Unit 4 : IP Addressing, Windows 2008 Server

LECTURER : NANDAN PANDYA

COURSE: BACHELOR OF COMPUTER APPLICATIONS (BCA)

SEMESTER: 4TH

SUBJECT: NETWORK TECHNOLOGY AND ADMINISTRATION

SUBJECT CODE: CS-21

COLLEGE: KAMANI SCIENCE COLLEGE, AMRELI

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Topics

- What is IP address?
- Types of IP address
- Class structure
- Subnet and Supernet
- Basic structure of ipv6
- Implementation of ipv6
- Migration from ipv4 to ipv6
- Installation of 2008 enterprise (practical)
- server and Various editions of windows 2008 server
- Installation & Configuration of Active Directory (Practical)
- Domains, Trees, Forests concept
- User account and user Group
- Security policy and audit policy
- Events logging
- MMC(Microsoft Management
- console)

IP Address

- IP address stands for internet protocol address; it is an identifying number that is associated with a specific computer or computer network. When connected to the internet, the IP address allows the computers to send and receive information.
- An IP address can be compared to a Social Security Number (SSN) since each one is completely unique to the computer or user it is assigned to. The creation of these numbers allows routers to identify where they are sending information on the internet. They also make sure that the correct devices are receiving what is being sent. Much like the post office needs a mailing address to deliver a package, a router needs an IP address to deliver to the web address requested.
- An example of an IP address would be: 123.234.223.255

Cont..

- There are four different types of IP addresses: public, private, static, and dynamic. While the public and private are indicative of the location of the network
- private being used inside a network while the public is used outside of a network
- static and dynamic indicate how they are assigned.
- A static IP address is one that was manually created, as opposed to having been assigned. A static address also does not change, whereas a dynamic IP address has been assigned by a Dynamic Host Configuration Protocol (DHCP) server and is subject to change.
- Dynamic IP addresses are the most common type of internet protocol addresses. Dynamic IP addresses are only active for a certain amount of time, after which they expire. The computer will either automatically request a new lease, or the computer may receive a new IP address.

IPV4

- IP stands for Internet Protocol and v4 stands for Version Four (IPv4). IPv4 was the primary version brought into action for production within the ARPANET in 1983.
- IP version four addresses are 32-bit integers which will be expressed in hexadecimal notation.
- Example- 192.0.2.126 could be an IPv4 address.

Parts of IPv4

- **Network part: (prefix)**
- The network part indicates the distinctive variety that's appointed to the network. The network part conjointly identifies the category of the network that's assigned.
- **Host Part: (suffix)**
- The host part uniquely identifies the machine on your network. This a part of the IPv4 address is assigned to every host.
- For each host on the network, the network part is the same, however, the host half must vary.

Characteristics of IPv4

- IPv4 could be a 32-Bit IP Address.
- IPv4 could be a numeric address, and its bits are separated by a dot.
- The number of header fields are twelve and the length of the header filed is twenty.
- It has Unicast, broadcast, and multicast style of addresses.
- IPv4 supports VLSM (Virtual Length Subnet Mask).
- IPv4 uses the Post Address Resolution Protocol to map to mack address.
- RIP may be a routing protocol supported by the routed daemon.
- Networks ought to be designed either manually or with DHCP.
- Packet fragmentation permits from routers and causing host.

Advantages of IPv4

- IPv4 security permits encryption to keep up privacy and security.
- IPV4 network allocation is significant and presently has quite 85000 practical routers.
- It becomes easy to attach multiple devices across an outsized network while not NAT.
- This is a model of communication so provides quality service also as economical knowledge transfer.
- IPV4 addresses are redefined and permit flawless encoding.
- Routing is a lot of scalable and economical as a result of addressing is collective more effectively.
- Data communication across the network becomes a lot of specific in multicast organizations.

Disadvantages of IPv4

- Limits net growth for existing users and hinders the use of the net for brand new users.
- Internet Routing is inefficient in IPv4.
- IPv4 has high System Management prices and it’s labor intensive, complex, slow & frequent to errors.
- Security features are nonobligatory.
- Difficult to feature support for future desires as a result of adding it on is extremely high overhead since it hinders the flexibility to attach everything over IP.

