Fall 9-2017

Active Directory Infrastructure Design and Network Topology Design for StarCom Software Developer Company

Bujar Lushta

Computer Science and Engineering Faculty

Active Directory Infrastructure Design and Network Topology Design for StarCom Software Developer Company

Thesis

Mentor: Fisnik Prekazi

Candidate: Bujar Lushta

September • 2017

Prishtina

Abstract

Active Directory is Microsoft trademarked directory service, an integral part of the Windows 2000 architecture and later server operating systems. Like other directory services, such as Novell Directory Services (NDS), Active Directory is a centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories.

A well-structured Active Directory hierarchy requires a well-defined underlying network infrastructure in which AD forest is built upon. The design shows Cisco best practices in terms of providing layered approach by segmenting the traffic and streamlining network traffic ultimately providing redundancy, scalability and traffic efficiency.

To demonstrate both Microsoft AD and Cisco network layout a fictive company was created for which both technologies and show why are they so important.

Contents

Introduction to StarCom Corp

The StarCom is a public multinational corporation comprised of seven operating companies, with primary headquarters located in Kosovo and over 5 major regional offices that provide a complete range of IT services (software management and software development and asset management). From an operating perspective each operating company is an autonomous business unit.

This company operates under the strict regulatory legislations govern by the government in each respective country location. Regulations manly state financial privacy, trading, IT functionality and security. As a result, maintaining secure and stable systems at both the network system level is required.

It is important to note that StarCom is fictive company taken as an example to prove a concept and demands for proper Active Directory forest structure and underlying network layout.

Current Network Setup

StarCom Developer Company has number of site around the globe, with HQ located at Kosovo and four branch offices in Albania, Bosna, Croatia and Serbia. All branch offices are interconnected thru serial connection with the central HUB site located at Kosovo HQ.

Kosovo HQ - is the Hub and it is also the main point of connection to the public Internet. The site has also largest data centre where most of the company server resources are maintained. In addition, this site house most of the administration staff and various departments.

Since team such as Engineers, Marketing, Administrators are located here, then we must ensure 100% connectivity and redundancy. The offices consist of four floors, with each department on their own individual VLAN.

Branch offices – the branch offices are located on four countries, each with its own domain infrastructure and departmental structure. Branch offices maintain smaller number of servers such as DHCP, DNS, File Servers and child domain.

Existing IT Environment

There is no central IT group for all operating companies, meaning there are no comprehensive IT standards for the entire organization. Each operating company has created its own standards, therefore, each company has its own IT infrastructure. In some locations, operating companies share one common network. In other locations, the number of networks matches the number of operating companies sharing that office location. Local offices, especially the consumer and retail locations, maintain their own file and print servers, although regional offices usually have domain controller's Regional offices are otherwise limited in their IT functions.

Customer Requirements

A parent company IT initiative driven by a group of IT professionals that represent each of the operating companies is also working to develop a company-wide Active Directory structure and they requirements are listed below.

- StarCom requires its own Active Directory structure with the goal of creating a common global directory design for the entire organization.
- Each major regional site has its own active directory forest, the requirement is to marge each site under common Active Directory forest.
- Reduce TCO through reduced client management while increasing the level of service.
- Allow each separate company to have its own child domain or domains.
- StarCom requires a network infrastructure that compliments they current Active Directory site topology.
- The network setup should provide redundancy at Kosovo site at access, distribution and core layer.
- The network should accommodate 200 nodes for each floor, each floor should be on its own subnet.
- The hole network should be routable.

Active Directory Design

Design Proposal

According to Microsoft best practice for companies with similar number of objects and WAN structure as StarCom is to use the single internal forest model. A single forest model will allow StarCom to streamline security within a single security boundary.

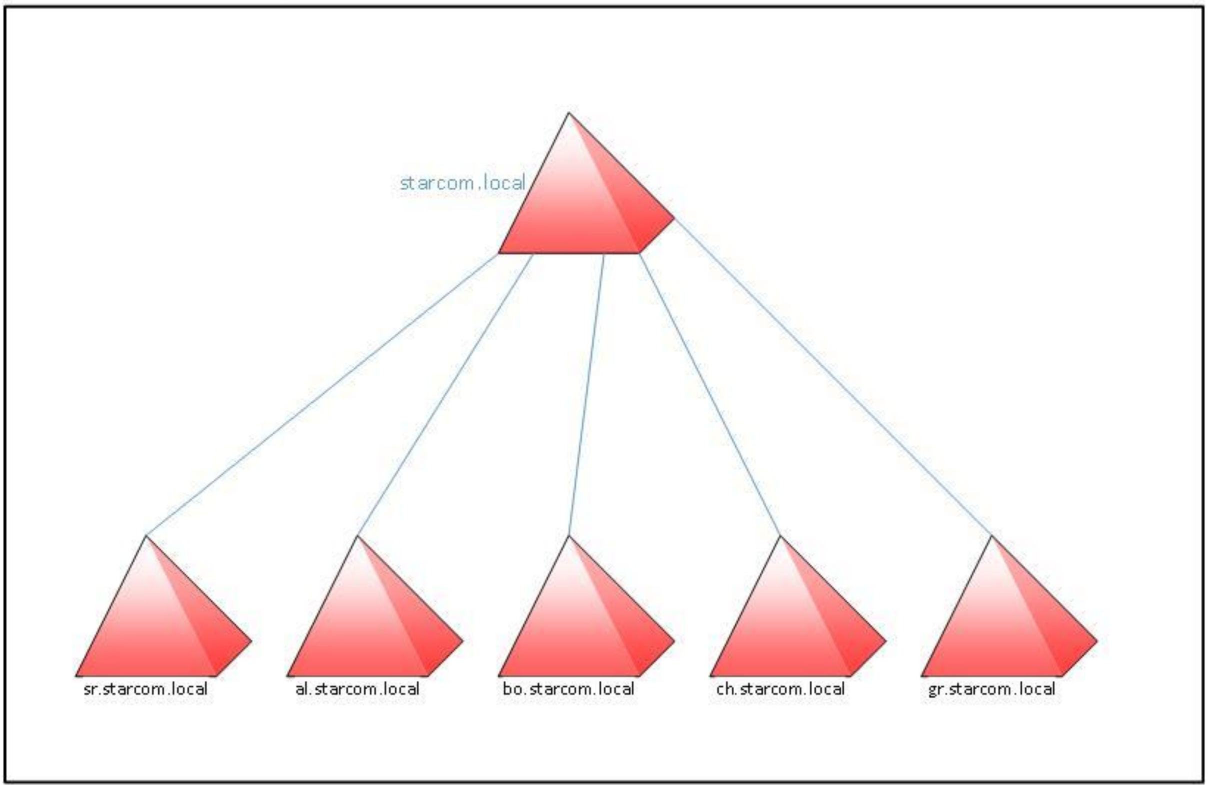
This model offers a low cost of operation and administration, and also for the total cost of ownership through centralized directory services, centralized resource management, consolidation of services, and standardization of configuration management.

