UNIFIED NETWORK

[1]Rajveer Rajawat,[2]Vikas Jain,[3]Rajesh Pokhriyal, [4]Rajesh Patil, [5]Jatin Nagpal
[1]DyManager,[2]Sr Manager,[3]Manager, [4]Manager, [5]Dy Manager
[1]Data Center
[1]RailTel Corporation, Gurugram,India

Abstract:Unified Network focuses on various methods and approaches preferred to unify network segment across organization (main office to branch offices) to a single network fabric.Unified Network also highlights the benefits and advantages of a common network across organization.

Index Terms- Unified Network, ISP, VRF, LDAP, DNS, DHCP, Proxy, NTP

1. INTRODUCTION

Today Organizations have advanced network communication infrastructure in each branch. The end-users use this infrastructure to exchange information with in the branch and to outside world. However, seamless end-to-end service delivery among the branches is missing for long time due to absence of unified network across all branches of an organization. But the efforts are put in here are to consolidate network infrastructure across organization branches over any ISP (Internet Service Provider). This document proposes a network infrastructure model for Organizations end-to-end services, that aims to identify the main entities, services, processes, and relationships involved in the multi-domain service operations and provide an architectural framework for the specification of present and future network infrastructure. It also tends to preserve mappings to existing network management standards at each branch, so that existing concepts can be reused and benefited from as much as possible.

2. OBJECTIVES

- To have a common network platform between all organizations branches for seamless network access (organization VRF).
- Uniform and transparent network usage policy across the organization.
- Smooth migration of existing network infrastructure at each branch without interrupting the existing services.
- To leverage on the available network infrastructure and bandwidth provided by Internet service provider

3. BENEFITS

A unified network platform offers integration of various applications and services across the organization keeping it private. This approach provides scalability, flexibility, security and availability of various services across the Intranet over WAN. Unified network provides seamless integration of sharing and collaboration activities like e-mail, projects, corporate training, audio and video conferencing, virtual team meetings, VOIP etc. Also web publishing through the corporate intranet reduces printing, distribution, and paper costs. Through this flexible approach and, administrators can migrate various network and security functions among centers to meet new business demands and changing network architectures. Also, to leverage on the available internet bandwidth offered by ISP leased lines.

4. ORGANIZATION'S UNIFIED NETWORK

Organization's unified network will be implemented over any ISP network infrastructure. The places/locations where ISP is currently not available have to connect to nearest ISP connected center via point to point private leased circuit.

Design and deployment architecture: Any network infrastructure should be designed in way such that it should provide availability, security, flexibility and manageability to meet the future needs and enhancements. A hierarchical network model is used to address the same. Unified network over an ISP follows a hierarchical network model by design. The hierarchical network model provides a modular view of a network, making it easier to design and build a deterministic scalable infrastructure. The hierarchical network structure is composed of the access, distribution, and core layers. Each layer has its own functions, which are used to develop a hierarchical design Also, this model provides a modular framework that enables flexibility in design and facilitates ease of implementation and troubleshooting.

Access layer: Grants user access to network devices. The access layer generally incorporates switched LAN devices with ports that provide connectivity to workstations (including virtualized desktops), IP phones, servers, and wireless access points. The

wide variety of possible types of devices that can connect and the various services and dynamic configuration mechanisms that are necessary, make the access layer one of the most feature-rich parts of the network infrastructure.

Distribution layer: The unique role of this layer is that it acts as a services and control boundary between the access and the core. Both access and core are essentially dedicated special purpose layers. The access layer is dedicated to meeting the functions of end-device connectivity and the core layer is dedicated to offer non-stop connectivity across the centers. The distribution layer on the other hand serves multiple purposes. It is an aggregation point for all of the access switches and acts as an integral member of the access-distribution block providing connectivity and policy services for traffic flows within the access-distribution block. It is also an element in the core of the network and participates in the core routing design. Its third role is to provide the aggregation, policy control and isolation demarcation point between the campus distribution building block and the rest of the network.

Core layer: The most critical part of the network infrastructure. It provides a very limited set of services and is designed to be highly available. The design objectives for the campus core are based on providing the appropriate level of redundancy to allow for near immediate data-flow recovery in the event of any component (switch, supervisor, linecard, or fiber) failure. The network design must permits the occasional, but necessary, hardware andsoftware upgrade/change to be made without disrupting any network applications. The core of thenetwork should not implement any complex policy services, nor should it have any directly attacheduser/server connections.

