may be automatically sent to the relevant users via email.

3. Change Tracking - Often, seemingly complicated problems can be traced back to what might have seemed like a harmless change. A CMDB allows for a central place in which all change-related information is stored, and the CMDB system can track the history of configuration details. This functionality is particularly helpful in modern network environments where it’s not uncommon for servers to change roles, network addresses, and names in response to changing business requirements.

4. Calculating Costs - Calculating the bottom line in network environments requires the ability to access data for software licenses and hardware configurations. Without a centralized solution, the process of collecting this information can take many hours. In addition, it’s difficult to trust the information because it tends to become outdated very quickly. A CMDB can help obtain details related to licenses, support contracts, asset tags, and other details that can help quickly assess and control costs.

4.9 Service Level Agreements

The primary focus of IT departments should be meeting the requirements of other members of their organizations. As businesses have become increasingly reliant on their technology investments, people ranging from desktop users to executive management have specific expectations related to the levels of service they should receive. Although these expectations sometimes coincide with understandings within an IT organization, in many cases, there is a large communications gap.

Service Level Agreements (SLAs) are intended to establish, communicate, and measure the levels of service that will be provided by IT departments. They are mutually agreed-upon definitions of scope, expected turnaround times, quality, reliability, and other metrics that are important to the business as a whole.

4.9.1 Challenges related to IT Services Delivery

In some areas of IT, the job can be rather thankless. In fact, it is sometimes said that no one even thinks about IT until something goes wrong. Although many organizations see investments in IT as a strategic business investment, others see it only as a cost center. The main challenge is to be able to come to an understanding that includes the capabilities of the IT department and the expectations of the “customers” it serves. That is where the idea of service levels comes in. In order to focus on these benefits, IT departments can think of themselves as outside vendors that are selling products and services to other areas of their organization.

4.9.2 Defining Service Level Requirements -

SLAs can be set up in a variety of ways, and there are several approaches that can be taken toward developing them. One common factor, however, is that all areas of the organization must be involved. SLAs are not something that can be developed by IT departments working in isolation. The process will require research and negotiations in order to determine an appropriate set of requirements.
4.10 **IT Processes**

Processes define a consistent set of steps that should be followed in order to complete a particular task. From an IT standpoint, processes can range from details about Service Desk escalations to communicating with end users. The goal of IT processes is to improve overall operations within the IT department and the organization as a whole.

It’s often a fact that the implementation of processes requires additional effort and may add steps to some jobs. The steps can be time-consuming and may result in resistance or non-compliance. That raises the challenge: Processes must be worth far more than the “trouble” they cause in order to be considered worthwhile. This section will look at details related to what makes a good process, how you can enforce processes, and the benefits of automating process management.

### 4.10.1 The Benefits of Processes -

The major goals and benefits of designing and implementing processes include -

1. Consistency - Tasks should be performed in the same way, regardless of who is performing them. In fact, in many cases, it can be argued that having something done consistently in a sub-optimal way is far better than having tasks sometimes completed well and sometimes completed poorly. Ad-hoc changes are difficult to manage and can lead to complex problems.

2. Repeatability - It’s often easy for IT staff to make the same mistakes over and over or to “reinvent the wheel.” The goal of defining processes is to ensure that the same task can be completed multiple times in the same way. Simply allowing everyone to complete goals in their own way might be good for tasks that involve creativity, but they often don’t work well for operations that require a lot of coordination and many steps.

3. Effectiveness - The process should indicate the best way to do things with respect to the entire organization and all that are involved. The steps involved in the process should enforce best practices.

4.11 **Policy Enforcement**

Well-managed IT departments are characterized by having defined, repeatable processes that are communicated throughout the organization. However, sometimes that alone isn’t enough — it’s important for IT managers and systems administrators to be able to verify that their standards are being followed throughout the organization.

### 4.11.1 Benefits of Policies

It usually takes time and effort to implement policies, so let’s start by looking at the various benefits of putting them in place. The major advantage to having defined ways of doing things in an IT environment is that of ensuring that processes are carried out in a consistent way. IT managers and staffers can develop, document, and communicate best practices related to how to best manage the environment.

### 4.11.2 Types of Policies

Policies can take many forms. For example, one common policy is related to password strength and complexity. These requirements usually apply to all users within the organization and are often enforced using technical features in operating systems (OSs) and directory services solutions. Other types of policies might define response times for certain types of issues or specify requirements such as approvals before important changes are made. Some policies are mandated by organizations outside of the enterprise’s direct control. The Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, and related governmental regulations fall into this category.
4.11.3 **Defining Policies**

Simply defined, policies specify how areas within an organization are expected to perform their responsibilities. For an IT department, there are many ways in which policies can be used. On the technical side, IT staff might create a procedure for performing system updates. The procedure should include details of how downtime will be scheduled and any related technical procedures that should be followed. For example, the policy might require systems administrators to verify system backups before performing major or risky changes.

On the business and operations side, the system update policy should include details about who should be notified of changes, steps in the approvals process, and the roles of various members of the team, such as the service desk and other stakeholders.

### 4.12 Business Processes

An important characteristic of successful businesses is a strong alignment of the efforts between multiple areas of the organization. This arrangement rarely occurs by itself — instead, it requires significant time and effort from organizational leaders. The end result is often the creation of processes that define how all areas of the enterprise should work together to reach common goals.

#### 4.12.1 Benefits of Well Defined Processes

Business processes are put in place to describe best practices and methods for consistently performing certain tasks. Often, the tasks involved will include input and interaction of individuals from throughout the organization. Before delving into details and examples of processes, let’s first look at the value and benefits.

There are several valuable benefits of implementing processes. The first is consistency: by documenting the way in which certain tasks should be completed, you can be assured that all members of the organization will know their roles and how they may need to interact with others. This alone can lead to many benefits. First, when tasks are performed in a consistent manner, they become predictable. For example, if the process of qualifying sales leads is done following the same steps, managers can get a better idea of how much effort will be required to close a sale. If the business needs to react to any changes (for example a new competitive product), the process can be updated and all employees can be instructed of the new steps that need to be carried out.

Another major benefit of defining business processes is related to ensuring best practices. The goal should not be to stifle creativity. Rather, it’s often useful to have business leaders from throughout the organization decide upon the best way to accomplish a particular task. When considering the alternative — having every employee accomplish the task a different way — consistency can greatly help improve efficiency. Additionally, when processes are documented, new employees or staff members that need to take on new roles will be able to quickly learn what is required without making a lot of mistakes that others may have had to learn “the hard way.
5. *Infrastructure Roadmap*
5. Infrastructure Roadmap

5.1 Roadmap – Shared Network Adoption

The architecture for a shared infrastructure can translate to many benefits for government agencies looking to address many of today’s IT and collaboration requirements.

Based on the SONA framework, PWC government programs and technical architectures integrate networked infrastructure services, constituent services, and business applications within and among agencies.

Having a phased roadmap allows a successful migration from the current infrastructure to an architecture supported by a center of excellence that enables shared infrastructure and services between multiple agencies.

Each phase of the roadmap introduces new technologies to reach a shared infrastructure, which enables agencies to share services through a center of excellence. Each agency may have different needs, requiring some tasks to be performed sooner, but the below table shows a transformation to a shared infrastructure model broken down into logical steps.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Shared / Dedicated across Agencies</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Time-Division Multiplexing (TDM)</td>
<td>Dedicated</td>
<td>Current state of the network which is typically characterized by siloed TDM technologies such as PBX for voice and Frame Relay/ATM for data connectivity.</td>
</tr>
<tr>
<td>2 IP Network</td>
<td>Dedicated</td>
<td>The first step in migration from TDM technologies to an IP-enabled infrastructure that builds the foundations for the transformation to occur. The IP network needs to be built with network characteristics to support QoS, high availability, etc.</td>
</tr>
<tr>
<td>IP Communications</td>
<td>Dedicated</td>
<td>Enable “Unified Communications”, voicemail, conferencing, rich-media communication, and extension mobility.</td>
</tr>
<tr>
<td>IP Contact Center</td>
<td>Dedicated</td>
<td>Enable a centralized contact center to deliver intelligent call routing and call treatment to support an IP-enabled customer contact center.</td>
</tr>
<tr>
<td>Self-Defending Network Security</td>
<td>Dedicated</td>
<td>Enable each site with the security needed to maintain the business through capabilities including stateful firewalls, intrusion protection and prevention, URL filtering, and trust and identity.</td>
</tr>
<tr>
<td>3 Intelligent Routing</td>
<td>Dedicated</td>
<td>• Site-to-site VPN with IPsec for encryption when required.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DCN for out-of-band management.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• QoS to ensure the site-to-site experience is equal to the experience of a single location, which is a key foundation to support differentiated services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hierarchical, end-to-end network.</td>
</tr>
<tr>
<td>Mobility</td>
<td>Dedicated</td>
<td>Enable mobile IP to support the mobile workforce.</td>
</tr>
<tr>
<td>Technology</td>
<td>Shared / Dedicated across Agencies</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Data Center</td>
<td>Dedicated</td>
<td>Consolidate data center into a centralized environment enabled through an IP network fabric that supports the network DNA to transform the data center architecture.</td>
</tr>
<tr>
<td>4 Intelligent Routing</td>
<td>Shared</td>
<td>Enable virtualization and segmentation of the intelligent routing layer to support shared infrastructure resources across multiple agencies.</td>
</tr>
<tr>
<td>Self-Defending Network Security</td>
<td>Shared</td>
<td>Virtualize security features such as firewall into the network to support multiple agencies.</td>
</tr>
<tr>
<td>Data Center</td>
<td>Dedicated</td>
<td>Enable data center consolidation with the server and storage fabric.</td>
</tr>
<tr>
<td>5 IP Communications</td>
<td>Shared</td>
<td>Virtualize IP Communications through the centralized environment supporting voicemail, conferencing, and other rich-media communication for multiple agencies.</td>
</tr>
<tr>
<td>IP Contact Center</td>
<td>Shared</td>
<td>Virtualize the IP contact center for multiple agencies.</td>
</tr>
<tr>
<td>Data Center</td>
<td>Shared</td>
<td>Consolidate data center functions across multiple agencies and introduce application acceleration and load balancing.</td>
</tr>
<tr>
<td>6 Data Center</td>
<td>Shared</td>
<td>Virtualize data center functions across multiple agencies and introduce application protocol optimization/translation.</td>
</tr>
</tbody>
</table>

### 5.2 Roadmap – Data Center Consolidation

#### 5.2.1 Phase 1 – IT Asset Inventory Baseline (Including Preliminary Assessment & Quick Wins)

Assessment will include details such as facility location, how the data center is utilized, and by whom, whether a facility is stand-alone or co-located with other activities, square footage of the facility, legal ownership details, measurement of energy consumption, and ongoing costs. Those who conduct the assessment will be required to:

- Create an inventory of HW.SW assets by data center
- Capture baseline metrics for utilization & energy for each data center
- Identify quick wins, including specific deliverables
- Provide an IT Asset inventory for the baseline and the quick wins.