Any modification of the schema attributes will have major impacts to Active Directory Architecture. That is why it is recommended to be done only by senior administrators and after passing the testing phase.

Domain Structure

A multi-domain model is the best case for StarCom. It will consist of one forest, a root domain and one child domain for every major country. Each domain will contain its own set of user and group accounts.

StarCom Domain Forest



Active Directory Namespace

Active Directory Namespace:

Root domain: **starcom.local**

Child domains: ***<country abbreviation*** **>. starcom.local**

Example:

For StarCom Albania the domain name will be: **al.starcom.local** and Netbios Domain Name will be: **ALBANIA**

For StarCom Bosnia the domain name will be: **bo.starcom.local** and Netbios Domain Name will be: **BOSNA**

Naming Standards Proposal

Administration of servers and workstations becomes easier if their location and function can be determined from their name. Computers identify network machines by their names (Server Name). In the physical world we mostly use information related to their whereabouts: physical location (town, street, building, floor, and room), function (e.g. mail server, domain controller, etc.), user, machine type, performance, etc.

According to this, the names of the servers must be chosen carefully. They should contain information required for physical identification, and in the same time remain consistent throughout a potentially changing physical environment.

Aspects to be considered for naming the servers:

- Servers are not often moved between sites.
- The server functions rarely change; the modification is usually carried out by re-installation.
- The role of the server should be included in the server name
- Version of the operating systems may change; therefore, including the version number in the machine name may easily lead to an inconsistent condition: we recommend against it.
- If clustered servers are used, it is recommended to point out the physical node in the name.

Part of the following limitations is inevitable, while another part facilitates assigning users and machines to each other:

- Machine name is maximum 15 characters – this limitation is due to the constraints of NetBIOS.
- It is recommended to apply only the English alphabet and numbers – in case if the use of code pages and keyboard layouts is not entirely standardized within the organization.
- Within a domain, login names must be individual. The user name convention must ensure a way to resolve potential conflicts, and it must make the name definition algorithmic.
- NetBIOS name of each computer must be individual.
- The machine should not contain only numbers.

- No special characters must be used – symbols other than letters and numbers should not be used in general, because they are considered illegal in a number of naming systems (e.g. computer name including a dot, when entered into DNS). There are some exceptions:
    - _ (underscore) and – (dash) can be applied in login and group names
    - . (dot) can be applied in e-mail addresses.

User Account Naming Convention Proposal

During migration process, user objects will be ported along using the naming convention currently in place at each country.

After ending the migration process, a new naming convention will be implemented at the group level: **[First Name].[Last Name]**.

As a best practice we recommend for service user accounts to be easily identified by **_svc** prefix followed by the abbreviation of the service that impersonates the user and its role. If more than one user is required for the same service two digits should be added at the end of the user name and logon name.
_svc[service][role].

Example:

_svcSMSClient01 – SMS Client installation Account

_svcSMSClient02 – SMS Client Installation Account

_svcSMSAcna – SMS Advanced Client Network Access account

_svcCluster01 – Service for MSCS service

Server Naming Convention

Server roles and their abbreviation:

DC	Domain Controller
TS	Terminal Server
FS	File Server
EX	Exchange Server
DNS	DNS Server
AP	Application Server
APD	Application Server for Development
APT	Application Server for Test purposes
DB	Database Server in Production
DBD	Database Server for Development
DBT	Database Server for Test purposes
BK	Backup

FW	Firewall
PRN	Network Printer
ACS	Access Server
WB	Web Server
CL	Cluster Server (virtual server name)
SMS	SMS Server
CM	Call Manager
WSxxx	Workstation

Server name proposal: **CountryAbbreviation][Town Abbreviation][Index][[Role][Index]**

Example: Proposed name for a domain controller in Albania child domain in Tirana city: **ALTR1DC01**

where:

AL	is the country abbreviation;
TR	is the town abbreviation;
1	is the town index
DC	is the role;
01	is the role index

Printers Naming Convention

Printers name will follow the same naming convention as the servers. Server role will be replaced by PRN abbreviation.

Example: ALTR1PRN034

Workstation Naming Convention

Workstations name will follow the same naming convention as the servers. Server role will be replaced by WS abbreviation and index will consist of 3 digits.

Example: ALTR1WS999

Forest / Domain Functional Levels

The goal is to raise the functional mode to Windows Server 2012 R2. For this reason, at the end of implementation, after the user, computer and application migration, StarCom administrators will upgrade forest and domain mode to Windows 2012 R2. This will enable the new Active Directory to leverage all of the improvements in Windows 2012 Active Directory.

Domain Controller Placement

According to Microsoft best practices each site hosting Domain Controllers must have at least two servers providing Domain Controller service. The main reason is to assure the load balance and fault tolerance inside each site. Each location designated to receive a domain controller must demonstrate the following attributes:

- Secure Facilities (Physical security) to where the Domain Controllers are kept.
- Standard US English language operating.