IP4 Address Classes

Class	Use	Range
A	Large numbers of nodes – Intended for a large organization	1.0.0.1 to 126.255.255.254
B	Medium number of nodes	128.1.0.1 to 191.255.255.254
C	Small number of nodes- Intended for a small organization	192.0.1.1 to 223.255.254.254
D	Reserved for multicast groups	224.0.0.0 to 239.255.255.255
E	Reserved for future use, or research and development purposes	240.0.0.0 to 254.255.255.254

Subnet/Subnet mask

- Short for subnetwork mask, a subnet mask is data used for bitwise operations on a network of IP addresses that is divided into two or more groups. This process, known as subnetting, divides an IP network into blocks of logical addresses. Subnetting can improve security and help to balance overall network traffic.
- A common example of a subnet mask for class C IP addresses is 255.255.255.0, the default subnet mask for many computers and network routers. When applied to subnet, a subnet mask shows the routing prefix.

Supernetting

- Supernetting is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.
- Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols.

Advantages/Disadvantages

- Control and reduce network traffic
- Helpful to solve the problem of lacking IP addresses
- Minimizes the routing table

- It cannot cover different area of network when combined
- All the networks should be in same class and all IP should be contiguous

IPV6

- An IPv4 address consists of four numbers, each of which contains one to three digits, with a single dot (.) separating each number or set of digits. Each of the four numbers can range from 0 to 255. This group of separated numbers creates the addresses that let you and everyone around the globe to send and retrieve data over our Internet connections. The IPv4 uses a 32-bit address scheme allowing to store 2^32 addresses which is more than 4 billion addresses. To date, it is considered the primary Internet Protocol and carries 94% of Internet traffic.
- An IPv6 address consists of eight groups of four hexadecimal digits.
- Here’s an example IPv6 address: 3001:0da8:75a3:0000:0000:8a2e:0370:7334
- This new IP address version is being deployed to fulfill the need for more Internet addresses. It was aimed to resolve issues which are associated with IPv4. With 128-bit address space, it allows 340 undecillion unique address space. IPv6 also called IPng (Internet Protocol next generation).

Types of IPv6 Address

- **Unicast addresses:** It identifies a unique node on a network and usually refers to a single sender or a single receiver.
- **Multicast addresses:** It represents a group of IP devices and can only be used as the destination of a datagram.
- **Anycast addresses:** It is assigned to a set of interfaces that typically belong to different nodes.

Advantages of IPv6

- Reliability
- Faster Speeds: IPv6 supports multicast rather than broadcast in IPv4.This feature allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations all at once.
- Stringer Security: IPSecurity, which provides confidentiality, and data integrity, is embedded into IPv6.
- Routing efficiency
- Most importantly it's the final solution for growing nodes in Global-network.