#### 5.2.2 Phase 2 – Application Mapping

Efforts must be made to extend the ongoing inventory to the level where administrators can map applications:

- To servers
- To specific databases and platforms
- To specific application dependencies
- With specific details on application security
• With details on application usage and service level agreements (SLAs)
• With information on segment architecture

5.2.3 Phase 3 – Analysis & Strategic Decisions

• Perform energy and cost evaluation for possible different approaches
• Identify the risks, alternatives, cost assumptions and business benefits
• Make strategic technology & consolidation investment decisions

5.2.3.1 Specific deliverables:
Consolidation analysis and strategic investment decisions on standard platforms and services

5.2.4 Phase 4 – Consolidation Design & Transition Plan

• Design and test consolidation alternative
• Develop transition plan for energy use optimization and data center consolidation
• Create a project plan and full Work Breakdown Structure for the transition plan

5.2.4.1 Specific deliverables:
Consolidation design and transition plan

5.2.5 Phase 5 – Consolidation & Optimization Execution

• Execute virtualization, consolidation and migration plans
• Execute energy use optimization plans
• measure and report on utilization and cost saving metrics

5.2.5.1 Specific deliverables:
Consolidation and execution plus progress reports

5.2.6 Phase 6 – Ongoing Optimization Support

• Based on lessons learned from previous work, continue energy use optimization and consolidation

5.2.6.1 Specific deliverables:
• Ongoing semi-annual metrics reports
• Continue ongoing monitoring and reporting of utilization and cost saving metrics.

5.2.7 End Goal

One likely end-goal if the extensive assessments are too slow the expansion of government data centers by instead focusing on enterprise architectures that will support more cloud-based IT services
6. Infrastructure Governance
6. Infrastructure Governance

6.1 Principles

From studying and working with hundreds of enterprises, we have distilled the lessons from many outstanding leaders into ten principles of IT governance. We intend these principles to provide leaders with a succinct summary to use as a primer, refresher, or checklist as they refine their IT governance.

6.1.1 Actively design governance

Many enterprises have created disparate IT governance mechanisms. These uncoordinated mechanism "silos" result from governance by default—introducing mechanisms one at a time to address a particular need (for example, architecture problems or overspending or duplication). Patching up problems as they arise is a defensive tactic that limits opportunities for strategic impact from IT. Instead, management should actively design IT governance around the enterprise's objectives and performance goals.

Actively designing governance involves senior executives taking the lead and allocating resources, attention, and support to the process. For some enterprises, this will be the first time IT governance is explicitly designed. Often there are mature business governance processes to use as a starting point. For example, the Tennessee Valley Authority piggybacked its IT governance on its more mature business governance mechanisms, such as its capital investment process. TVA's IT governance included a project review committee, benchmarking, and selective chargeback—all familiar mechanisms from the engineering side of the business.

Not only does overall governance require active design, but each mechanism also needs regular review. Focus on having the fewest number of effective mechanisms possible. Many of the enterprises we studied had as many as fifteen different governance mechanisms, all varying in effectiveness. Fifteen mechanisms may possibly be needed but it's highly unlikely. All fifteen will certainly not be very effective, integrated, and well understood. Many enterprises with effective IT governance have between six and ten integrated and well-functioning mechanisms. One goal of any governance redesign should be to assess, improve, and then consolidate the number of mechanisms. Early in the learning cycle, mechanisms may involve large numbers of managers. Typically, as senior managers better understand IT value and the role of IT, a smaller set of managers can represent enterprise needs.

6.1.2 Know when to redesign

Rethinking the whole governance structure requires that individuals learn new roles and relationships. Learning takes time. Thus, governance redesign should be infrequent. Our recommendation is that a change in governance is required with a change in desirable behavior.

6.1.3 Involve senior managers

In our study, firms with more effective IT governance had more senior management involvement. CIOs must be effectively involved in IT governance for success. Other senior managers must participate in the committees, the approval processes, and performance reviews. For many enterprises, this involvement is a natural extension of senior management's normal activities. For example, MPS-Scotland Yard used its strong existing management committee structure to improve IT governance and gain greater synergies across all its operations. The Information Management Steering Group (IMSG) is one of fourteen strategic committees that connect to the top-level executive committee. This interlocking committee structure ensures senior management attention to IT in the context of the whole enterprise.
CIOs must be effectively involved in IT governance for success.

Senior management necessarily gets involved in strategic decisions. This means that senior management is rarely concerned with the exception process. However, if an exception has strategic implications, it may reach the executive level IT Steering Committee.

Many senior managers are willing to be involved but are not sure where to best contribute. It's very helpful for the CIO and his or her staff to communicate IT governance on one page with a picture like the Governance Arrangements Matrix. The matrix provides a vehicle for discussing each senior manager's role and any concerns they have.

6.1.4 Make choices

Good governance, like good strategy, requires choices. It's not possible for IT governance to meet every goal, but governance can and should highlight conflicting goals for debate. As the number of tradeoffs increases, governance becomes more complex. Top-performing enterprises handle goal conflicts with a few clear business principles. The resulting IT principles reflect these business principles. Old Mutual South Africa's (OMSA) six IT principles, or "nonnegotiables," as they are called, provide a useful framework or how to use IT.

For example, The first principle, which all OMSA business units must observe, states: "The interest and needs of the Group/OMSA come first when exploiting technology or when contracting with suppliers."

Appropriate stakeholders must be involved in the approval process prior to contracts being signed.

Some of the most ineffective governance we have observed was the result of conflicting goals. This problem was often observed in the government sector, where directives come from many agencies. The result was confusion, complexity, and mixed messages, so the governance was ignored. The unmanageable number of goals typically arose from not making strategic business choices and had nothing to do with IT. We observed that good managers trying diligently to meet all these goals became frustrated and ineffective.

6.1.5 Clarify the exception-handling process

Exceptions are how enterprises learn. In IT terms, exceptions challenge the status quo, particularly the IT architecture and infrastructure. Some requests for exceptions are frivolous, but most come from a true desire to meet business needs. If the exception proposed by a business unit has value, a change to the IT architecture could benefit the entire enterprise. Some common elements in exceptions procedures:

1. The process is clearly defined and understood by all. Clear criteria and fast escalation encourage only business units with a strong case to pursue an exception.

2. The process has a few stages that quickly move the issue up to senior management. Thus, the process minimizes the chance that architecture standards will delay project implementation.

3. Successful exceptions are adopted into the enterprise architecture, completing the organizational learning process.

Formally approved exceptions offer a second benefit in addition to formalizing organizational learning about technology and architecture. Exceptions serve as a release valve, relieving the enterprise of built-up pressure. Managers become frustrated if they are told they can’t do something they are sure are good for business. Pressure increases and the exceptions process provides a transparent vehicle to release the frustration without threatening the governance process.

6.1.6 Provide the right incentives

There has been so much written about incentive and reward systems in enterprises that we feel the topic is well covered and understood. Nevertheless, a common problem we encountered in studying IT governance was a...
misalignment of incentive and reward systems with the behaviors the IT governance arrangements were designed to encourage. The typical concern: "How can we expect the governance to work when the incentive and reward systems are driving different behavior?" This mismatch is bigger than an IT governance issue. Nonetheless, IT governance is less effective when incentive and reward systems are not aligned with organizational goals.

A major governance and incentive alignment issue is business unit synergy. If IT governance is designed to encourage business unit synergy, autonomy, or some combination, the incentives of the executives must also be aligned. For example, in a large consumer products firm, the CEO wanted to increase synergies between business units to provide a single face to the small number of important customers that did business with several business units. The CEO and CIO worked together to design IT governance to align the enterprise IT assets to support the new objective. The new IT governance encouraged sharing of customer information, contact logging, pricing, and order patterns across business units. However, it was not until the business unit executives' incentive system was changed from being nearly 100 percent based on business unit performance to being 50 percent based on firm-wide performance that the new IT governance gained traction.

Avoiding financial disincentives to desirable behavior is as important as offering financial incentives. DBS Bank in Singapore does not charge for architectural assistance to encourage project teams to consult with architects. Whenever incentives are based on business unit results, chargeback can be a point of contention. Enterprises can manipulate charges to encourage desirable behavior, but chargeback pricing must be reasonable and clearly understood.

It is hard to overestimate the importance of aligning incentive and reward systems to governance arrangements. If well-designed IT governance is not as effective as expected, the first place to look is incentives.

**6.1.7 Assign ownership and accountability for IT governance**

Like any major organizational initiatives, IT governance must have an owner and accountabilities. Ultimately, the board is responsible for all governance, but the board will expect or delegate an individual (probably the CEO or CIO) or group to be accountable for IT governance design, implementation, and performance—similar to the finance committee or CFO being accountable for financial asset governance. In choosing the right person or group, the board, or the CEO as their designate, should consider three issues.

First, IT governance cannot be designed in isolation from the other key assets of the firm (financial, human, and so on). Thus the person or group owning IT governance must have an enterprise-wide view that goes beyond IT, as well as credibility with all business leaders.

Second, the person or group cannot implement IT governance alone. The board or CEO must make it clear that all managers are expected to contribute to IT governance as they would contribute to governance of financial or any other key asset.

Third, IT assets are more and more important to the performance of most enterprises. A reliable, cost-effective, regulation-compliant, secure, and strategic IT portfolio is more critical today than ever before. The person or group owning IT governance must understand what the technology is and is not capable of. It is not the technical details that are critical but a feel for the two-way symbiotic connection between strategy and IT.

The CIO owns IT governance in the majority of sizable firms today. Other enterprises have chosen either another individual (the COO or occasionally the CEO) or a committee (say, of senior business and IT leaders) to own IT governance. We have not observed any one approach that always works best. It takes a very business-oriented—and well-positioned—CIO to deliver on the first consideration and a very technically interested COO or CEO to deliver on the third. Committees have the problem of meeting only periodically and dispersing the responsibility and accountability.

Our recommendation is that the board or CEO hold the CIO accountable for IT governance performance with some clear measures of success. Most CIOs will then create a group of senior business and IT managers to help design and implement IT governance. The action of the board or CEO to appoint and announce the CIO as
accountable for IT governance performance is an essential first step in raising the stakes for IT governance. Without that action, some CIOs cannot engage their senior management colleagues in IT governance. Alternatively, the board or CEO may identify a group to be accountable for IT governance performance. This group will then often designate the CIO to design and implement IT governance.