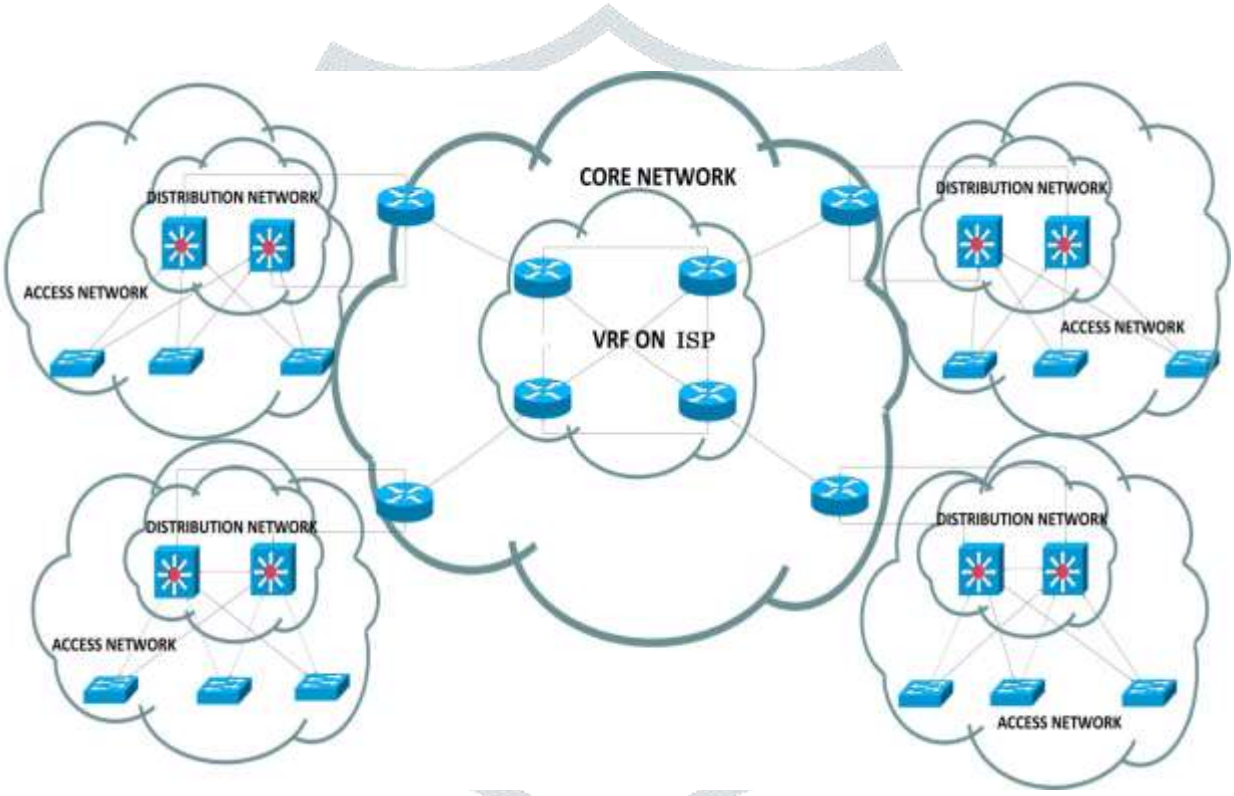

Fig 1. Architecture of unified network

Referring to above diagram, core network is the portion involving ISP cloud and end device/router connecting organization to organization VRF on ISP. Distribution layer is the part, involving core switching/routing infrastructure at each branch. Access layer is the one which connects to distribution layer for reaching rest of the network.

5. UNIFIED NETWORK SERVICES:

5.1 LDAP

LDAP is a standard and widely-implemented protocol, which makes it extremely valuable for integrating multiple applications that need to share common data. It is a shared information infrastructure that provides a comprehensive picture of employs relationship with the organization by merging identification and role information from all systems of record in an Enterprise. This infrastructure is the foundation of campus identity management, authentication, and authorization. It is possible to make one directory service serve many applications in an organization. This has the advantage of reducing the effort required to maintain the data, but it does require a careful design plan be thought out before implementation starts.
LDAP directories are structured as a tree of entries, where each entry consists of a set of attribute-value pairs describing one object. The objects are often people, organizations, and departments/groups, but can be anything. Schema is the term used to describe the shape of the directory and the rules that govern its content. A plan is proposed for the layout of the directory tree,

with particular emphasis on avoiding the need to re-organize it later. This involves careful separation of the data describing people, departments, groups, and application-specific objects.