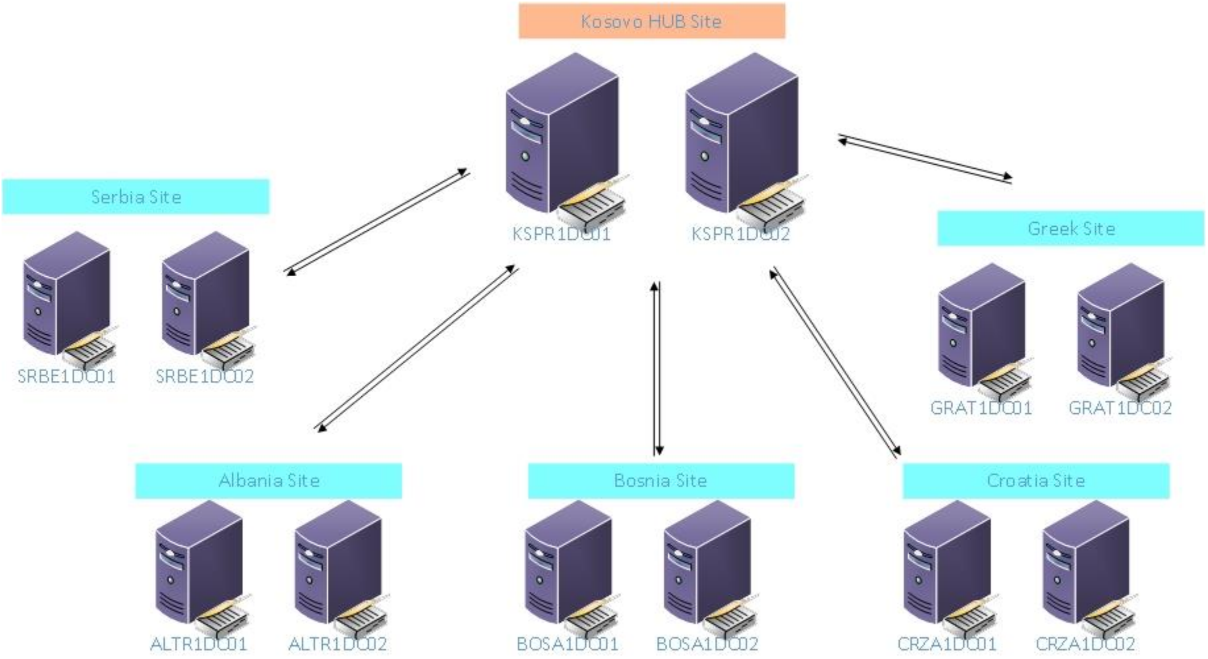
Placing a Domain Controller in every site ensures that login and authentication will be available regardless of the state of the WAN connection. However, for fault tolerance reasons, it is recommended that two Domain Controllers should be placed in each site.

Also for designing Domain Controller server placement must be take into consideration the following aspects:

- Number of machines available;
- Network bandwidth and availability;
- Replication optimization;
- User experience.

Design Proposal

The following diagram presents the envisioned architecture from the Domain Controller's perspective:



where:

RODC01 Site and RODC02 Site are the Romania Sites defined one per location.
For Serbia, Macedonia, Croatia, Kosovo and Turkish the picture contains one site per each country. Based on local requirements each local IT Admin will propose the number of sites for his country. The design will be updated to contain the final sites structure.

In the description field of Site object will be typed the address of the location.

Convention proposal for site name is:

<country abbreviation>DC<Index>

Convention proposal for DC server name is:

<town abbreviation><country abbreviation>DC<Index>

Note: In each site one Domain Controller will be a physical machine. The rest can be virtual machines.

Global Catalogue Placement

In multiple-domain forests, global catalog servers facilitate user logon requests and forest-wide searches. A Domain Controller (DC) normally contains the naming context for its domain plus the NS for the forest's Schema and Configuration data. It is possible to designate a DC to be a Global Catalog Server (GC). A GC is a special subset of domain controller that contains a read-only subset of the data from each domain in the forest. This subset consists of a reference to every active directory object plus a subset of attributes for those objects. Thus a GC participates in the replication topology for every domain in the forest. GCs can replicate data from both normal DCs and other Global Catalog Servers. Normal DCs can replicate only from other writeable domain controllers.

Design Proposal

As StarCom infrastructure will consist of multiple domains, for every domain the Infrastructure Master Role and Global Catalog Role will not coexist on the same server. In the following table is a proposal for placement of Infrastructure Master and GC roles for each major country.

Domain	**GC name**	**GC (yes/no)**
starcom.local	<*town abbreviation*>KSDC01	Yes
starcom.local	<*town abbreviation*>KSDC02	No
al.starcom.local	<*town abbreviation*>ALDC01	Yes
al.starcom.local	<*town abbreviation*>ALDC02	No
bo.starcom.local	<*town abbreviation*>BODC01	Yes
bo.starcom.local	<*town abbreviation*>BODC02	No
sr.starcom.local	<*town abbreviation*>SRDC01	Yes
sr.starcom.local	<*town abbreviation*>SRDC02	No
cr.starcom.local	<*town abbreviation*>CRDC01	Yes
cr.starcom.local	<*town abbreviation*>CRDC02	No
gr.starcom.local	<*town abbreviation*>GRDC01	Yes
gr.starcom.local	<*town abbreviation*>GRDC02	No

Active Directory Sites and Replication

Sites are created as group of one or more IP subnets containing domain controllers and defining local area network LAN, or set of LANs interconnected with high speed backbone (MAN). Domain controllers within a site are using other notification and replication mechanisms than domain controllers in other sites. Site subnets are typically connected using fast media (10 Mbps or higher), which generally represents single subnet or switched subnets. Sites are inter-connected using link slower then LAN speed (512 Kb - 2 Mb). From the client computers' perspective, some specific scenarios may require that this general rule be modified and sites can be formed by subnets inter-connected by lines even lower than 10 Mbps.

The main reason would be the existence of small locations with just a few client computers where there is no justification for installing domain controllers. Users in these remote subnets will get the same resources as users from main site's subnets, but performance for some specific tasks can be slower (user logon, Group Policy processing, remote installation, security updates, roaming profile download, shared files access etc.). Even while adding slow connected IP subnets to a site, there is still a need to underline that domain controllers within each site should be connected by lines of at least 10 Mbps (because of nature of their intra-site communication).

Design Proposal

Every major country will have its own domain and for every domain a site will be created. Site naming convention: **[Country abbreviation]DC[Index]**.

Replication

The Active Directory is basically a complex distributed database, with copies located on several domain controllers, and with changes that can occur on different locations. In order to have up-to-date data on all domain controllers, the changes must be forwarded to all servers. This is the replication process.

In the Active Directory the sites determine the replication border lines. The replication topology is influenced by the following components:

- KCC (Knowledge Consistency Checker Service);
- ISTG (Intersite Topology Generator Service);

- Bridgehead Server;
- Connection Object;
- Site;
- Site Link.

Based on these components and parameters, the actual replication topology is developed by KCC and ISTG, they create the Connection objects required for the replication. The actual replication is performed via these objects.

Design proposal

In the Active Directory, the automatic replication must be used for replication within the site. One must let the KCC to create and manage the replication topology, because the replication within the site is not bandwidth-sensitive.