6.1.8 Design governance at multiple organizational levels

In large multi-business unit enterprises it is necessary to consider IT governance at several levels. The starting point is enterprise-wide IT governance driven by a small number of enterprise-wide strategies and goals. Enterprises with separate IT functions in divisions, business units, or geographies require a separate but connected layer of IT governance. JPMorgan Chase has IT governance at the enterprise, division, and business unit level. Usually the demand for synergies increases at the lower levels, whereas the need for autonomy between units is greatest at the top of the organization.

The lower levels of governance are influenced by mechanisms designed for higher levels. Thus, we advocate starting with the enterprise-wide IT governance, as it will have implications for the other levels of governance. However, starting enterprise-wide is sometimes not possible for political or focus reasons, and starting at the business unit level can be practical. Assembling the governance arrangements matrixes for the multiple levels in an enterprise makes explicit the connections and pressure points.

6.1.9 Provide transparency and education

It's virtually impossible to have too much transparency or education about IT governance. Transparency and education often go together—the more education, the more transparency, and vice versa. The more transparency of the governance processes, the more confidence in the governance. Many firms like State Street Corporation use portals or intranets to communicate IT governance. State Street's portal includes under the section "IT Boards, Committees, and Councils" a description of the Architecture Committee and all the other governance bodies. The portal includes tools and resources, such as a glossary of IT terms and acronyms and the "Computer Contract Checklist." Often portals include lists of approved or recommended products. Templates for proposing IT investments complete with spreadsheets to calculate the IT business value are often available.

It is hard to overestimate the importance of aligning incentive and reward systems to governance arrangements.

The less transparent the governance processes are, the less people follow them. The more special deals are made, the less confidence there is in the process and the more workarounds are used. The less confidence there is in the governance, the less willingness there is to play by rules designed to lead to increased firm-wide performance. Special deals and nontransparent governance set off a downward spiral in governance effectiveness.

Communicating and supporting IT governance is the single most important IT role of senior leaders. The person or group who owns IT governance has a major responsibility for communication. Firms in our study with more effective governance also had more effective governance communication. The more formal venues for communication were the most important. For example, CIOs on average assessed their enterprises' documentation of governance processes as ineffective. However, the firms with successful IT governance had highly effective documentation. Highly effective senior management announcements and CIO offices were also important to successful governance.

When senior managers, particularly those in business units, demonstrate lack of understanding of IT governance, an important opportunity is presented. Working with managers who don’t follow the rules is an opportunity to understand their objections. These discussions provide insight on whether the rules need refinement as well as a chance to explain and reinforce the governance.
6.1.10 Implement common mechanisms across the six key assets

We began the book by describing how IT governance fits into corporate governance. We contend that enterprises using the same mechanisms to govern more than one of the six key assets have better governance. For example, executive committees that address all enterprise issues including IT, such as the one at MPS-Scotland Yard, create synergies by considering multiple assets.

Recall the exercise (in Chapter 1) of listing all the mechanisms implementing each of the six key assets. Each asset may be expertly governed, but the opportunity for synergistic value is lost. For example, a firm implementing a single point of customer contact strategy must coordinate its assets to deliver that uniform experience. Just having good customer loyalty (that is, relationship assets) without the products to sell (IP assets) will drain value. Not having well-trained people (human assets) to work with customers supported by good data and technology (information and IT assets) will drain value. Not having the right buildings and shop fronts to work from or in which to make the goods (physical assets) will drain value. Finally, not coordinating the investments needed (financial assets) will drain value.

Put this way, the coordination of the six assets seems blindingly obvious. But just glance back at your six lists of mechanisms and see how well coordinated—and more importantly, how effective—they are. Many enterprises successfully coordinate their six assets within a project but not across the enterprise via governance. In designing IT governance, review the mechanisms used to govern the other key assets and consider broadening their charter (perhaps with a subcommittee) to IT rather than creating a new, independent IT mechanism.

These ten management principles highlight many of the key findings in our work with enterprises. Attention to all of them should lead to greater value from IT. The leadership of the CIO is also critical to creating IT value.

6.2 Governance Framework

Government bodies have a unique combination of councils, committees and working groups, all with diverse membership that make, influence, guide, or assist with IT decision making. These structures reveal different levels of complexity and centralisation or decentralisation, and the provide diverse ideas about how an institution structures IT decision making.

A framework for governance needs to be able to address the decision-making environment, including the people involved, the decisions made, and the specific situation encompassed.

6.2.1 The Weill and Ross Framework

The framework includes three major components: domains, styles, and mechanisms. Each component poses a question about IT, the answer to which provides a key part of the governance framework.

- Domains – What decisions need to be made?

The IT Governance framework proposes that an institution make five key governance decisions, captured by the following questions:

- IT principles – how will IT create business value?
- IT infrastructure strategies – how will we build shared services?
- IT architecture – what technical guidelines and standards will we use?
- Business applications – what applications do we need?
- IT investment and prioritisation – how much and where will we invest?
- Styles – Who has input and/or decision rights?
Once the scope has been defined, the next step is to identify who is involved in decision making and how they are involved. The IT Governance framework proposes the involvement of six groups of people (the who) and specify whether each group has input and/or decision rights (the how) for each of the five domain IT questions listed above.

- Mechanisms – How are the decisions formed and enacted?

The last component of the framework is how the institution implements the governance arrangement: what decision-making structures, processes and approaches are used. Following the identification of decisions and the specification of input and/or decision rights, an institution must decide detailed decision responsibility and accountability, how alignment will occur, and how information will be communicated throughout the institution. These three mechanisms, properly selected, ensure, the institutions approach to IT governance will perform as desired.

The IT Governance framework provides three categories of mechanisms to specify how the decisions made by the identified individuals (or groups) will be enacted.

- Decision-making structures – these mechanisms clarify who is responsible and accountable for decisions. Examples of these structures are committees, executive teams, and business / IT relationship managers.

- Alignment processes – these mechanisms ensure effective input to decision makers and implementation of their decisions. Examples of these processes are IT investment and evaluation process, architecture exception process, service-level agreements, and metrics.

- Communication approaches – these mechanisms disseminate governance processes and individual responsibilities to everyone who needs to know. Examples of these approaches are announcements, advocates, channels, and education efforts.

6.2.2 Summary - Key Questions to Ask

- How understandable and transparent is IT governance at our institution? What percentage of our senior executives can accurately explain how IT is governed in the institution?

- What decisions need to be made about IT at our institution (Example: How will IT create business value? What technical guidelines and standards will we use? What applications do we need? How much and where will we invest?)

- Who should we gather input from and who should make the decisions to ensure that academic, administrative, research, and enterprise concerns are appropriately represented? What should the scope of each person or group be for each decision?

- How should the decision-making, alignment, and communication approaches of the people and groups involved be related so that IT governance is simple, clear, and effective?

- How can we effectively monitor our IT decisions and modify our approach to governance when appropriate?

6.3 Proposed Matrix

To fit Nepal’s IT infrastructure maturity, a modified Weills IT framework is proposed below.
<table>
<thead>
<tr>
<th>IT Principles</th>
<th>Enterprise Needs</th>
<th>IT Infrastructure Strategies</th>
<th>IT Architecture</th>
<th>Business Applications</th>
<th>IT Investment and Prioritization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head of IT for the Country</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>CIO and/or other directors</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functional leaders / delegates</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT cabinet and atleast one functional area “VP” equivalent</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>CIO/IT directors and atleast one functional area head</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Functional area that owns a business process or end user</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
7. Infrastructure Best Practices
7. **Infrastructure – Best Practices Checklist**

### 7.1 Facility and Physical Requirements

- Multiple physically separate connections to public power grid substations
- Continuous power supply with backup uninterruptible power supply (UPS) systems:
  - Adequate UPS capacity including air conditioning and lights
  - UPS systems tested at full load on monthly schedule
  - Fuel for UPS generators (48 hours worth) kept on premises and monitored for local environmental compliance
- Conform to or exceed applicable local structural building codes utilizing standards such as bullet proof glass, fire doors and reinforced walls and complying with disaster proof design:
  - Comply with all local zoning ordinances
- Certify not located in a 100-year flood plain
- Earthquake and hurricane bracing on all racks and cable trays (where appropriate)

- Adequate multizone air conditioning, including a backup system for the multizone air conditioning:
  - Climate control including humidity sensors and control
- Heat and smoke detectors that meet or exceed all local fire code regulations.
  - Very Early Smoke Detection Alarm (VESDA)
  - FM200 [ETG5] fire suppression system in data center and NOC
  - Separate detection/FM200 zone under raised floors
- Preaction dry pipe system zoned to release water only where needed
- Easily removable access panels in raised flooring
- Flood sensors and monitoring under raised floors and in other critical areas
- Separate grounding systems to prevent grounding loops; true ground versus green wire ground
- Sealed cable vault entrances to facility, remotely monitored
- Formalized physical facility preventive maintenance program
- Sub-breakers per relay rack or lineup
- 48 VDC power converters, 220 VAC, 20A, 30A, 40A
- Power filtering in UPS system

### 7.2 Physical Security

- Written security policies readily accessible:
  - Badge sharing and piggy back entry rules
  - All visitors must be admitted through reception
  - Written statement of work upon sign-in
- Building access procedures:
  - Limited number of building entrances in compliance with local fire ordinance
  - Provide access to limited and managed security policies for all facility entrances
  - 24x7 onsite security guards
  - Visitor-logging procedure
  - Card-key, biometric, or similar entry locks
  - ID-badge system for all employees and visitors
  - Staff and visitors must wear badges at all times on premises
- Individual cabinet locks; master in NOC; key list from customer

- Equipment locations:
  - Video surveillance and motion sensors for entrances, interior doors, equipment cages, and critical equipment locations within the building
  - Locked cages with ceilings; locking cabinets with climate control for those wanting more privacy
  - Secure rooms available
  - Managed firewall services with 24x7 monitoring available
  - Backup lighting systems for entry ways and cable vaults
  - Individual cabinet locks; master in NOC; key list from customer

### 7.3 Network Security

- Written network access security policies readily accessible:
  - Password policies (such as not sharing, lengths, forced renewal, aging)
  - Acceptable use (ISP not allowed to run programs that are illicit or illegal; use of sniffers or cracking/hacking programs are not required)
  - Documented user responsibilities on security in company policies and re-enforced by education
  - Asset protection