5.2 DHCP Integration

The Dynamic Host Configuration Protocol defines a standard client-server mechanism for configuring hosts on a TCP/IPnetwork dynamically. A host running TCP/IP needs to be assigned anIP address and other parameters such as gateway and DNS server addresses before it can function properly on the network. Suchassignment can be done either manually or automatically using DHCP.DHCP eliminates the need to configure hosts one by one. The DHCPserver becomes the central administration point of IP configurationsfor all clients it serves. DHCP eases the task of managing IPaddresses and other parameters. DHCP also makes it possible totransparently apply changes to host IP configurations.
Typically the organizationsdeploy more than one DHCP server for load balancing and faulttolerance. Without a central store for DHCP configuration, DHCPservers have to hold their own configuration separately. Each servercontains a subset of a TCP/IP network's IP addresses and related IPparameters. Maintaining configurations of multiple servers or making changes to them is often a multi-step process. Centralizing DHCPconfigurations can improve the management of multiple DHCP servers.
An LDAP-based directory is a central database with standard query and retrieval methods. It is accessible throughout an organization's network. DHCP can use an LDAP-based directory to centralize its configurations. By integrating with an LDAP-based directory, DHCP as an organization-wide network service can be managed from a single point of administration. All DHCP servers can use the same directory structures for their configurations. Furthermore, administrative boundaries of DHCP service can be aligned closely with existing organizational structure in the directory. The latest packages of ISC-DHCP and OpenLDAP will be used for implementation.

5.3 Captive portal

Captive portal authentication is a Layer 3 authentication method that redirects new / non-registered users to a captive portal page when they start a web session. Once the system connects to network, the system will be assigned a quarantined IP (first time users only). The quarantined IP will have limited network access and the IP will be always redirected to captive portal. This is done by intercepting all packets, regardless of IP address or port, until the user opens a browser and tries to access the Internet. Captive portal is maintained for user registration purpose. Separate registration mechanism based on the user level privilege will be implemented for different type (guest, students etc) of users. Captive portal will be hosted at central location which in-turn updates the master LDAP server.

5.4 DNS, Domain Name System

The Domain Name System converts machine names to IP addresses. The mapping is done from name to address and address to name. The domain mapping in DNS uses a hierarchical naming standard. This hierarchy works from right-to-left with the highest level being on the right and separated by dots.The data stored in the DNS is identified by domain names that are organized as a tree according to organizational or administrative boundaries. Each node of the tree, called a domain, is given a label. The domain name of the node is the concatenation of all the labels on the path from the node to the root node. A label need only be unique within its parent domain. For administrative purposes, the name space is partitioned into areas called zones, each starting at a node and extending down to the leaf nodes or to nodes where other zones start. The data for each zone is stored in a name server, which answers queries about the zone using the DNS protocol. The data associated with each domain name is stored in the form of resource records (RRs).

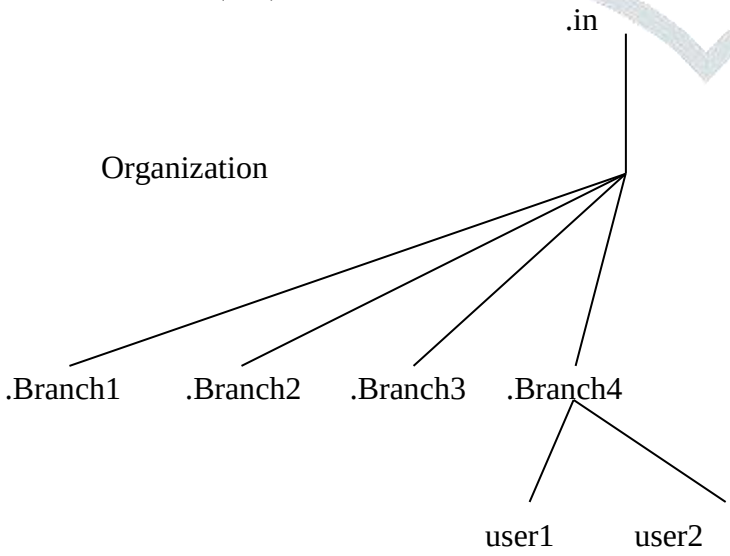

Fig 2. Domain Name Space/Naming structure

5.4.1 Dynamic DNS

The DNS system discussed above needs manual intervention whenever a change in IP address or name. The situation becomes worse when DHCP is used to assign IP address to end system. To resolve this issue RFC 2136 was defined by ETF and it is called "Dynamic DNS Update". The DDNS allowed DHCP server to send updates to primary name server, avoiding the need for user intervention. DDNS provides the capability for a networked device to notify a DNS server to change, in real time, the active DNS configuration of its configured hostnames, addresses or other information. It has a number of benefits, including:

Ease & Efficiency - There's no need to go from PC to PC setting up static addresses every time network infrastructure changes.