Disadvantages of IPv6

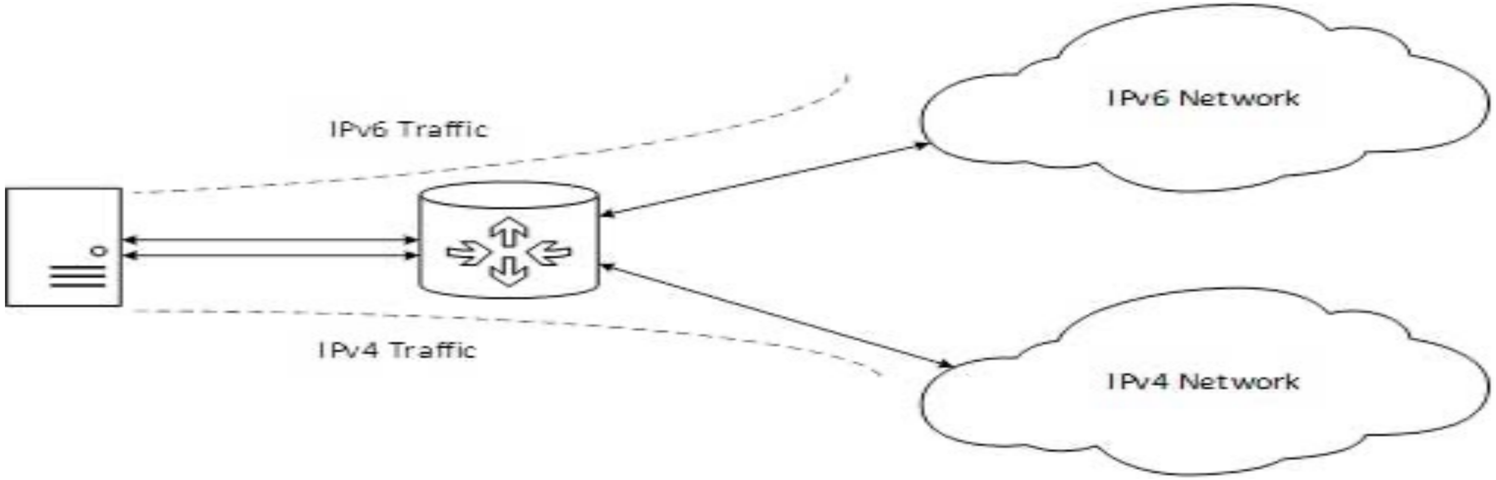
- Conversion: Due to widespread present usage of IPv4 it will take a long period to completely shift to IPv6.
- Communication: IPv4 and IPv6 machines cannot communicate directly with each other. They need an intermediate technology to make that possible.

IPv6 Transition/migration/converting

- **Dual Stack** – Running both IPv4 and IPv6 on the same devices
- **Tunneling** – Transporting IPv6 traffic through an IPv4 network transparently
- **Translation** – Converting IPv6traffic to IPv4 traffic for transport and vice versa.

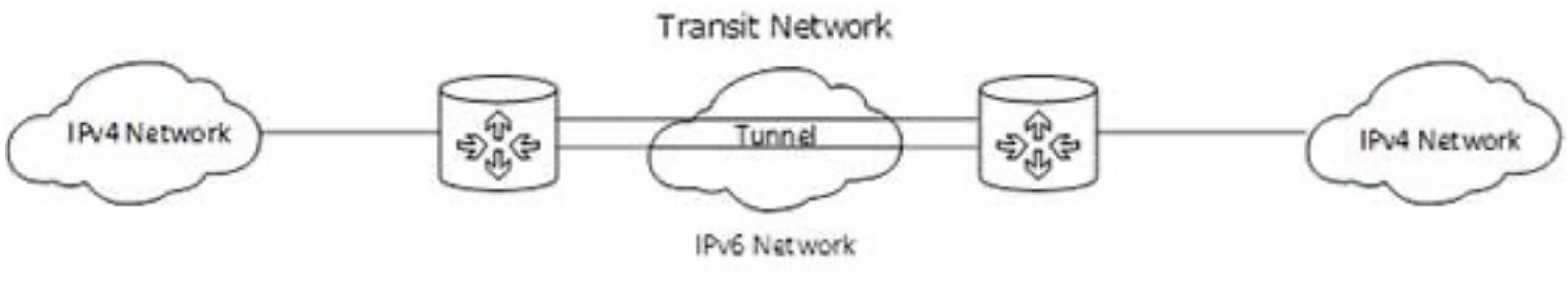
Dual Stack

- The simplest approach when transitioning to IPv6 is to run IPv6 on all of the devices that are currently running IPv4. If this is something that is possible within the organizational network, it is very easy to implement. However, for many organizations, IPv6 is not supported on all of the IPv4 devices; in these situations other methods must be considered.



Tunneling

- A given packet is encapsulated into a wrapper than enables its transport from a source to destination transparently where it is decapsulated and retransmitted. There are a number of different tunneling methods that exist for IPv6, many that are integrated as part of Cisco and other manufactures certification tests.