- Network security infrastructure in place:
  - Perimeter protection (firewalls, filtering router)
  - Intrusion detection
  - Authentication and authorization (passwords, RADIUS/TACACS, Secure IDs)
  - Backup and recovery systems to restore after a problem, such as load balancing, failover protection
  - Regular assessment of network infrastructure
  - Assessment of network expansions or additions
  - Tape or media storage offsite backup
  - Regularly scheduled security audits
  - Server antivirus software protection as relevant

### 7.4 Operations

- Database of all installed equipment and configurations
- Toll-free telephone support
- Supported monitoring:
- 24x7 monitoring of dedicated servers and network equipment (note both frequency and method, such as PING, Simple Network Management Protocol [SNMP])
- 24x7 monitoring of the health of the equipment with alarms and pager alerts for network failure and failovers
- 24x7 monitoring firewall services available
- Alternate NOC available
- Second-tier support personnel located nearby

Trouble ticket processes:
- Created and logged for all unusual or unexpected events

Automated case escalation procedures in place including escalation timeframes

Reporting that provides trending statistics on trouble tickets and minutes (above) to facilitate quality and customer reports

Performance reporting and end-user impact monitoring

Periodic and exception reports provided to customers (including usage and problem reports)

Spare equipment on site for key networking equipment available in case of hardware failure

Business continuity plan:
- Daily site backups
- Tape vaults or other secure storage facilities on site in case of natural disaster
- Onsite and offsite storage available

Customer callout and escalation database

Intercom system

Written procedures for each customer on alarm handling

7.5 **Backbone Connectivity**

- Multiple direct connections to Tier 1 Internet carriers using high speed routers as gateways
- Border Gateway Protocol vs. 4 BGP-4 routing
- Class C Internet address blocks available
- Each carrier has a secure termination area, and location supported via the NOC or the carrier providing the termination
- Fiber enters the data center through diverse conduits or routes (for example, if a backhoe cuts though conduit, the network reroutes to minimize loss of service)
- Aggregate bandwidth sufficient to scale the network to meet customer’s service demands
- Describe policy on facility utilization or over-subscription
- Provider must have private facilities connecting to other data centers, and a documented process
- Multiple Internet access
- Carrier XCONN and distribution system; separate carrier point-of-presence (POP) area
- Formalized SLA policies
- Roof rights and riser conduit right of way
- Multiple riser conduit from cable vault to data center

### 7.6 Gateway/WAN Edge Layer
- High-end routers (such as Cisco 7500 or 12000 Series) in a redundant configuration
- Router redundancy protocol implemented (Virtual Router Redundancy Protocol, RFC #3768)
- BGP-4 implemented (http://www.ietf.org/rfc/rfc1771.txt)
- Adequate total packet-per-second capacity for peak customer load
- Firewalls in place
- Network security team in place
- Remote firewall management offered

### 7.7 Core Layer
- High-end switches (such as Cisco Catalyst® 8500 or 6500 Series) deployed
- Switching and links entirely redundant with no single points or paths of failure
- Web cache redirection implemented
- Content and Transmission Control Protocol (TCP) offloading implemented via reverse proxy caching
- VRRP implemented for fail-over protection
- Intrusion detection implemented
- Automatic notification of intrusion attempts in place

### 7.8 Distribution Layer
- High to mid-range switches (such as Cisco Catalyst 6500 or 6000 Series) deployed
- Switching and links entirely redundant with no single points or paths of failure
- Caching systems (such as Cisco 500 Content Engine or 7300 Series) implemented
- Server load balance (Cisco CSS 11000 Series) implemented
- Server content routing (Cisco 4400 series) implemented if multiple data centers

### 7.9 Access Layer
- Mid range switches (Cisco Catalyst 6000 or 4000 Series) deployed
- All servers dual homed
7.10 Cabling

- All cable runs located under raised flooring and appropriately marked
- All cable runs physically protected from damage via tie-downs or where appropriate in conduit
- All cabling designed to Category 6 specifications (to support 1-Gbps data rates)
- Communications cabling raceways separate from electrical; no intersections
- Shielded cabling for T1/T3s. DSX panels for XCONN, demarcation, and test points
- All cabling on raceways, tied down
8. Appendix
8. APPENDIX

8.1 Appendix A

8.1.1 Routing Protocols

Implementation of standards provides an avenue for integration and interoperability. Legacy routing protocols such as RIP, OSPF, ISIS, and BGP must all be supported to help ensure smooth integration of products into existing infrastructures. Standards also enable support and interoperability of new protocols. In today's high-performance networks, organizations need the freedom to implement packet forwarding and routing according to their own defined policies in a way that goes beyond traditional routing protocol concerns. Where administrative issues dictate that traffic be routed through specific paths, policy-based routing (PBR) can provide the solution. By using PBR, agencies and departments can implement policies that selectively cause packets to take different paths. PBR provides a mechanism for expressing and implementing forwarding/routing of data packets based on policies defined by network administrators. It provides a more flexible mechanism for routing packets through routers, complementing the existing mechanism provided by routing protocols.

Routers forward packets to the destination addresses based on information from static routes or dynamic routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System to Intermediate System (ISIS), or Enhanced Interior Gateway Routing Protocol (Enhanced IGRP). Instead of routing by the destination address, PBR allows network administrators to determine and implement routing policies to allow or deny paths based on the following:

- Identity of a particular end system
- Application
- Protocol
- Size of packets

Policies can be defined as simply as “my network will not carry traffic from the engineering department” or as complex as “traffic originating within my network with the following characteristics will take path A, while other traffic will take path B.”

PBR also provides a mechanism to mark packets so that certain kinds of traffic receive differentiated, preferential service when used in combination with queuing techniques enabled through Cisco IOS software. These queuing techniques provide an extremely powerful, simple, and flexible tool to network managers who implement routing policies in their networks.

Traditional IP Communications allows a host to send packets to a single host (unicast transmission) or to all hosts (broadcast transmission). IP Multicast provides a third possibility, allowing a host to send packets to a subset of all hosts as a group transmission. IP Multicast allows better utilization of network bandwidth by allowing the sender to transmit traffic only once, yet going to many destinations; only the members of a specific multicast group receive the traffic.

This overview provides a brief summary of IP Multicast. First, general topics such as multicast group concept, IP Multicast addresses, and Layer 2 multicast addresses are discussed. Then intradomain multicast protocols are reviewed, such as Internet Group Management Protocol (IGMP), Cisco Group Management Protocol,
Protocol Independent Multicast (PIM), and Pragmatic General Multicast (PGM). Finally, interdomain protocols are covered, such as Multiprotocol Border Gateway Protocol (MBGP), Multicast Source Directory Protocol (MSDP), and Source Specific Multicast (SSM).

IP Multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to potentially thousands of recipients. Applications that take advantage of multicast include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

IP Multicast delivers application source traffic to multiple receivers, without burdening the source or the receivers, while using a minimum of network bandwidth. Multicast packets are replicated in the network at the point where paths diverge by routers enabled with PIM and other supporting multicast protocols, resulting in the most efficient delivery of data to multiple receivers.

Many alternatives to IP Multicast require the source to send more than one copy of the data. Some, such as application-level multicast, require the source to send an individual copy to each receiver. Even low-bandwidth applications can benefit from using IP Multicast when there are thousands of receivers. High-bandwidth applications, such as MPEG video, may require a large portion of the available network bandwidth for a single stream. In these applications, IP Multicast is the only way to send to more than one receiver simultaneously.

PIM is IP routing protocol-independent and can leverage whichever unicast routing protocols are used to populate the unicast routing table, including Enhanced EIGRP, OSPF, BGP, and static routes. PIM uses this unicast routing information to perform the multicast forwarding function. Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the RPF check function instead of building up a completely independent multicast routing table. Unlike other routing protocols, PIM does not send and receive routing updates between routers.

Sources register with the rendezvous point and then data is forwarded down the shared tree to the receivers. The edge routers learn about a particular source when they receive data packets on the shared tree from that source through the RP. The edge router then sends PIM (S, G) join messages toward that source. Each router along the reverse path compares the unicast routing metric of the rendezvous point address to the metric of the source address. If the metric for the source address is better, it forwards a PIM (S, G) join message toward the source. If the metric for the rendezvous point is the same or better, then the PIM (S, G) join message is sent in the same direction as the RP. In this case, the shared tree and the source tree are considered congruent.

8.1.2 IGMP Snooping

High performance switches can use another method to constrain the flooding of multicast traffic, IGMP Snooping. IGMP Snooping requires the LAN switch to examine, or “snoop,” some layer 3 information in the IGMP packet sent from the host to the router. When the switch hears an IGMP Report from a host for a particular multicast group, the switch adds the host’s port number to the associated multicast table entry. When it hears an IGMP Leave Group message from a host, it removes the host’s port from the table entry.

On the surface, this seems like a simple solution to put into practice. However, depending on the architecture of the switch, implementing IGMP Snooping may be difficult to accomplish without seriously degrading the performance of the switch. The CPU must examine every multicast frame passing through the switch just to find an occasional IGMP packet. This results in performance degradation to the switch and in extreme cases switch failure. Unfortunately, many low-cost, Layer 2 switches that have implemented IGMP snooping rather than CGMP suffer from this problem. The switch may perform IGMP Snooping just fine in a limited demo environment, but when the buyer puts it into production networks with high-bandwidth multicast streams, it melts down under load.

The only viable solution to this problem is a high-performance switch designed with special ASICs that can examine the Layer 3 portion of all multicast packets at line-rate to determine whether or not they are IGMP packets.
8.1.3 Distribution Trees

IP multicast traffic flows from the source to the multicast group over a distribution tree that connects all of the sources to all of the receivers in the group. This tree may be shared by all sources (a shared-tree), or a separate distribution tree can be built for each source (a source-tree). The shared-tree may be one-way or bidirectional.

Applications send one copy of each packet using a multicast address, and the network forwards the packets to only those networks, LANs, that have receivers.

Source trees are constructed with a single path between the source and every LAN that has receivers. Shared-trees are constructed so that all sources use a common distribution tree. Shared-trees use a single location in the network to which all packets from all sources are sent and from which all packets are sent to all receivers.

These trees are loop-free. Messages are replicated only when the tree branches.

Members of multicast groups can join or leave at any time, so the distribution tree must be dynamically updated. Branches with no listeners are discarded (pruned). The type of distribution tree used and the way multicast routers interact depend on the objectives of the routing protocol, including receiver distribution, number of sources, reliability of data delivery, speed of network convergence, shared-path or source path, and if shared path, direction of data flow.

8.1.3.1 Tree Structure

Distribution trees may be formed as either source-based trees or shared trees. Source-based distribution trees build an optimal shortest-path tree rooted at the source. Each source/group pair requires its own state information, so for groups with a very large number of sources, or networks that have a very large number of groups with a large number of sources in each group, the use of source-based trees can stress the storage capability of routers.