The replication between remote sites is done in a scheduled and compressed way. On each site a domain controller (ISTG) is responsible for the management of the inbound replication connections. In case the ISTG server is not available on the network, then the KCC automatically relocates the role to another server.

No site link bridges will be created. A Site link bridge is used to provide connectivity to site links when they are not directly routable. This would only be used when a network is not fully routable.

There will be 2 bridgehead servers in the KSDC01 site. This will ensure redundancy in the case that one fails and also load balancing to distribute the load.

No manually bridgehead servers will be configured in the rest of the branches. The selection of bridgeheads is automatic by default. Manually defining preferred bridgeheads is generally not required, because it incurs additional administrative overhead, can reduce the inherent redundancy of Active Directory, and can easily result in replication failures due to invalid configurations. Designating a single bridgehead for a domain in a site that contains multiple DCs of that domain will result in a single point of failure. This is because the other DCs will not take over inter-site replication if the preferred bridgeheads go offline. In case of a major hub location, this would cause widespread replication failures in the event of a single DC going offline.

FISMO Placement

Most operations can be made at any Domain Controller and the effects of these operations (for example, deleting a user object) are replicated to all other Domain Controllers that store a replica of the same directory partition in which the change occurred. However, there are certain operations that must occur on specific Domain Controllers.

The Domain Controllers that are assigned to manage single-master operations are called role owners for the operations. The single-master operations include the following:

- **Schema Master (Forest Level FSMO).** The Domain Controller that holds the Schema Master role is the only Domain Controller that can perform write operations to the directory Schema. Those Schema updates are replicated from the Schema Master to all other Domain Controllers in the Forest.
- **Domain Naming Master (Forest Level FSMO).** The Domain Controller that holds the Domain Naming Master role is the only Domain Controller that can add new Domains to the Forest and remove existing Domains from the Forest.
- **RID Pool Master (per Domain FSMO).** A new security principal object (user, group, or computer) can be created on any Domain Controller. However, after creating several hundred security principal objects, a Domain Controller must communicate with the DC holding the Domain's RID Master role before creating the next security principal object.
- **PDC Emulator (per Domain FSMO).**The Domain Controller holding the PDC emulator provides backward compatibility to down-level BDCs (Backup Domain Controllers) when running in Mixed Mode. The PDC emulator also serves other roles, including Time Synchronization and Password Latency Control. Changes to security account passwords present a replication latency problem wherein a user's password is changed on the BDC "A", perhaps by an admin at a hub site, and the user subsequently attempts to logon, being authenticated by BDC "B" (in his local branch office). If the password has not replicated from A to B, the attempt to logon fails. Active Directory

replication remedies this situation by forwarding password changes immediately to a single Domain Controller in the Forest, the PDC emulator.

- **Infrastructure Master (per Domain FSMO)**. The Domain Controller holding the Infrastructure Master role for the group’s Domain is responsible for updating the cross-Domain group-to-user reference to reflect the user's new name. The Infrastructure Master updates these references locally and uses replication to bring all other replicas of the Domain up to date. If the Infrastructure Master is unavailable, these updates are delayed. When an object on one Domain Controller references an object that is not on that Domain Controller, it represents that reference as a record containing the GUID, the SID (for references to security principals), and the DN of the object being referenced. If the referenced object moves, its GUID does not change its SID changes if the move is cross-Domain, and its DN always changes. The Infrastructure Master for a Domain periodically examines the references, within its replica of the directory data, to objects not held on that Domain Controller.
- **Global Catalog.** It is recommended to configure at least one domain controller in each site as global catalog. This allows users to obtain fast and reliable domain logon (global catalog is – when in native mode - used for universal group membership enumeration). When using the default configuration the logon to a domain is not allowed when a global catalog is not available. In a multi-domain model domain controllers configured as global catalog servers besides its domain database also store partial replicas from other domains in the forest (approximately 40% of each domain Active Directory database size in the same forest). These data are replicated between domains.

Design Proposal

In each site the FSMO roles will be split between the two domain controllers. The table below shows example using KSPR1DC01 and KSPR1DC02 to demonstrate roles split among the two servers.

Domain Controller	**FSMO Role**	**Global Catalog**
KSPR1DC01	Domain Naming Master	Yes
KSPR1DC01	Schema Master	yes
KSPR1DC02	PDC Emulator	No
KSPR1DC02	RID Master	No

KSPR1DC02	Infrastructure Master	No

OU Structure

Active Directory allows administrators to create a hierarchy within a domain that meets the needs of their organization. The object class of choice for building these hierarchies is the class Organizational Unit, a general-purpose container that can be used to group most other object classes together for administrative purposes. An organizational unit in Active Directory is analogous to a directory in the file system; it is a container that can hold other objects.

Organizational units can be nested to create a hierarchy within a domain and form logical administrative units for users, groups, and resource objects, such as printers, computers, applications, and file shares. The organizational unit hierarchy within a domain is independent of the structure of other domains; each domain can implement its own hierarchy. Likewise, domains that are managed by a central authority can implement similar organizational unit hierarchies. The structure is completely flexible, which allows organizations to create an environment that mirrors the administrative model, whether it is centralized or decentralized.

Organizational units can be used to delegate the administration of objects, such as users or computers, within the OU to a designated individual or group. To delegate administration by using an OU, place the individual or group to which will be delegated administrative rights into a group, place the set of objects to be controlled into an OU, and then delegate administrative tasks for the OU to that group.

Design Proposal

While OUs offer an easy way to group users and other security principals, they also provide an effective mechanism to segment administrative boundaries. In addition, using OUs to provide different Group Policy objects (GPOs) based on server role is an integral piece of the overall security architecture for the organization. We can apply Group Policy security settings at several different levels in an organization. The baseline environment discussed above used Group Policy to apply settings at the following three hierarchy levels in the domain infrastructure:

- Domain Level — to address common security requirements, such as account and password policies that must be enforced for all servers in the domain.
- Baseline Level — to address specific server security requirements that are common to all servers in the domain infrastructure.
- Role Specific Level — to address security requirements for specific server roles.

In each country domain will be created the following OU structure:

- KS System Integration;
- KS Banking;
- KS MASS;
- KS CARD;
- Infrastructure servers (will hold general IT infrastructure servers).