Tunneling methods

- **Manual IPv6 Tunnels** – A manually created IPv6 tunnel is configured between two routers that each must support both IPv4 and IPv6. Incoming traffic that is destined for networks on the other side of the tunnel is encapsulated on the source router and tunneled through IPv4.
- **6to4 Tunnels** – As the name suggest a 6to4 tunnel allows IPv6 to be tunneled via IPv4. Unlike the previously discussed tunneling methods, the 6to4 method is automatically set up using the 2002::/16 IPv6 address space. The IPv4 address for the edge routers is embedded in an IPv6 address that is created.
- **IPv6 rapid deployment (6rd)** – The 6rd method was derived from the 6to4 method but allows the implementer to use the IPv6 block that was assigned to it.
- **IPv4 Compatible Tunnels** – The IPv4 Compatible tunneling method is very similar to 6to4 tunneling; both provide a mechanism to tunnel IPv6 over IPv4. The major difference is how the IPv4 address is embedded inside the IPv6 address that is used by the edge device. IPv4 Compatible tunnels have been depreciated but are still covered in some certification exams (including the current Cisco ROUTE exam).

Translation

- A translation method provides a way to translate IPv6 to IPv4 traffic and vice versa. When using translation, the traffic is not encapsulated but is converted to the destination type (be that IPv4 or IPv6).
- **Network Address Translation**—Protocol Translation (NAT-PT) – The NAT-PT method enables the ability to either statically or dynamically configure a translation of a IPv4 network address into an IPv6 network address and vice versa. For those familiar with more typically NAT implementations, the operation is very similar but includes a protocol translation function. NAT-PT also ties in an Application Layer Gateway (ALG) functionality that converts Domain Name System (DNS) mappings between protocols.
- **NAT64** – One of the main limitations to NAT-PT was that it tied in ALG functionality; this was considered a hindrance to deployment. With NAT64 also came DNS64, both of which are configured and implemented separately; when these were defined and accepted the use of NAT-PT was depreciated. NAT64 offers both a stateless and stateful option when deploying, the later that keeps track of bindings and enables 1-to-N functionality.

Conversion IPV4 to IPV6

- An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols.
- Even after converting into Hexadecimal format, IPv6 address remains long. IPv6 provides some rules to shorten the address.
- **Rule 1**: Discard leading Zero(es)
- **Rule 2**: If two of more blocks contain consecutive zeroes, omit them all and replace with double colon sign ::
- **Rule 3** : Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address, they can be shrunk down to a single zero

Example

- **IPV4**: 192.168.68.1
- **Binary**: 11000000.10101000.01000100.00000001
- **IPV6**: 0000:0000:0000:0000:2AEE:52FF:FEBA:071B
- **Binary**: 0000000000000000_0000000000000000_0000000000000000 0000000000000000_0010101011101110_0101001011111111 _1111111010111010_0000011100011011
- **Final IPV6**: 0::2AEE:52FF:FEBA:71B

Windows server 2008 installation

- http://bit.ly/ser2008
- https://www.youtube.com/watch?v=GGUIl_95aTM

Windows Server 2008 Standard

- It is the standard edition of Windows Server 2008 and is directed to the SMB sector, the servers with this operating system will often play the roles of domain controller, file and print server, DNS, DHCP server and application server. These functions do not require much memory. When planning the installation of such system it must been take into account that the functions of failover cluster and AD Federation Services are functions of the Enterprise edition or Datacenter edition. The 32-bit version supports up to 4GB of RAM and up to 4 processors in SMP configuration has a 64-bit version supports up to 32GB of RAM and up to 4 processaodres SMP configuration. It supports cluster Load Balancing Network, but does not support failover clustering.

Windows Server 2008 Enterprise

- The Enterprise edition will be indicated for large companies running heavy applications like SQL Server 2008 or Exchange Server 2007, these applications will require more memory than the Standard edition supports. In addition, the Enterprise has the resources Failover cluster and ADFS. The wise thing to do is put the Standard and Enterprise working together when these demands exist, the Standard running the most plain papers and Enterprise applications running the heavier ones or working in failover cluster. the 32-bit version supports up to 64GB of RAM and up to 8 processors in SMP configuration has a 64-bit version supports up to 2TB of RAM and up to 8 processaodres SMP configuration.