Shared distribution trees are formed around a central router, called a rendezvous point or core, from which all traffic is distributed regardless of the location of the traffic sources. The advantage of shared distribution trees is that they do not create lots of source/group state in the routers. The disadvantage is that the path from a particular source to the receivers may be much longer, which may be important for delay-sensitive applications. The rendezvous router may also be a traffic bottleneck if there are many high data rate sources.
8.1.3.2 Distribution of Receivers

One criterion to determine what type of tree to use relates to whether receivers are sparsely or densely distributed throughout the network (for example, whether almost all of the routers in the network have group members on their directly attached subnetworks). If the network has receivers or members on every subnet or the receivers are closely spaced, they have a dense distribution. If the receivers are on only a few subnets and are widely spaced, they have a sparse distribution. The number of receivers does not matter; the determining factor is how close the receivers are to each other and the source.

Sparse-mode protocols use explicit join messages to set up distribution trees so that tree state is set up only on routers on the distribution tree and data packets are forwarded to only those LANs that have hosts who join the group. Sparse-mode protocols are thus also appropriate for large internetworks where dense-mode protocols would waste bandwidth by flooding packets to all parts the internetwork and then pruning back unwanted connections. Sparse-mode protocols may build either shared trees or source trees or both types of distribution trees. Sparse-mode protocols may be best compared to a magazine subscription since the distribution tree is never built unless a receiver joins (subscribes) to the group.

Dense mode protocols build only source-distribution trees. Dense mode protocols determine the location of receivers by flooding data throughout your network and then explicitly pruning off branches that do not have receivers therefore creating distribution state on every router in your network. Dense mode protocols may use fewer control messages to set up state than sparse-mode protocols, and they may be able to better guarantee delivery of data to at least some group members in the event of some network failures. Dense mode protocols may be compared to junk mail in that every network will receive a copy of the data whether they want it or not.

8.1.4 IP Multicast Routing Protocols

In addition, there are several multicast routing protocols including Protocol Independent Multicast (PIM), Core Based Trees (CBT), and Multicast Open Shortest Path First (MOSPF).

8.1.4.1 Protocol Independent Multicast (PIM)

PIM can support both dense mode and sparse mode groups. Protocol Independent Multicast (PIM) can service both shared trees and shortest path trees. PIM can also support bi-directional trees. PIM is being enhanced to support explicit joining toward sources so that once an alternative method of discovering sources is defined, PIM will be able to take advantage of it. PIM-SM (Sparse Mode) Version 2 is an IETF standard: RFC # 2362. PIM-DM (Dense Mode) is an IETF draft.

PIM uses any unicast routing protocol to build the data distribution trees. PIM is the only multicast routing protocol deployed on the Internet to distribute multicast data natively and not over a bandwidth-limited, tunneled topology.

8.1.4.2 Protocol Independent Multicast-Sparse Mode (PIM-SM)

PIM Sparse Mode can be used for any combination of sources and receivers, whether densely or sparsely populated, including topologies where senders and receivers are separated by WAN links, and/or when the stream of multicast traffic is intermittent.

- Independent of unicast routing protocols—PIM can be deployed in conjunction with any unicast routing protocol.
- Explicit-join—PIM-SM assumes that no hosts want the multicast traffic unless they specifically ask for it. It creates a shared distribution tree centered on a defined “rendezvous point” (RP) from which source traffic is relayed to the receivers. Senders first send the data to the RP, and the receiver's last-hop router sends a join message toward the RP (explicit join).
- Scalable—PIM-SM scales well to a network of any size including those with WAN links. PIM-SM
domains can be efficiently and easily connected together using MBGP and MSDP to provide native multicast service over the Internet.

- Flexible—A receiver's last-hop router can switch from a PIM-SM shared tree to a source-tree or shortest-path distribution tree whenever conditions warrant it, thus combining the best features of explicit-join, shared-tree and source-tree protocols.

### 8.1.4.3 Protocol Independent Multicast-Dense Mode (PIM-DM)

PIM dense mode (PIM-DM) initially floods all branches of the network with data, then prunes branches with no multicast group members. PIM-DM is most effective in environments where it is likely that there will be a group member on each subnet. PIM-DM assumes that the multicast group members are densely distributed throughout the network and that bandwidth is plentiful.

PIM-DM creates source-based shortest-path distribution trees; it cannot be used to build a shared distribution tree.

### 8.1.4.4 Bidirectional PIM (bidir-PIM)

Bidirectional PIM (bidir-PIM) is an enhancement of the PIM protocol that was designed for efficient many-to-many communications within an individual PIM domain. Multicast groups in bidirectional mode can scale to an arbitrary number of sources with only a minimal amount of additional overhead.

The shared trees that are created in PIM-SM are unidirectional. This means that a source tree must be created to bring the data stream to the rendezvous point (the root of the shared tree) and then it can be forwarded down the branches to the receivers. Source data cannot flow up the shared tree toward the RP, as this would be considered a bidirectional shared tree.

In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the rendezvous point for the group. In bidir-PIM, the IP address of the rendezvous point acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address need not be a router address, but can be any unassigned IP address on a network that is reachable throughout the PIM domain.

MBGP provides a method for providers to distinguish which route prefixes they will use for performing multicast RPF checks. The RPF check is the fundamental mechanism that routers use to determine the paths that multicast forwarding trees follow and to successfully deliver multicast content from sources to receivers.
MSDP was developed for peering between Internet service providers (ISPs). ISPs did not want to rely on an rendezvous point maintained by a competing ISP to provide service to their customers. MSDP allows each ISP to have its own local rendezvous point and still forward and receive multicast traffic to the Internet.

MSDP enables rendezvous points to share information about active sources. Rendezvous points know about the receivers in their local domain. When rendezvous points in remote domains hear about the active sources, they can pass on that information to their local receivers and multicast data can then be forwarded between the domains. A useful feature of MSDP is that it allows each domain to maintain an independent rendezvous point that does not rely on other domains. MSDP gives the network administrators the option of selectively forwarding multicast traffic between domains or blocking particular groups or sources. PIM-SM is used to forward the traffic between the multicast domains.

The rendezvous point in each domain establishes an MSDP peering session using a TCP connection with the rendezvous points in other domains or with border routers leading to the other domains. When the rendezvous point learns about a new multicast source within its own domain (through the normal PIM register mechanism), the rendezvous point encapsulates the first data packet in a Source-Active (SA) message and sends the message to all MSDP peers. MSDP uses a modified RPF check in determining which peers should be forwarded the SA messages. This modified RPF check is done at a SA level instead of a hop-by-hop metric. The message is forwarded by each receiving peer, also using the same modified RPF check, until the message reaches every MSDP router in the internetwork-theoretically, the entire multicast Internet. If the receiving MSDP peer is a rendezvous point, and the rendezvous point has a (*, G) entry for the group in the message (that is, there is an interested receiver), the rendezvous point creates (S, G) state for the source and joins to the shortest path tree for the source. The encapsulated data is decapsulated and forwarded down the shared tree of that rendezvous point. When the packet is received by the last hop router of the receiver, the last hop router also may join the shortest path tree to the source. The MSDP speaker periodically sends messages that include all sources within the own domain of the rendezvous point.

8.1.4.5 Protocol Dependent Multicast Choices

Protocol Dependent Multicast, in contrast to PIM, requires building routing tables that support either distance vector (e.g., Distance Vector Multicast Routing Protocol, DVMRP) or link-state (e.g., Multicast Open Shortest Path First, MOSPF) routing algorithms.

- Distance Vector Multicast Routing Protocol (DVMRP)—DVMRP was the first multicast routing protocol developed. DVMRP must calculate and exchange its own RIP-like routing metrics so it cannot take advantage of the enhancements and capabilities of advanced routing protocols such as OSPF, IS-IS and EIGRP. It is dense-mode and so must flood data throughout the network and then prune of branches so that state for every source is created on every router in your network.

- Multicast Open Shortest Path First (MOSPF)—MOSPF is an extension to the OSPF unicasting routing protocol. OSPF works by having each router in a network understand all of the available links in the network. Each OSPF router calculates routes from itself to all possible destinations. MOSPF works by including multicast information in OSPF link-state advertisements so that an MOSPF router learns which multicast groups are active on which LANs. MOSPF builds a distribution tree for each source/group pair and computes a tree for active sources sending to the group. The tree state must be recomputed whenever link state change occurs. If there are many sources and/or many groups, this calculation, called the Dijkstra algorithm, must be recomputed for every source/group combination which can be very CPU intensive.

MOSPF incorporates the scalability benefits of OSPF but can only run over OSPF routing domains. It is best used when relatively few source/group pairs are active at any given time, since all routers must build each distribution tree. It does not work well where unstable links exist. It can be deployed gradually since MOSPF routers can be combined in the same routing domain with non-multicast OSPF routers. It is not widely implemented and does not support tunneling.
- Other Protocols—Other protocols exist that are designed for research purposes, such as Core Based Trees (CBT), Simple Multicast, Express Multicast, etc. CBT and Simple Multicast, a variation of CBT, support only shared trees.

EXPRESS supports source trees only and must be implemented on every host to initiate construction of the data path. EXPRESS assumes that receivers will learn about receivers via some mechanism outside of the EXPRESS protocol. EXPRESS does not use IGMP.

8.1.4.6 Reverse Path Forwarding (RPF)

Reverse Path Forwarding (RPF) is an algorithm used for forwarding multicast datagrams. The algorithm works as follows:

- The packet has arrived on the RPF interface if a router receives it on an interface that it uses to send unicast packets to the source.
- If the packet arrives on the RPF interface, the router forwards it out the interfaces that are present in the outgoing interface list of a multicast routing table entry.
- If the packet does not arrive on the RPF interface, the packet is silently discarded to avoid loop-backs.

If a PIM router has source tree state, it does the RPF check using the source IP address of the multicast packet. If a PIM router has shared tree state, it uses the RPF check on the rendezvous point’s (RP) address (which is known when members join the group).

Sparse-mode PIM uses the RPF lookup function to determine where it needs to send Joins and Prunes. Shared-tree state joins are sent towards the RP. Source-tree state joins are sent towards the source.

Dense-mode DVMRP and PIM groups use only source-rooted trees and make use of RPF forwarding as described above. MOSPF does not necessarily use RPF since it can compute both forward and reverse shortest path source-rooted trees by using the Dijkstra computation.

8.1.5 Interdomain Multicast Routing

8.1.5.1 Multicast Border Gateway Protocol

Multicast Border Gateway Protocol (MBGP) offers a method for providers to distinguish which prefixes they will use for performing multicast reverse path forwarding (RPF) checks. The RPF check is fundamental in establishing multicast forwarding trees and moving multicast content successfully from source to receiver(s).