For each of the above OU's will be defined the following OU substructure:

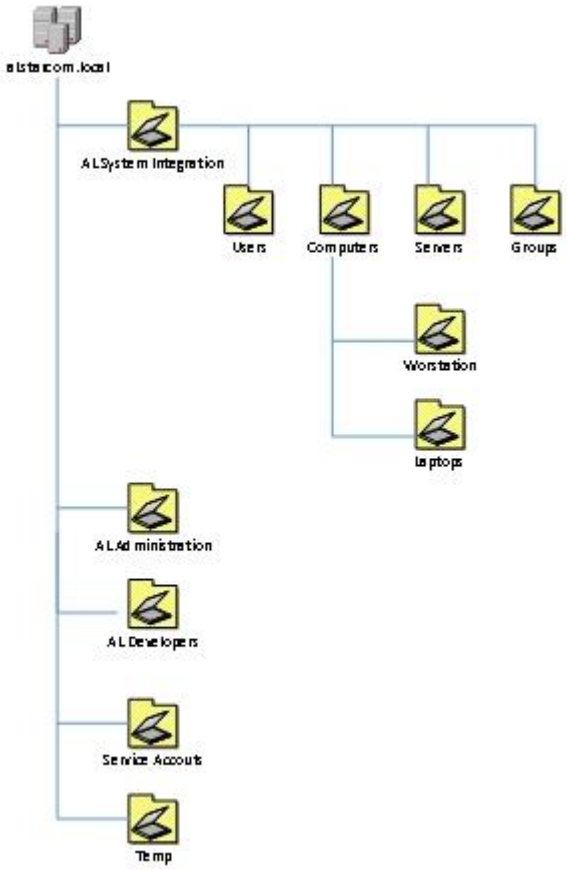
- Users;
- Computers with the following structure:
  - Workstations;
  - Laptops.
- Servers (will hold servers administered and used by that business unit);
- Groups.

This approach will assure flexibility for delegation and also for group policy.

In each country domain in the first level will be also the following OU's:

- Temp;
- Admins;
- Service Accounts.

In the next picture is presented as an example the OU structure for al.starcom.local domain.



DNS Role Placement

A basic service of all IP-based infrastructures is the registration of IP addresses regarding computer names. From the technologies used for name resolution the most widely used is the DNS, the smooth operation of which is an absolutely necessary requirement for the Active Directory service.

Design Proposal

All of the servers with Domain Controllers role will have also the DNS role. The DHCP server will provide the clients locally the addresses of the DNS servers to be used. The internal DNS zone will be Active Directory integrated and located on the DCs in the DNS-defined partition.

STARCOM.LOCAL zones will require secure updates.

The proposed replication model for the zones:

- **_msdcs.Starcom.local** – To all DNS Servers in Active Directory forest starcom.local

- **starcom.local** – To all DNS Servers in Active Directory Domain starcom.local

Country forward lookup zones:

- al.starcom.local
- bo.starcom.local
- cr.starcom.local
- sr.starcom.local
- gr.starcom.local

Each DNS server’s NIC will be configured to use itself for the primary DNS server and the closest DNS for the secondary DNS server. For example the domain controllers in Albania in the ALDC01 Site will point to themselves as primary DNS and to other server from the same site as secondary DNS.

Aging and scavenging will be enabled, with dynamic secure updates.
DHCP will be configured to register clients in DNS. Based on local requirements for special conditions DHCP can be configured not to register clients in DNS. IT Local Admins must informe if they have this special request.

HOST files will never be used.

For every child domain the primary DNS suffix will be set by DHCP as a connection specific DNS Suffix. The primary DNS suffix will automatically become <*country*>.starcom.local as computers are included in the domain. Applications using unqualified domain names will require this information to be setup properly to continue functioning. All client computers joined to the Active Directory domain will be configured to use the Active Directory closest DNS servers. This will be achieved by configuring the DHCP server client’s options.

DHCP Usage

Dynamic Host Configuration Protocol (DHCP) is a service that runs on a Windows Server 2003 operating system.

Its function is to automatically allocate IP addresses and other TCP/IP-related information [such as Windows Internet Naming Service (WINS) IP addresses, Domain Name System (DNS) IP addresses, default gateway IP addresses, and subnet mask information] to DHCP-enabled clients.

For an IP address to be configured on a DHCP client workstation, four steps take place:

- When a client is booting up, it sends out a broadcast packet over the network segment requesting a DHCP server response. Broadcast traffic does not go over a router unless the router is specifically configured for this purpose. This is called the IP Lease Discover phase.
- All DHCP servers configured with a valid range of IP addresses send the client an offer. This IP Lease Offer includes the MAC address of the client, an IP address, subnet mask, length of lease, and the IP address of the DHCP server offering the IP address.
- The DHCP client accepts the offer from the first DHCP server to respond and sends the server a request to lease the IP address. This request is sent in a DHCPDISCOVER message and contains the MAC address (hardware address) and the computer name of the DHCP client.
- The DHCP server that offered the IP address responds to the DHCP DISCOVER message, and the IP address is assigned to the client. If other DHCP servers offered IP address to the client, it would now withdraw its offer.

Before IP addresses can be issued, ranges of IP addresses, called a scope, must be defined on the DHCP server. A scope is a range of valid IP addresses that can be leased to DHCP clients. Each DHCP server must be configured with a minimum of one scope, which has the following properties:

- The range of IP addresses that will be leased to DHCP clients;
- The subnet mask;
- The duration of the lease;
- DHCP scope options, such as DNS and WINS IP addresses;
- Reservations, if you want particular DHCP clients to always receive the same IP address and TCP/IP configuration at startup.

Assigning IP addresses to workstations and servers on a large network saves the time that would otherwise be spent on physically visiting each machine. Broadcast traffic does not get forwarded by an IP router unless the router is configured to do so. This can be problematic if DHCP clients are located on a subnet that does not contain a DHCP server. This problem can be easily solved in two ways:

- Configure one or more workstations in the branches to be a DHCP relay agent;
- Configure the router to be a DHCP relay agent.

By configuring one of the workstations in the subnet to be a relay agent, the workstation hears the broadcast request made by the DHCP client and it forwards the request to a designated DHCP server, using unicast instead of broadcast packets.

If a router is DHCP/BOOTP (Bootstrap Protocol) compliant (RFC 1542), there is no need to configure a workstation to be a DHCP relay agent.

A major factor that impacts the DHCP design is the availability of network lines.

Design Proposal

The goal of using this service is represented by a central management of the IP settings. Major benefits of the service are:

- There will be no more errors related to manual IP address setting, no more configuration errors due to the manual configuration (the DHCP service delivers all the necessary information to the client);
- The client will not have to be re-configured, when moved to another *subnet* (mobile users);
- The name resolution service configurations become adjustable;
- If necessary, fixed IP addresses can also be recorded and allocated (DHCP reservation).