Accessibility – Access to system using a consistent name in the URL is possible even though the IP address changes.

5.4.2 DNS design and deployment architecture

DNS is a critical service on unified network. The services like web, email cannot function with DNS. Improper deployment of DNS can leads to service outages, failures and security risk. The design and deployment plan of DNS is purely based on the fault tolerance, reliability and security.

The basic requirement is one primary DNS server (Master server) at each center handling authoritative domains of that center. Central secondary server (Slave server) hosting the copies of the primary zone. Based on the expected request to DNS server at each center, the center should plan for secondary server. Primary servers are writable and all updates should be made to them. Secondary servers are read only and exist only to provide fault tolerance or to share the load of the primary system. The updates on primary server are replicated to slave server by zone transfer mechanism.

DNS update needs to be dynamic since it is planned to use DHCP for IP address allocation on unified network. The DDNS method will be used to update the DNS. The remaining portion of the document covers implementation and configuration part of DDNS and master slave setup.

5.5 Proxy Service

A proxy server is a server that sits between a client application, such as a web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests by itself. Otherwise, it forwards the request to the real server. Proxy servers have two main purposes on a network, firstly, to improve network performance through the delivery of previously requested objects from the cache and secondly to filter request, i.e. preventing users from accessing some specific sets of website. Proxy caching has been widely used to cache static (text/image) objects on the Internet so that subsequent requests to the same objects can be served directly from the proxy server without contacting the real server. In order to reduce client perceived access latencies as well as server/network loads, caching of frequently used data at proxies close to the client is an effective technique. This will enhance the availability of objects and reduce packet losses, as local transmission is more reliable than remote transmission.

5.5.1 Deployment Architecture

The proxy server can be deployed in many ways. The two main methods are Non-transparent mode (explicit proxies) and transparent mode. In non-transparent mode the client software should be made aware of the existence of proxy server in the network it is connected. The client sends its web requests to the proxy server regardless of the URL specified in the request. In addition to requested URL retrieval the proxy client also delegate the DNS resolution functionality to Proxy server. Proxy server then resolves the URL to an IP if required and retrieve the object from the destined server on behalf of proxy client and provide the retrieved information to the client. The different method for making clients to make aware of proxy servers are

Explicit client configuration- Clients (browsers or other proxies) are explicitly configured to send requests to a proxy instead of the origin servers.

Browser configuration- Modern browsers implement proxy autoconfiguration capability. Instead of being configured directly to use a certain proxy, a browser is configured to download a special URL every time it is started, called an autoconfiguration file, which identifies the proxy the browser should use. This level of indirection allows the administrator to maintain the proxy configuration information in a centralized manner.

Proxy auto discovery- A mechanism for discovering an explicit proxy, called Web Proxy Auto-Discovery (WPAD) and it utilizes various protocols that hosts may use to discover resources on the network.

Since it is planned to deploy transparent proxy on C-DAC unified network the detail of the same is covered in rest of the document.

5.6 NTP

In modern computer networks time synchronization is critical because every aspect of managing, securing, planning, and debugging a network involves determining when events happen. Time also provides the only frame of reference between all devices on the network. Without synchronized time, accurately correlating log files between these devices is difficult, even impossible. If server doesn't keep accurate time, log files are useless in the event of an incident that requires log-dependent

information, including security breaches. E-mail servers and other clients depend on accurate time to relay, send, and receive data. Following are just a few specific reasons for which we should have a time synchronization system.

- Tracking security breaches, network usage, or problems affecting a large number of components can be nearly impossible if timestamps in logs are inaccurate. Time is often the critical factor that allows an event on one network node to be mapped to a corresponding event on another.
- To reduce confusion in shared filesystems, it is important for the modification times to be consistent, regardless of what machine the filesystems are on.
- Job scheduling in computing cluster and grid systems
- High available clusters and
- Financial and HRMS service are required to be time synchronized

NTP is the protocol which is designed to synchronize the clocks of computers over network to common timebase and it becomes de facto standard today.

5.7 Network Service Monitoring

Implementation of C-DAC VRF will create a massive network infrastructure. As the infrastructure grows it is equally important that network administrators are aware of and have a handle on the different types of traffic that is traversing their networks. Traffic monitoring and analysis is essential in order to more effectively troubleshoot and resolve issues when they occur, so as to not bring network services to a standstill for extended periods of time. Numerous tools are available to help administrators with the monitoring and analysis of network traffic. Network monitoring is a difficult and demanding task that is a vital part of a Network Administrators job. If a network were to be down even for a small period of time productivity may decline, and in case of public service department, the ability to provide essential services would be compromised. In order to be proactive rather than reactive, administrators need to monitor traffic movement and performance throughout the network and verify that all services are up and running. In C-DAC VRF we are proposing to implement Nagios monitoring solution for network and service monitoring. Cacti graphing solution will be used to graph the traffic on the network device.