MBGP is based on RFC 2283, Multiprotocol Extensions for BGP-4. This brings along all of the administrative machinery that providers and customers like in their inter-domain routing environment. Examples include all of the AS machinery and the tools to operate on it (e.g., route maps). Therefore, by using MBGP, any network utilizing internal or external BGP can apply the multiple policy control knobs familiar in BGP to specify routing (and therefore forwarding) policy for multicast.

Two path attributes, MP_REACH_NLRI and MP_UNREACH_NLRI, are introduced to yield BGP4+ as described in Internet Draft draft-ietf-idr-bgp4-multiprotocol-01.txt. MBGP is a simple way to carry two sets of routes—one set for unicast routing and one set for multicast routing. The routes associated with multicast routing are used by the multicast routing protocols to build data distribution trees.

The advantages are that an internet can support non-congruent unicast and multicast topologies and, when the unicast and multicast topologies are congruent, can support differing policies. MBGP provides for scalable policy-based inter-domain routing that can be used to support non-congruent unicast and multicast forwarding paths.
8.1.5.2 Multicast Source Discovery Protocol

Multicast Source Discovery Protocol (MSDP) is a mechanism to connect PIM-SM domains to enable forwarding of multicast traffic between domains while allowing each domain to use its own independent rendezvous points (RPs) and not rely on RPs in other domains.

The RP in each domain establishes an MSDP peering session using a TCP connection with the RPs in other domains or with border routers leading to the other domains. When the RP learns about a new multicast source within its own domain (through the normal PIM register mechanism), the RP encapsulates the first data packet in a Session Advertisement (SA) and sends the SA to all MSDP peers. The SA is forwarded by each receiving peer using a modified RPF check, until it reaches every MSDP router in the internet. If the MSDP peer is an RP, and the RP has a (*,G) entry for the group in the SA, the RP will create (S,G) state for the source and join to the shortest path for the source. The encapsulated packet is decapsulated and forwarded down that RP's shared-tree. When the packet is received by a receiver's last hop router, the last-hop may also join the shortest path to the source. The source's RP periodically sends SAs which include all sources within that RP's own domain.

MSDP peers may be configured to cache SAs to reduce join latency when a new receiver joins a group within the cache.

8.1.5.3 Reliable Multicast

Reliable multicast protocols overcome the limitations of unreliable multicast datagram delivery and expand the use of IP multicast. IP multicast is based on UDP in which no acknowledgments are returned to the sender. The sender therefore does not know if the data it sends are being received, and the receiver cannot request that lost or corrupted packets be retransmitted. Multimedia audio and video applications generally do not require reliable multicast, since these transmissions are tolerant of a low level of loss. However, some multicast applications require reliable delivery.

Some elements that are relevant to deciding whether reliable multicast is applicable include the degree of reliability required, requirements for bandwidth and for ordered packet delivery, the burstiness of data, delay tolerance, timing (real-time vs. non-real-time), the network infrastructure (LAN, WAN, Internet, satellite, dial-up), heterogeneity of links in the distribution tree, router capabilities, number of senders and size of multicast group, scalability, and group setup protocol.

Reliable multicast will be useful in areas where loss is not tolerated or where a high-degree of fidelity is required, as for example, in such areas as bulk data transfer, inventory updates, financial stock quotes, data conferencing, hybrid broadcasting (Whiteboard), software distribution, push (Webserver content), data replication, caching, and distributed simulation. Reliable multicast applications are also frequently deployed over satellite networks with terrestrial (e.g., Internet) back channels.

8.1.6 Mobility

Mobile IP is an open standard, defined by the Internet Engineering Task Force (IETF) RFC 2002, that 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.

In IP networks, routing is based on stationary IP addresses, similar to how a postal letter is delivered to the fixed address on an envelope. A device on a network is reachable through normal IP routing by the IP address it is assigned on the network.

The problem occurs when a device roams away from its home network and is no longer reachable using normal IP routing. This results in the active sessions of the device being terminated. Mobile IP was created to enable users to keep the same IP address while traveling to a different network (which may even be on a different
wireless operator), ensuring that a roaming individual could continue communication without sessions or connections being dropped.

Because the mobility functions of Mobile IP are performed at the network layer rather than the physical layer, the mobile device can span different types of wireless networks while maintaining connections and ongoing applications. Remote login, remote printing, and file transfers are some examples of applications where it is undesirable to interrupt communications while an individual roams across network boundaries. Also, certain network services, such as software licenses and access privileges, are based on IP addresses. Changing these IP addresses could compromise the network services.

Network mobility is enabled by Mobile IP, which provides a scalable, transparent, and secure architecture. It is scalable because only the participating components need to be Mobile-IP aware—the mobile node and the endpoints of the tunnel. No other routers in the network or any hosts with which the mobile node is communicating need to be changed or even aware of the movement of the mobile node. It is transparent to any applications while providing mobility. Also, the network layer provides link-layer independence, interlink layer roaming, and link-layer transparency. Finally, it is secure because the setup of packet redirection is authenticated.

### 8.1.7 MPLS

MPLS complements IP technology. It is designed to leverage the intelligence associated with IP routing and the switching paradigm associated with ATM. MPLS consists of a control plane and a forwarding plane. The control plane builds what is called a forwarding table, while the forwarding plane forwards packets to the appropriate interface (based on the forwarding table).

The efficient design of MPLS uses labels to encapsulate IP packets. A forwarding table lists label values, which are each associated with determining the outgoing interface for every network prefix.

MPLS TE was initially envisioned as technology that would enable service providers to better utilize the available network bandwidth by using alternate paths (i.e., other than the shortest path). It has evolved to provide multiple benefits, including connectivity protection using fast reroute and tight QoS. Tight QoS results from using MPLS TE and QoS mechanisms together.

MPLS TE uses IGP, IS-IS, and OSPF to flood bandwidth information through a network. It also uses RSVP extensions to distribute labels and constraint-based routing to compute paths in the network. These extensions are defined in RFC3209.

Service providers that deploy MPLS TE tend to deploy a full mesh of TE tunnels. This creates a logical mesh, even when a physical topology is not a full mesh. In this environment, service providers have noticed an additional 40% to 50% bandwidth availability on the network. This gain is optimal network usage, which leads to a reduction in CapEx.

MPLS TE provides connectivity protection using FRR. FRR protects primary tunnels by using pre-provisioned backup tunnels. During a failure condition, it takes approximately 50 milliseconds for the primary tunnel to switch over to the backup tunnel. FRR is dependent on Layer 3 protection, unlike SONET or SDH protection that occurs at the interface level. The restoration time is therefore dependent on the number of tunnels and the number of prefixes being switched over.

Today's government agencies are deploying applications that require guaranteed levels of service in the network. Voice, video, as well as control systems and other mission-critical applications will not tolerate the delays and packet loss of a best-effort network. To meet the needs of these applications, agencies are turning to QoS mechanisms in their networks. The next section examines the state of QoS tools in the networking industry today and discusses how they can be deployed to protect mission-critical applications.
8.1.8 Goals in QoS

QoS in a shared network infrastructure is essential to provide the service levels required by and contracted for by customers or tenants. It is also essential to maintain the health of the network to help ensure traffic is transported or dropped based on the policies established by the provider.

QoS tools aim to provide preferred, and in some cases guaranteed, service to certain applications in the network. Typically network characteristics such as latency, jitter, and packet loss are the main concerns of these tools as they work to protect mission critical applications. Although packet loss, and its effect on applications, is the most commonly thought of negative attribute of networks, latency and jitter may not be as well understood.

Latency is defined as the end-to-end delay in the network from one endpoint to another. There are two types of latency that need to be considered when designing a network, static latency and dynamic latency. Static latency values do not change from one moment to the next and is the easiest to deal with when designing a network. This type of delay includes propagation delay and serialization delay. Dynamic latency can, and does, change from one moment to the next. This type of delay includes forwarding delay and buffering delay.

Jitter indicates the change in delay. For example, imagine two endpoints on a network. Endpoint A sends a packet to endpoint B. The delay for this packet is 100 milliseconds. Endpoint A then sends a second packet to endpoint B that takes 125 milliseconds. The difference between these values is the jitter, 25 milliseconds in this example. Due to its very dynamic nature, jitter is much more difficult to control and its effects can be devastating to real-time applications such as voice and video.

The primary cause of delay in networks is congestion. In a congestion-free network, every packet gets services immediately by the switches and routers in the network and there is no need for QoS. Unfortunately, networks are designed to be inherently oversubscribed and congestion is almost inevitable. It is important to note that congestion has no relationship to the backplane speed of the devices in the network. Even switches with the most powerful backplanes will experience congestion and must be capable of supporting QoS tools. Hence, QoS aims at buffer management of the network devices.

There are two categories of tools that are available to assist with congestion, congestion avoidance mechanisms and congestion control mechanisms. As their names imply, congestion avoidance mechanisms aim to prevent congestion and congestion control mechanisms help mediate the effects of congestion when it occurs.

- Congestion avoidance—Random Early Detect (RED) and Weighted Random Early Detect (WRED)
- Congestion control—Priority Queuing (PQ), Class-Based Queuing (CQ), Weighted Fair Queuing (WFQ), and Low-Latency Queuing (LLQ)
Bandwidth, delay, jitter, and packet loss can be effectively controlled. By ensuring the desired results, QoS features lead to efficient, predictable services for business-critical applications.

Using the QoS feature set, agencies can build networks that conform to either the IETF Integrated Services (IntServ) model and/or the Differentiated Services (DiffServ) model. QoS features also provide value-added functionality such as network-based application recognition (NBAR) for classifying traffic on an application basis, a service assurance agent (SAA) for end-to-end QoS measurements, and RSVP signaling for admission control and reservation of resources.

There are two broad categories of QoS tools available today:

- IntServ
- DiffServ

These techniques try to deliver the same preference for high-priority traffic, but use vastly different mechanisms. IntServ is a signaling-based mechanism that gives applications the ability to negotiate a contract with the network, guaranteeing that their needs are met. DiffServ is a mechanism that defines simple labels for distinguishing between packets from different applications, so that priority can be given to important traffic.

8.1.8.1 IntServ

IntServ is a technique that allows applications and end stations to request levels of service from the network. This is useful in that the end stations negotiate with each other and the network to establish transmission parameters for that stream. IntServ follows the signaled-QoS model, where the end-hosts signal their QoS needs to the network. The most common application of IntServ is the RSVP. RSVP allows requests to be made for characteristics such as bandwidth, latency, and jitter. These requests are made on behalf of an application and sent to the network where they are processed. The network devices along the path to the destination (switches, routers, etc.) examine the request and compare its requirements against the available resources. If all devices along the path to the destination can meet the request, then the network accepts it and the application
can be assured that the parameters of its request will be met. If the network cannot meet the request, then it is rejected and the application must change its requirements and resignal the network.