The need for permanent (dedicated) IP address allocation will not prevent the use of the DHCP service. In this case, preliminary reserved IP addresses linked to the network card of the computer (to its *MAC address*) can be used (*Reservation*), so we can allocate permanent IP addresses also for the servers (e.g. WINS).

In order to ensure that client connectivity is not impaired in the unfortunate event of a server crash there will be two DHCP servers configured based on the 80/20 rule in all of the major sites.

Group Policy

Group Policy provides a powerful set of tools for managing many aspects of an enterprise network. It is fast to deploy, can scale up to the largest deployments, and can accommodate specific needs of small groups, all at the same time. Within Active Directory, Group Policy provides a powerful system for enforcing specific configuration settings for sets of users/computers based on individual sites, domains, or organizational units.

A group policy can be defined on four levels:

- Locally;
- As per site;
- As per domain;
- As per organizational unit.

Group policies are processed according to the above order. The group policy processed at a later time can modify the settings specified into the previous ones. Because of this, the group policies must be designed carefully, and the creation of a “too deep” must be avoided, because – besides that it becomes nearly incomprehensible – the login of clients will also be slowing down, proportionately with the assessment of the group policies.

Group policies consist of two major parts:

- Computer policies;
- User policies.

Design Proposal

STARCOM Domain Policy” will contain the common domain policy. This policy will be applied at the child domain level. The configuration of “STARCOM Domain Policy” is:

Computer Configuration (Enabled)

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	10 passwords remembered
Maximum password age	30 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts

Reset account lockout counter after	30 minutes

Account Policies/Kerberos Policy

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	12 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Local Policies/Security Options

Accounts

Policy	Setting
Accounts: Administrator account status	Enabled
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled

Accounts: Rename administrator account	"supervisor"
Accounts: Rename guest account	"outsider"

Devices

Policy	Setting
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled
Devices: Restrict floppy access to locally logged-on user only	Enabled
Devices: Unsigned driver installation behavior	Warn but allow installation

Interactive Logon

Policy	Setting
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Enabled
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons
Interactive logon: Prompt user to change password before expiration	5 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Enabled

Shutdown

Policy	Setting
Shutdown: Allow system to be shut down without having to log on	Disabled
Shutdown: Clear virtual memory pagefile	Enabled

Other

Policy	Setting
Interactive logon: Display user information when the session is locked	Do not display user information

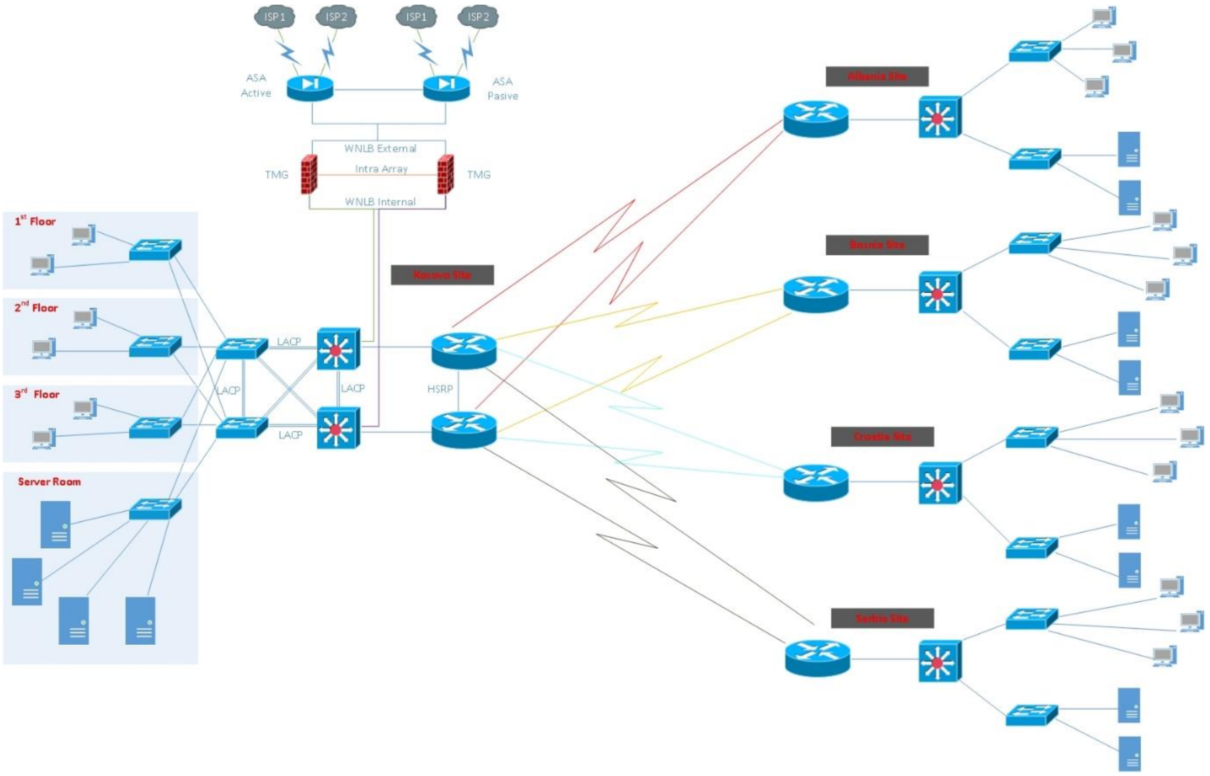
Event Log

Policy	Setting
Maximum application log size	16384 kilobytes
Maximum security log size	32768 kilobytes
Maximum system log size	16384 kilobytes
Prevent local guests group from accessing application log	Enabled
Prevent local guests group from accessing security log	Enabled
Prevent local guests group from accessing system log	Enabled
Retain application log	7 days
Retain security log	7 days
Retain system log	7 days
Retention method for application log	By days

Retention method for security log	By days
Retention method for system log	By days

Network Topology

The network below shows logical representation of the StaCom network infrastructure. The topology shows a cetral HUB site located at Kosovo HQ, which is also a primary datacentre where most of the server resources are held and where most of the administrative and developer employees are concentrated.