Nagios Monitoring Server

Nagios is a network monitoring application that is capable of detecting and notifying abnormal behavior. The definition and monitoring behaviour is defined using a set of flat-file configurations. The files indicate what and how things should be monitored. There are three primary atomic entities in Nagios:

Host	A physical device on a network that is intended to be monitored (e.g. a desktop, printer, router, switch, hub, etc...).
Service	Indicates the specific component of a host that should be monitored (e.g. CPU utilization, memory consumption, HTTP, etc...)
Command	A utility that allows for a host/service check, notification handling, alerts, etc.... For example, check_CPU can be a command used to monitor the CPU utilization on a particular host.

Nagios can be configured to define hosts, services, and commands to effectively monitor a set of resources. The actual monitoring of a host/service is not done by Nagios. It is instead done by add-on plug-ins that is defined as individual commands. This architecture provides the capability to virtually monitor any aspect of a system that can be automated. There are already many available plug-ins for monitoring common hosts/services in a typical networking environment. Custom plug-ins can be written to accomplish the monitoring of an uncommon host/service. The data collected from plug-ins are logged to flat files. The Nagios service runs on Linux but it is capable of monitoring desktops running Windows via its plug-in architecture. As part of its monitoring solution, Nagios also provides an alerting mechanism that broadcasts a problem to sets of contacts or contact groups.

6. TRAFFIC FLOW AND MINIMAL POLICY

- User connect to network
- Quarantined IP will be assigned to System if it is connecting for the first time. (Each network will be allocated a set of IPs as quarantined IP. This IP will be restricted access to rest of the network. All DNS resolution request for any domain from said quarantined IP addresses will resolve/redirected to captive portal IP address. The quarantined IP will have a leased period of 2 to 3 Minutes. Expiring the leased time, the client will be forced to renew the IP from DHCP server. If registration is successful, the new IP will be allocated to the system).
- User will be redirected to captive portal.
- User should fill MAC address of the device, hostname along with E-mail username and password and submit it. Upon authentication, MAC addresses of the device from which the registration has been initiated and the hostname submitted by the user on the portal will be stored in LDAP. Separate registration mechanism for guest, students will be made available later

- (Upon registration, the user is allowed to connect to any network across organization branches. However as a policy if the usage request from a particular network is not found for more than 30 days, users need to re-register).

- Once LDAP update is happened, and quarantined IP's lease time expiration, DHCP server fetches updated configuration from LDAP (Which has MAC and Hostname) and allocate IP address from the valid pool to the device. Thereafter, whenever registered device connect to network, the DHCP server will update hostname of device in Dynamic DNS server.
- Once all the above process is completed, the quarantined IP will be released and back to its DHCP pool
- Guest users will be provided limited access i.e. only to Internet.
- 16 nos or as per requirement of IP address (225-240) on each subnet will be used for guest users.
- Organization user need to register the respective guest user through captive portal. The registration procedure is same that of normal user. The IP address allocated from the guest pool will have restrictions and therefore does allow access to organization network.

6.1 Implementation

Redirection by HTTP
If an unauthenticated client requests a website, DNS is queried by the browser and the appropriate IP resolved as usual. The browser then sends an HTTP request to that IP address. This request, however, is intercepted by a firewall (configured as a transparent proxy) and forwarded to a redirect server. This redirect server responds with a regular HTTP response which contains HTTP status code 302 to redirect the client to the Captive Portal. To the client, this process is totally transparent. The client assumes that the website actually responded to the initial request and sent the redirect.

DNS Black Hole
In this setup, unauthenticated system will use IP and DNS information provided by the DHCP server. There will be a separate DNS server which will resolve all the queries to captive portal IP address. When an unauthenticated client tries to browse something, a DNS request will be send to DNS server. The DNS server resolves this request to captive portal IP address. The client system connects to the resolved IP (Captive portal IP) received from DNS server. The user has to register his credentials in the form provided in the portal. On submitting the form user information will be added to backend database and user will be provided access to network resources.

REFERENCES

[1] O'REILLY DNS and BIND Book – By Cricket Liu & Paul Albitz
[2] Mastering OpenLDAP – By Matt Butcher
[3] NAGIOS BOOK – BY WOLFGANG BARTH