8.1.8.2 DiffServ

DiffServ is a packet-tagging scheme that labels packets relative to one another. These labels are then used during times of network congestion to make queuing and discard decisions. DiffServ works on the provisioned-QoS model where network elements are set up to service multiple classes of traffic with varying QoS requirements. DiffServ actually got its start in the first iterations of the TCP/IP protocol in the 1970s. The Type of Service field in the IP header contains three bits that can be used to label packets. These values, now called IP Precedence, are in wide use today to provide priority to mission-critical applications.

In the mid 1990s, the IEE formed a working group to expand the capabilities of IP Precedence. That group, the Differentiated Services Working Group, defined a total of 6 bits in the Type of Service field of the IP header to be the Differentiated Services Code Point (DSCP). This expanded number of bits allows for 64 classes to be defined for application differentiation. Thirty-two DSCPs are reserved for future use and thirty-two are available for use today. The DSCPs are broken into 3 different Per Hop Behaviors (PHBs): Expedited Forwarding, Assured Forwarding, and Default PHBs. The Default PHB has the lowest priority (0) and is handled as best-effort traffic. The Expedited Forwarding PHB is the highest-priority traffic (46) and receives prioritized handling in the network.

8.1.8.3 IntServ or DiffServ—Which to Deploy?

DiffServ is the most widely deployed QoS model in networks today. This section examines why the differentiated services model has become so popular and how and why the IntServ model is resurfacing.

DiffServ services mechanisms, namely IP Precedence values, have been around since IP was developed in the 1970s. Those bits, however, went unused for more than two decades since applications on the network did not require different levels of service.

The IETF completed the request for comments (RFCs) for DiffServ toward the end of 1998. As stated in the DiffServ working group objectives [Ref-C], “There is a clear need for relatively simple and coarse methods of providing differentiated classes of service for Internet traffic, to support various types of applications, and specific business requirements. The differentiated service approach to providing quality of service in networks employs a small, well-defined set of building blocks from which a variety of aggregate behaviors may be built. A small bit-pattern in each packet, in the IPv4 To octet or the IPv6 Traffic Class octet, is used to mark a packet to receive a particular forwarding treatment, or per-hop behavior, at each network node.

A common understanding about the use and interpretation of this bit-pattern is required for inter-domain use, multi-vendor interoperability, and consistent reasoning about expected aggregate behaviors in a network. Thus, the working group has standardized a common layout for a six-bit field of both octets, called the DS field. RFC 2474 and RFC 2475 define the architecture, and the general use of bits within the DS field (superseding the IPv4 ToS octet definitions of RFC 1349).”

To deliver end-to-end QoS, this architecture (RFC-2475) has two major components, Packet Marking using the IPv4 ToS byte and PHBs.

8.1.8.4 Packet Marking

Unlike the IP Precedence architecture, the ToS byte is completely redefined. Six bits are now used to classify packets. The field is now called the DS (Differentiated Services) Field, with two of the bits unused (RFC-2474). The 6 bits replace the three IP Precedence bits and is called the DSCP. With DSCP, in any given node, up to 64 different aggregates/classes can be supported ($2^6$). All classification and QoS revolves around the DSCP in the DiffServ model.
8.1.8.5 PHBs

Now that packets can be marked using the DSCP, how do we provide meaningful classification on flows (CoS) and provide the required QoS? First, the collection of packets that have the same DSCP value (also called a codepoint) in them and crossing in a particular direction is called a Behavior Aggregate (BA). Thus, packets from multiple applications/sources could belong to the same BA. Formally, RFC-2475 defines a PHB as the externally observable forwarding behavior applied at a DS-compliant node to a DS behavior aggregate. In more concrete terms, a PHB refers to the packet scheduling, queuing, policing, or shaping behavior of a node on any given packet belonging to a BA and as configured by an SLA or policy. To date, four standard PHBs are available to construct a DiffServ-enabled network and achieve coarse-grained, end-to-end CoS and QoS:

8.1.8.6 Default PHB (Defined in RFC-2474)

The default PHB essentially specifies that a packet marked with a DSCP value (recommended) of ‘000000’ gets the traditional best effort service from a DS-compliant node (a network node that complies to all the core DiffServ requirements). Also, if a packet arrives at a DS-compliant node and its DSCP value is not mapped to any of the other PHBs, it is mapped to the default PHB.

8.1.8.7 Class-Selector PHBs (Defined in RFC-2474)

To preserve backward compatibility with the IP Precedence scheme, DSCP values of the form ‘xxx000’ where x is either 0 or 1, are defined. These codepoints are called class-selector codepoints. Note that the default codepoint is also a class-selector codepoint (‘000000’). The PHB associated with a class-selector codepoint is a class-selector PHB. These PHBs retain almost the same forwarding behavior as nodes that implement IP Precedence-based classification and forwarding.

As an example, packets with a DSCP value of ‘110000’ (IP Precedence 110) have a preferential forwarding treatment (scheduling, queuing, etc.) as compared to packets with a DSCP value of ‘100000’ (IP Precedence 100). These PHBs ensure that DS-compliant nodes can co-exist with IP Precedence aware nodes, with the exception of the DTS bits.

8.1.8.8 Expedited Forwarding PHB (Defined in RFC-2598)

Just as RSVP, via the IntServ model, provides for a guaranteed bandwidth service, the Expedited Forwarding (EF) PHB is the key ingredient in DiffServ for providing a low-loss, low-latency, low-jitter, and assured bandwidth service. Applications such as VoIP, video, and online trading programs require such a robust network treatment. EF can be implemented using priority queuing, along with rate limiting on the class (formally, a BA). Although EF PHB, when implemented in a DiffServ network, provides a premium service, it should be specifically targeted toward the most critical applications, since if congestion exists, it is not possible to treat all or most traffic as high priority. EF PHB is especially suitable for applications (like VoIP) that require very low packet loss, guaranteed bandwidth, low delay, and low jitter. The recommended DSCP value for EF is ‘101110’ (RFC-2474).

8.1.8.9 Assured Forwarding PHB (Defined in RFC-2597)

The rough equivalent of the IntServ Controlled Load Service is the Assured Forwarding (AFxy) PHB. It defines a method by which BAs can be given different forwarding assurances. For example, traffic can be divided into gold, silver, and bronze classes, with gold being allocated 50 percent of the available link bandwidth, silver 30 percent, and bronze 20 percent.

The AFxy PHB defines four AFx classes, AF1, AF2, AF3, and AF4. Each class is assigned a certain amount of buffer space and interface bandwidth, dependent on the SLA with the service provider/policy. Within each AFx class, it is possible to specify three drop precedence values. Thus, if there is congestion in a DS-node on a specific link, and packets of a particular AFx class (say AF1) need to be dropped, packets in AFxy are dropped such that the dP(AFx1) <= dP(AFx2) <= dp(AFx3), where dP(AFxy) is the probability that packets of the AFxy
class are dropped. Thus, the subscript “y” in AFxy denotes the drop precedence within an AFx class. In our example, packets in AF13 are dropped before packets in AF12 and before packets in AF11. This concept of drop precedence is useful, for example, to penalize flows within a BA that exceed the assigned bandwidth. Packets of these flows could be re-marked by a policer to a higher drop precedence. The in previous section shows the DSCP values for each class and drop precedence. And AFx class can be denoted by the DSCP ‘xyzab0’, where ‘xyz’ is 001 / 010 / 011 / 100, and ‘ab’ represents the drop precedence bits (RFC-2597).

8.1.8.10 DiffServ Issues—The Challenges

Although DiffServ is powerful in enabling scalable and coarse-grained QoS throughout the network, it has some drawbacks which present both challenges for tomorrow and opportunities for enhancements and simplification of QoS delivery:

- Provisioning—Unlike RSVP/IntServ, DiffServ needs to be provisioned. Setting up the various classes throughout the network requires knowledge of the applications and traffic statistics for aggregates of traffic on the network. This process of application discovery and profiling can be time-consuming, although tools such as NBAR application discovery, protocol analyzers, and RMON probes can simplify it a bit.

- Billing and monitoring—Management remains an issue. Even though packets/sec., bytes/sec., and many other counters are available via the class-based Management Information Base (MIB), billing and monitoring are still difficult. For example, it may not be sufficient to prove to a customer that 9 million VoIP packets got the EF PHB treatment at all times, since it is possible that the qualitative nature of the calls that the customer made were very poor.

- Loss of granularity—Even though QoS assurances are being made at the class level, it may be necessary to drill down to the flow level to provide the requisite QoS. For example, although all HTTP traffic may have been classified as gold and assigned a bandwidth of 100Mbps, there is no inherent mechanism to ensure that a single flow does not use up that allocated bandwidth. It is also not easy (although not impossible) to ensure that, for example, the manufacturing department’s HTTP traffic gets priority before another department’s HTTP traffic. The MQC allows you to define hierarchical policies to accomplish this, however it is not generic enough to control it at a flow/granular level.

- QoS and routing—One of the biggest drawbacks of both the IntServ and DiffServ models derives from the fact that signaling/provisioning happens separately from the routing process. Thus, there may exist a path (other than the non-default IGP, such as OSPF, ISIS, EIGRP, and so on)/EGP, such as BGP-4, path in the network that has the required resources, even when RSVP/DiffServ fails to find the resources. This is where traffic engineering and MPLS come into play. True QoS with maximum network utilization will arrive with the marriage of traditional QoS and routing.

IntServ, in the form of RSVP, was very prevalent in the media in the mid 1990s. However ATM and RSVP were difficult to deploy and very cumbersome to manage. RSVP began to run into scalability issues in the core of networks where devices had to keep track of hundreds of thousands of reservations (and their associated flows), as well as switching packets.