WAN Network

All four branch offices within StarCom are interconnected over dedicated broadband connections to the central HUB site. The topology resembles a star topology layout. Each branch office requires access to resources on central HUB site, resource access from Branch-to-Branch are rare. If the demand for access network resources between braches rises, a full mash topology may be considered, where each Branch is connected to one another, lowering the number of routes required to reach each site, in the same time increasing WAN path redundancy. Each WAN connection between central HUB site and branch office has 20Mbps dedicated WAN bandwidth.

Considering that central HUB site utilizes HSRP for automatic failover for the perimeter WAN connections, interconnecting branch offices to the HUB site.

Each office is interconnected DCE\DTE serial connection with 64000 clock rate speed.

HSRP

One way to achieve near-100 percent network uptime is to use HSRP, which provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits.

By sharing an IP address and a MAC (Layer 2) address, both routers at the edge can act as a single virtual router. The members of the virtual router group continually exchange status messages. This way, one router can assume the routing responsibility of another, should it go out of commission for either planned or unplanned reasons. Hosts continue to forward IP packets to a consistent IP and MAC address, and the changeover of devices doing the routing is transparent.

Edge Firewall Protection

Front-End Firewall

Kosovo HQ utilizes multivendor dual layer firewall protection at the network Edge. The setup ensures that ASA as a front-end firewall provides fast State-full packet inspection reducing inbound traffic that need to processed by back-end firewall (TMG Firewall), which means lower hardware requirements for back-end firewall. The same principle applies to back-end firewalls TMG.

The ASA firewall is configured with dual ISP connection for increased internet bandwidth and redundancy if any of the WAN connection shell fail. ASA provides load balancing capabilities combined with link failover, ensuring high network availability at the Edge.

The configuration setup shows Active\Standby m Active/Standby failover enables you to use a standby ASA to take over the functionality of a failed unit. When the active unit fails, it changes to the standby state while the standby unit changes to the active state. The unit that becomes active assumes the IP addresses (or, for transparent firewall, the management IP address) and MAC addresses of the failed unit and begins passing traffic. The unit that is now in standby state takes over the standby IP addresses and MAC addresses. Because network devices see no change in the MAC to IP address pairing, no ARP entries change or time out anywhere on the network.

It is important to note that Cisco ASA supports active-active model as well.

Back-End Firewall

The back-end firewall shows a TMG array with two nodes. The TMG firewall is an application layer firewall with advance application layer inspection. Having a multivendor configuration such as this, ensures greater security in terms complexity for the intruder to penetrate a multivendor setup, the intruder needs to have a deep knowledge of both vendors for attack to take place.

The TMG firewall uses active-active model where both nodes service both inbound and outbound connections. Both TMG firewalls and domain members, which allows titter domain integration in terms of user authentication for proxy and firewall clients. StarCom takes advantage of TMG web cache capabilities, built in IPS and VPN capabilities for external mobile workers.

Switched Network

The StarCom switched network follows best Cisco practices which includes a three layered approach Core, Distribution and Access layer. This model simplifies the task of building a reliable, scalable, and less expensive hierarchical internetwork because rather than focusing on packet construction.

Kosovo HQ is the only site following three layered approach, branch offices use only two layered approach access and distribution the network. Branch office do not required high level of path redundancy neither the flexibility that three layered approach offers.

The core network comprises of two layer ‘3’ 3560 Catalyst Switches. The switched offer routeing capabilities supporting inter VLAN communication.

The distribution and access layer comprises of two layer 2950 switches.

Link Aggregation

The interconnection or the uplink connection between core, distribution and access are interconnected by two Ethernet connections for increased fault tolerance and bandwidth needs. To achieve link aggregation and open standard LACP protocol is used.

```
Group: 1
----------
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP

Group: 2
----------
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP

Group: 3
----------
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
```

Protocol: LACP

Spanning Tree

Having multiple paths increases fault tolerance however it introduces another problem so called loops, at which a packet can travel at layer 4 can travel endlessly without timeing out. Cisco solves this problem by blocking redundant paths by acknowledging and monitoring each link path and building Spanning Tree topology starting from the root bridge.

At StarCom at Kosovo site the primary root bridge is cKSsw1 and secondary cKSsw2. The two switched have been manually setup as Root Bridge switches since they are the most powerful switches on the network.

Routing Protocol

A routed protocol is any network layer protocol that provides enough information in its network layer address to allow a packet to be forwarded from one host to another. In a complex network where multiple network exists maintaining a routing table manly by creating static routes, can be a challenging task and painful to maintain.

Therefore, a more elegant choice would be to use routing protocols such as EIGRP.

Enhanced Interior Gateway Routing Protocol (EIGRP) is Cisco's proprietary routing protocol, based on IGRP. EIGRP is a distance-vector routing protocol, with optimizations to minimize routing instability incurred after topology changes, and the use of bandwidth and processing power in the router.

The EIGRP provides fast convergence time, is much more scalable and provide greater cost path configuration which makes it routing protocol of choice. StarCom network consists of Cisco devices only, there for it utilizing EIGRP as a routing problem is not an issue.

Other routing protocols have been considered as well such as RIP and OSPF.

RIP – The Routing Internet Protocol is a distance vector protocol. Although very easy to configure, RIP has been discounted as the routing protocol because of drawbacks such as it can only use in networks that have fewer than 15 hops, it converges slowly on larger networks, it is prone to routing loops and routing updates can require significant bandwidth because the entire routing table is sent.

OSPF – On the other hand is a link state routing protocol. OSPF is a ‘Link-state protocol that was developed as a replacement for the distance vector routing protocol Routing Information Protocol. Link-state protocols do not exchange routes and metrics, they exchange only the state of the links they know about, and the cost associated with those links. This saves considerably on bandwidth.

StarCom uses EIGRP with autonomous system 1.

NTP

Synchronizing time with a reliable time source is not just important for Cisco devices, but for servers as well. In general any device that logs, processes certain time related task an accurate time and date is crucial to the operator.

Cisco devices such as switches, routers etc. relay on the external time source since they do not have an internal time clock to keep the time accrued, especially when the devices are cycled down or a power outage accurse. Cisco devices if logging is required accrued time and date is a must when log events are to be accured.

On a Cisco Packet Tracer all switches and routers are configured with an NTP time server with time authentication key. Ideally fore larger corporate environment we would have an on premise atomic clock device, however external time source can be used as well.

HSRP

The Hot Standby Router Protocol (HSRP) provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits.

The perimeter routers at StarCom WAN perimeter routers utilizes HSRP for transparent failover to ensure WAN traffic availability between StarCom HQ at Kosovo and branch offices located on different countries such as Albania, Croatia, Bosnia etc.