Windows Server 2008 Datacenter

- The Datacenter edition is intended only to large enterprise market, the main difference from the Enterprise is on the number of virtual machines that can be used with a single license is unlimited . Normally a license of the Datacenter will be associated with a physical server in the form of OEM, meaning that they can be only been bought together. The reason is that these servers typically cost tens or even hundreds of thousands of dollars and the support from those who sold is given about the software and hardware, is not permissible for a server to stop due to a faulty motherboard much less by a system error.

Windows Web Server 2008

- This edition is indicated only for servers that run IIS service, the Microsoft web server. The 32-bit version supports up to 4GB of RAM and up to 4 processors in SMP configuration as the 64 bit supports up to 32GB of RAM and up to 4 processors in SMP configuration.

Windows Server 2008 Server Core

- All editions of Windows Server 2008 have two types, Full and Server Core Installation, Full installation is where most functions are managed via the GUI (graphical user interface) or CLI (command line interface), Server Core run only in CLI, and it has two direct implications: First, a reduction in the attack interface, which means that the attacks of malicious agents is decreased. The second implication is that once running the server will have fewer components requisites for the installation are simpler, as less memory and processing. The most of time, you can use MMC, and add a snap-in for use configure you're Server Core (after enabling preferences with sconfig.cmd)

Domain

- A domain, in the context of networking, refers to any group of users, workstations, devices, printers, computers and database servers that share different types of data via network resources. There are also many types of subdomains.
- A domain has a domain controller that governs all basic domain functions and manages network security. Thus, a domain is used to manage all user functions, including username/password and shared system resource authentication and access. A domain is also used to assign specific resource privileges, such as user accounts.

Cont..

- A domain contains a group of computers that can be accessed and administered with a common set of rules. For example, a company may require all local computers to be networked within the same domain so that each computer can be seen from other computers within the domain or located from a central server. Setting up a domain may also block outside traffic from accessing computers within the network, which adds an extra level of security.
- While domains can be setup using a variety of networking software, including applications from Novell and Oracle, Windows users are most likely familiar with Windows Network Domains. This networking option is built into Windows and allows users to create or join a domain. The domain may or may not be password-protected. Once connected to the domain, a user may view other computers within the domain and can browse the shared files and folders available on the connected systems.

Activity Directory

- An Activity Directory is a product of Microsoft that runs on Server of Windows. It allows managing, accessing, and permissions for the network resources. The data is stored as an object in this directory and the object can be anyone such as user, files, shared folders, device, groups or an application. The categorization of these objects is done either by name or attribute.
- An active directory can be found in most of the windows server operating system in the form of services and processes. The beginning of this directory was started with windows server 2001 and later on they became a part of various other directory-based identity-related services.

Cont..

- In the active directory, there is a domain which is the core unit in logical structure. All the objects that are named under common directory database, security policies and trust relationships with other domain are known as Domains. Each domain stores information only about the objects that belong to that domain.
- All security polices and settings, such as administrative rights, security policies, and Access Control Lists (ACLs), do not cross from one domain to another. Thus, a domain administrator has full rights to set policies only within domain they belong to. Domains provide administrative boundaries for objects and manage security for shared resources and a replication unit for objects.
- Thus, the active directory organizes all the information. Moreover, it allows the domain controller to perform authorization and authentication for users to access resources. An object is a physical entity of a network and there can be multiple objects in active directory. Tree and Forest are two such objects

Activity Directory setup

- https://www.youtube.com/watch?v=gg5fQTtG69Y

Tree

- The tree can be defined as the collection of one or more domains that allow the sharing of resources globally. It comprises of single domain or multiple domain in the contiguous namespaces. Whenever we add the domain in the tree it becomes the offspring of the tree root domain and the domain it is attached with becomes the parent domain. Parent domain name is utilized by the child domain and further gets the unique Domain Name System (DNS).
- As an example, if abc.com is the root domain, users can create one or more Child domains to abc.com such as south.abc.com and or north.abc.com. Further, these “child” domains may also have sub-child domains that can be created under them, such as profit.south.abc.com.
- The domains created in a tree has two way of relationship named as Kerberos transitive trust relationships. A Kerberos transitive trust simply means that if Domain 1 trusts Domain 2 and Domain 2 trusts Domain 3, then Domain 1 trusts Domain 3. Therefore, it implies that a domain joining a tree immediately has trust relationships established with every domain in the tree.