The IETF-defined models, IntServ and DiffServ, are simply two ways of considering the fundamental problem of providing QoS for a given IP packet. The IntServ model relies on RSVP to signal and reserve the desired QoS for each flow in the network. A flow is defined as an individual, unidirectional data stream between two applications and is uniquely identified by the 5-tuple (Source IP address, Source Port#, Destination IP address, Destination Port#, and the Transport Protocol). Two types of service can be requested via RSVP (assuming all network devices support RSVP along the path from the source to the destination). The first type is a very strict guaranteed service that provides for firm bounds on end-to-end delay and assured bandwidth for traffic that conforms to the reserved specifications. The second type is a controlled load service that provides for a better-than-best effort and low-delay service under light to moderate network loads. Thus it is possible (at least
theoretically) to provide the requisite QoS for every flow in the network, provided it is signaled using RSVP and the resources are available. However there are several practical drawbacks to this approach:

- Every device along a packet’s path, including the end systems like servers and PCs, need to be fully aware of RSVP and capable of signaling the required QoS.
- Reservations in each device along the path are “soft,” which means they need to be refreshed periodically, thereby adding to the traffic on the network and increasing the chance that the reservation may time out if refresh packets are lost. Though some mechanisms alleviate this problem, it adds to the complexity of the RSVP solution.
- Maintaining soft-states in each router, combined with admission control at each hop, adds to the complexity of each network node along the path and increased memory requirements to support large numbers of reservations.
- Since state information for each reservation needs to be maintained at every router along the path, scalability with hundreds of thousands of flows through a network core becomes an issue.

DiffServ offered an alternative that was easier to deploy and manage and was able to scale to the largest networks. Although DiffServ has the ability to offer different levels of service to applications, it offers no guaranteed delivery of data. Because of this, the networking industry has turned back towards IntServ as the future of QoS.

8.1.8.11 PEP

PEPs are designed to work with the transport protocol TCP. They are designed to compensate for the long delay networks experience due to congestion, error, or total distance travelled. This technique typically consists of a software protocol and some hardware appliance that must be placed at each end on the link being “accelerated.” Remember, they typically only accelerate TCP-based transmissions, so not all communication benefits from this technique.

Selection of these protocols is also important. There are several available on the market today and typically each is designed for one of the three delay conditions described above. These protocols “spoof” the TCP protocol into thinking that it is receiving the expected acknowledgments within the time window.

The implementation of IPSec in a network poses an issue for PEPs. The IPSec process takes effect prior to the PEP engaging, hence no acceleration occurs. This should be considered when designing placement of PEP appliances and security systems.

8.2 Appendix B

8.2.1 Security Terminology

- Authentication—Determining the origin of information, from an end user or a device such as a host, server, switch, router, etc.
- Data integrity—Ensuring that data was not altered during transit
- Data confidentiality—Ensuring that only the entities allowed to see the data; see it in a usable format
- Encryption—A method of scrambling information in such a way that it is not readable by anyone except the intended recipient, who must decrypt it to read it
- Decryption—A method of unscrambling encrypted information to make it legible
- Key—A digital code that can be used to encrypt, decrypt, and sign information
• Public key—A digital code used to encrypt/decrypt information and verify digital signatures; this key can be made widely available; it has a corresponding private key

• Private key—A digital code used to decrypt/encrypt information and provide digital signatures; this key should be kept secret by its owner; it has a corresponding public key

• Secret key—A digital code that is shared by two parties; it is used to encrypt and decrypt data

• Key fingerprint—A legible code that is unique to a public key; it can be used to verify ownership of the public key

• Hash function—A mathematical computation that results in a string of bits (digital code); the function is not reversible to produce the original input

• Hash—The resulting string of bits from a hash function

• Message digest—The value returned by a hash function (same as a hash)

• Cipher—Any method of encrypting data

• Digital signature—A string of bits appended to a message (an encrypted hash) that provides authentication and data integrity

8.2.2 Security Standards

It is generally recognized that the best way to manage security risk and compliance requirements is through a systematic and comprehensive approach, based on industry best practices that work within the requirements of The Committee of Sponsoring Organizations of the Treadway Commission’s (COSO) Enterprise Risk Management framework. The starting point should be a single, overarching, and organization wide control framework within which all individual network security and compliance requirements can be addressed. There are two widely recognized and widely deployed IT control frameworks. The first, developed by the IT Governance Institute in America, is the Control Objectives for Information and related Technologies (COBIT). The second, developed by the International Standards Organization (ISO) with worldwide input, is ISO/IEC 17799 (supported by ISO 27001). COBIT and ISO/IEC 17799 offer good starting points and are capable of working together. Between them, they support an IT governance framework that can help organizations manage IT-related risk and network security compliance audit requirements, including PCI standard, HIPAA, and GLBA data security regulations, as well as the needs of current corporate governance and internal control regimes.

COBIT and ISO/IEC 17799 allow companies to use established best practices to simplify and unify their IT processes and internally defined controls. In support of the Sarbanes-Oxley Act, recent Public Company Accounting Oversight Board (PCOAB) guidance encourages Sarbanes-Oxley Act auditors to recognize that high-level controls can establish the validity of contributing controls, providing a formal context for deployment of an established hierarchical IT framework that could significantly streamline the auditing process. This approach “helps coordinate enterprise wide risk and compliance efforts and reduces the cost and dislocation of IT audits because if auditors can easily see how an auditee’s control framework fits together, they are likely to take up considerably less IT staff time and resources in their risk assessment effort.” In fact, many organizations are adopting this systematic approach worldwide.

COBIT is used primarily by the IT audit community to demonstrate risk mitigation and avoidance mechanisms deployed by technologists to the management community of an organization. In 1998, management guidelines were added and COBIT became an internationally accepted framework for IT governance by clarifying IT processes and their associated controls. ISO/IEC 17799 (The Code of Practice for Information Security Management) is an internationally recognized standard and is a best-practice framework for implementing security management. The two standards are not in competition; they complement one another. COBIT focuses
on the information system’s life cycle processes while ISO/IEC 17799 focuses on security. ISO/IEC 17799 addresses control objectives, while COBIT addresses information security management process requirements.

One of the most visible benefits to organizations that adhere to COBIT and ISO/IEC 17799 best practice frameworks is that by complying with and enforcing the regulatory security policies, they can reduce both human and monetary costs.

In addition, application and network infrastructures constructed from a common base significantly ease the “pain” associated with audit and compliance. If the point-product-specific architectures are removed and common system, network, application, and control architectures are deployed, the effort required for compliance is dramatically reduced. Although little commonality is at first perceived between the various compliance regimes, they share an overriding element—the protection of the availability, confidentiality, and integrity of information, whether at rest, in transit, or process.

8.2.2.1 COBIT

IT is relatively new to the auditor and is often difficult for management to understand. COBIT incorporates the concept of an overarching framework by which audits can be performed in an IT environment. Audit frameworks such as COBIT are built upon ISO/IEC 17799 for their information security components. COBIT removes the challenges of the dynamic IT landscape by focusing on processes and objectives as opposed to technological specifications, becoming a recognized framework used for many audit regimes and entities such as the Sarbanes-Oxley Act, HIPAA, the U.S. Government Accountability Office (GAO), and GLBA. Developed and promoted by the IT Governance Institute, COBIT is an open standard for IT control that benefits management, technologists, and auditors as a risk-avoidance methodology that covers the process life cycle of both an IT project and the IT infrastructure as a whole. This framework identifies 34 IT processes within four domains of control corresponding to the lifecycle of an IT project:

- Planning and organization
- Acquisition and implementation
- Delivery and support
- Monitoring

From a security perspective, the most important COBIT domain is DS5. This is a broad domain, targeted at “ensuring system security.” This is also one of the few COBIT domains where specific technology requirements are given. They are:

- Confidentiality and privacy requirements
- Authorization, authentication, and access control
- Cryptographic key management
- Incident handling, reporting, and follow-up
- Virus prevention and detection
- Firewalls
- Centralized security administration
- User training
- Tools for monitoring compliance
- Intrusion testing and reporting
- User identification and authorization to profiles
- Need-to-have and need-to-know

8.2.2.2 ISO/IEC 17799

Private, fixed networks that carry sensitive data between local computers require proper security measures to protect the privacy and integrity of that traffic. However, there is more to network security than simply protecting fixed private networks. LANs and WANs must be considered, as must the VPNs and extranets that augment existing fixed private networks. Networks must also be scalable, to allow future growth to be supported quickly, easily, and inexpensively. At the same time, networks must ensure that properly authenticated users can only access the services they are authorized to access. ISO/IEC 17799 provides substantial guidance on these and other network security and compliance issues.

ISO/IEC 17799 defines a “code of practice” surrounding 132 security controls structured under 12 major headings (clauses), to enable organizations to identify the specific safeguards that are appropriate to their particular business or specific area of responsibility. These security controls contain further detailed controls bringing the number to more than 5000 controls and elements of best practice. It is important to keep in mind that the controls within ISO/IEC 17799 do not address requirements; rather, they speak toward objectives.

ISO/IEC 17799 contains best-practice control objectives and controls in the following 12 clauses of information security management. It includes a number of sections, covering a wide range of security issues. Broadly, the 12 clauses that ISO/IEC 17799 objectifies are:

1. Risk assessment
2. Security policy
3. Organization of information security
4. Asset management
5. Human resources security
6. Physical and environmental security
7. Communications and operations management
8. Access control
9. Information systems acquisition, development, and maintenance
10. Information security incident management
11. Business continuity management
12. Compliance

8.2.3 ITIL Framework

1. Service support - An important aspect of IT operations is determining how services are provided and how changes are managed. The beginning of service operations is usually a request for a change from an end user, and the process involves communicating with a service desk. It is the service desk’s responsibility to ensure that the issue is documented and eventually resolved. Specifically, this area includes problem management, incident management, configuration management, and Help desk operations.

2. Service Delivery - Service Delivery focuses on defining and establishing the types of services and
infrastructure an IT department must provide to its “customers.” Topics include creating SLAs, managing overall capacity, developing availability goals, and determining financial management methods.

3. Planning to implement Service Management - Many organizations quickly realize the value of using the ITIL approach and want to know how best to move to this model. As few IT organizations have the luxury of starting completely from scratch, it’s important to understand how to migrate to ITIL recommendations.

4. Security Management - In recent years, computer security has moved to the forefront of issues for technical staff. As businesses store and provide larger amounts of information, protecting that data has become a critical part of operations.

5. ICT Infrastructure Management - The term Information Communications Technology (ICT) refers to traditional computer-based resources such as workstations and servers as well as the applications that they run (for example, office productivity suites, accounting packages, and so on).

6. The Business perspective - It is important for both business leaders and technologists to understand the overall benefits that can be provided by IT.

7. Application Management - The primary purpose of IT infrastructure is to support the software that is required by users to perform their job functions. This set covers best practices related to managing the entire application life cycle, beginning with gathering and documenting the business requirements for the software.

8. Software Asset Management - Managing applications throughout an entire IT environment can be a daunting and time-consuming task. Furthermore, the process must be ongoing as new programs are frequently added or updated. This set describes best practices for creating an inventory of software applications and managing the installed base. The topic enables IT to accurately track licensing compliance and to ensure that purchasing does not exceed requirements.