With HSRP, members of the virtual router group continually exchange status messages. One router can assume the routing responsibility of another if a router goes out of commission for either planned or unplanned reasons.

Basic Security

To enable ease of configuration and to assist technician’s when fault finding, each router has been given a unique hostname and for security passwords have been set up. When trying to access the router a prompt will ask the user to enter a password which will allow him access to User Exec Mode, a mode which will allow him to monitor things only. A second password is then required to enter Privileged Exec Mode, a mode which allows the user to gain detailed information. Here the user can also access the Configure Terminal Mode, where router configuration changes can be made.

Legal Banner

Login banners are common among network devices such as routers, switches, firewalls etc. The banner shows legal binding information to the user attempting to gain access to the device. Some corporate environments are bound by regulation that such a message is displayed others don't, generally such a decdion as what the contents of the message should be is made by security department or network administrators them self.

```
#########################################
#          Welcome to StaCom Corp          #
#        unauthorized users prohibited        #
#########################################
```

Cisco enables two types of login banners: login banner which is displayed upon successful logon to exec mode and a MOTD message or (Message of the Day) which is displayer before the login.

StarCom banner is rather simple one, welcoming any user login attempt however warning about unauthorized access. The same message is displayed for both MOTD and exec mode. Generally exec mode login banner incorporates more information such as dynamic variables that can show the router name and session ID, however StarCom banner is rather simple one.

Hostnames and Passwords

All network devices on the network follow some naming convention. The naming convention used identifies the network device location, role, and index number if more than one device with the same location and role is present.

Switches and Routers

[role][country][type][index]

Example: cKSsw1

c – core switch

KS – Kosovo

sw – switch

1 - index

Passwords

Generally password should follow complexity requirements, however for demonstration purposes a simple password was used.

Type	Password
Console	starcom
VTY 0-4	starcom
Secret	starcom

IP Addressing Table

For subneting information a class A IP address 10.0.0.0 /24 was used. The first three octets are used for network address where the last orated is left for host portion.

Kosovo Site

Device	Interface	IP Address	Subnet Mask
KSrouter	Gi 0/0	10.10.21.254	/24
	Gi 0/1	10.10.22.254	/24

	Gi 0/2	10.10.23.1	/24
	Serial 0/0/0	10.1.1.1	/24
	Serial 0/1/0	10.2.1.1	/24
	Serial 0/0/1	10.3.1.1	/24
	Serial 0/1/1	10.4.1.1	/24
cKSsw1	Fa 0/2	10.10.21.1	/24
cKSsw2	Fa 0/2	10.10.22.1	/24
Albania Site			
ALrouter	Gi 0/0	10.20.21.1	/24
	Serial 0/0/1	10.1.1.254	/24
dALsw1	Gi 0/2	10.20.21.254	/24
Bosnia Site			
BSrouter	Gi 0/0	10.21.21.1	/24
	Serial 0/0/0	10.2.1.24	/24
dBOsw1	Fa 0/1	10.21.21.254	/24
Croatia Site			
CRrouter	Gi 0/0	10.22.21.1	/24
	Serial 0/0/0	10.22.21.1	/24
dCRsw1	Fa 0/1	10.22.21.254	/24
Serbia Site			
SRrouter	Gi 0/0	10.23.21.1	/24
	Serial 0/0/0	10.4.1.254	/24
dSRsw1	Fa 0/0	10.23.21.254	/24

VLAN Information Table

Kosovo Site

VLAN Number	**Network Address**	**VLAN Name**	**Port Mapping**
1	NA	Default	**aKSsw1** fa0/4-24 **aKSsw2**

			fa0/4-24 **aKSsw4** fa0/6-24
2	10.10.1.254	Server Room	**aKSsw4** fa0/1, fa0/2, fa0/3
11	10.10.11.254	1st Floor	**aKSsw1** fa0/1, fa0/2, fa0/3
12	10.10.12.254	2nd Floor	**aKSsw2** fa0/1, fa0/2, fa0/3
13	10.10.13.254	3rd Floor	**aKSsw3** fa0/1, fa0/2
100	10.10.100.254	Management	**aKSsw3** fa0/3
Albania Site			
1	NA	Default	**aALsw1** fa0/2-24 **aKSsw2** fa0/3-24
2	10.20.1.254	Server Room	**aALsw2** fa0/1, fa0/2
11	10.20.11.254	1st Floor	**aALsw1** fa0/1
12	10.20.12.254	2nd Floor	NA
13	10.20.13.254	3rd Floor	NA
100	10.20.100.254	Management	NA
Bosnia Site			
1	NA	Default	**aBOsw1** fa0/2-24 **aBOsw2** fa0/3-24
2	10.21.1.254	Server Room	**aBOsw2** fa0/1, fa0/2
11	10.21.11.254	1st Floor	**aBOsw1**

			fa0/1
12	10.21.12.254	2nd Floor	NA
13	10.21.13.254	3rd Floor	NA
100	10.21.100.254	Management	NA
		Croatia Site	
1	NA	Default	**aCRsw1** fa0/2-24 **aCRsw2** fa0/3-24
2	10.22.1.254	Server Room	**aCRsw2** fa0/1, fa0/2
11	10.22.11.254	1st Floor	**aCRsw1** fa0/1
12	10.22.12.254	2nd Floor	NA
13	10.22.13.254	3rd Floor	NA
100	10.22.100.254	Management	NA
		Serbia Site	
1	NA	Default	**aSRsw1** fa0/2-24 **aSRsw2** fa0/3-24
2	10.23.1.254	Server Room	**aSRsw2** fa0/1, fa0/2
11	10.23.11.254	1st Floor	**aSRsw1** fa0/1
12	10.23.12.254	2nd Floor	NA
13	10.23.13.254	3rd Floor	NA
100	10.23.100.254	Management	NA

Literature Used

1. Active Directory, 5th Edition (Designing, Deploying, and Running Active Directory) by O'Reilly Media
2. Network Topology Optimization: The Art and Science of Network Design by Roshan Lal Sharma

Conclusion

Designing a proper malty geo separated Active Directory Infrastructure with underlying network layout takes a lot of planning effort and time. However, there is nothing more important than actual planning, unfortunately this process in many times overlooked by engineers with believe that certain steps can be overlooked in favour of more rapid deployment and time savings. Unfortunately, many times this believe can become a costly decision especially in large deployments as StarCom corporation.