Forest

- A Forest can be explained as a collection of multiple trees which is shared by the common global catalogue, logical structure, directory schema, and directory configuration. It comprises of in built two ways transitive trust relationships. The very first domain created in the forest is called the forest root domain.
- If there are different naming schemes than the forest allows each organization to group their divisions and it may need to operate independently. But being as an organization, they want to communicate with the entire organization via transitive trusts and share the same schema and configuration container.

Difference

Parameter	Tree	Forest
Definition	A Tree is a collection of one or more domains or domain trees in a contiguous namespace that is linked in a transitive trust hierarchy.	A Forest is a collection of trees that share a common global catalogue, directory schema, logical structure and directory configuration.
Association	A tree is a set of domain.	A forest is a set of trees.
Communication	Domains inside a Tree can communicate with each other using one way or two-way trust	Two Forests can communicate by creating a forest level trust.

User and user group

- Users can be either people, meaning accounts tied to physical users, or accounts which exist for specific applications to use.
- Groups are logical expressions of organization, tying users together for a common purpose. Users within the same group can read, write, or execute files owned by the group.
- Each user and group has a unique numerical identification number called a userid (UID) and a groupid (GID) respectively.

Security Policy

- A security policy is a written document in an organization outlining how to protect the organization from threats, including computer security threats, and how to handle situations when they do occur.
- A security policy must identify all of a company's assets as well as all the potential threats to those assets. Company employees need to be kept updated on the company's security policies. The policies themselves should be updated regularly as well.
- In business, a security policy is a document that states in writing how a company plans to protect the company's physical and information technology (IT) assets. A security policy is often considered to be a "living document", meaning that the document is never finished, but is continuously updated as technology and employee requirements change. A company's security policy may include an acceptable use policy, a description of how the company plans to educate its employees about protecting the company's assets, an explanation of how security measurements will be carried out and enforced, and a procedure for evaluating the effectiveness of the security policy to ensure that necessary corrections will be made.

Security Audit

- Network security audits are a vital component of an organization’s ongoing risk mitigation strategy. Whether the audit is conducted by an internal team or an external auditing firm, the process involves a detailed and measurable assessment of an organization’s security policies and controls. While the word “audit” might suggest that such assessments are unexpected, in most cases, a cybersecurity audit is carried out with the full knowledge and cooperation of the company in question.
- A security audit is an exhaustive process that can take some time to complete. That’s because auditors don’t just look at the technical side of network security (such as firewalls or system configurations), but also at the organizational and human side of security policies. In addition to examining IT systems and historical data, they also need to conduct a series of personal interviews and review documentation to ensure information security procedures meet relevant compliance standards and are actually being followed on a day-to-day basis.

Event Logging

- Many applications record errors and events in proprietary error logs, each with their own format and user interface. Data from different applications can't easily be merged into one complete report, requiring system administrators or support representatives to check a variety of sources to diagnose problems.
- Event logging provides a standard, centralized way for applications (and the operating system) to record important software and hardware events. The event logging service records events from various sources and stores them in a single collection called an event log. The Event Viewer enables you to view logs; the programming interface also enables you to examine logs.

Microsoft Management Console(MMC)

- You use Microsoft Management Console (MMC) to create, save and open administrative tools, called consoles, which manage the hardware, software, and network components of your Microsoft Windows operating system. MMC runs on all client operating systems that are currently supported.
- You can use MMC to create custom tools and distribute these tools to users. With both Windows XP Professional and Windows Server 2003, you can save these tools so that they're available in the Administrative Tools folder.
- A snap-in is a tool that is hosted in MMC. MMC offers a common framework in which various snap-ins can run so that you can manage several services by using a single interface. MMC also enables you to customize the console. By picking and choosing specific snap-ins, you can create management consoles that include only the administrative tools that you need.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli