Online Supplements

Domain 1.0 Networking Concepts

[IPv6]
1.3 Explain the purpose and properties of IP Addressing

Similar to IPv4 classless addresses, IPv6 addresses are fundamentally divided into a network portion followed by a host portion. The network portion is called the **network prefix**and the number of bits used is the **prefix length**. The prefix is represented with a slash followed by the prefix length. This is the same notation used to designate the CIDR in IPv4. For example, the IPv6 address of 2001:DB8:FEED:BEEF::12 has a 64-bits network prefix. It then can be represented as 2001:DB8:FEED:BEEF::12/64. However, the concept of a CIDR is not relevant in IPv6, since there is enough IP address space for everyone. So, in IPv6 the host portion of the address or what is called the **interface identifier** is always 64-bits in length. This automatically leaves 64 bits as the network prefix. In a typical IPv6 customer site, a network of /48 is usually allocated by IANA. This provides the site with 65536 subnets which is more than sufficient.This means that when a site is assigned a /48. The site is capable of having up to 65536 subnets.

There are three types of IPv6 addresses. These are unicast, multicast, and anycast.The **unicast** IPv6 address is used to identify a single network interface address and data packets are sent directly to the computer with the specified IPv6 address. There are several types of unicast addresses including link-local addresses, global unicast addresses, and unique local addresses. Link-local addresses are designed to be used for and are limited to communications on the local link. Every IPv6 interface will have one link-local address.

Per RFC 4291, IP Version6 Addressing Architecture, the network prefix of link-local addresses is defined as FE80::/10. Unique local unicast addresses are addresses for local use only and they are similar to the private ip addresses used in IPv4. Unique local unicast addressesuse the prefix of FD00::/8 and were designed to replace site-local addresses, which are being deprecated.

Global unicast addresses are equivalent to the public ip addresses in IPv4. They have unlimited scope and they are routable on the Internet. IANA is responsible for allocating the IPv6 global unicast address space. Currently, the range of allocated IPv6 addresses starts from prefix 2000::/3.

MulticastIPv6 addresses are defined for a group of networking devices. Data packets sent to a multicast address are sent to the entire group of networking devices such as a group of routers running the same routing protocol. Multicast addresses all start with the prefix FF00::/8. The next group of characters in the IPv6 multicast address (the second octet) are called the scope. The scope bits are used to identify which ISP should carry the data traffic.

The **anycast**IPv6 addresses may seem like a new type of address, but its concept was not new. Anycast addresses can be thought of a cross between unicast and mutlicast addresses. While the unicast traffic sends information to one address and the muticast traffic sends information to every address in the

group, the anycast traffic sends information to any one address of the group. The trick is which address of the group to send information to. The most logical and efficient answer is the nearest or the closet address. Similar to multicast where the nodes will join the multicast group, the anycast nodes share the same anycast address. The data will be sent to a node within the anycast group. This node is the nearest to the sender.

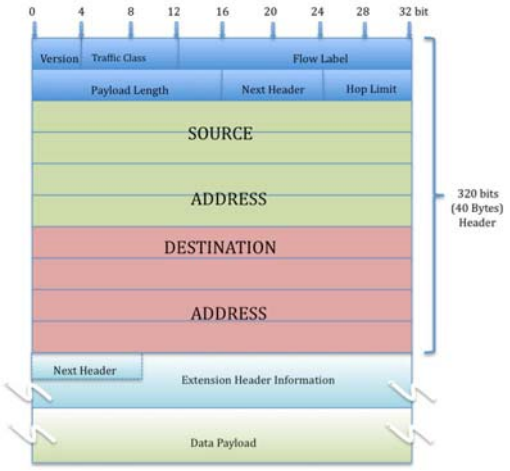
The interface identifier of the link-local address is derived by transforming the 48 bits of the EUI-48 MAC address to 64 bits for EUI-64. This EUI-48 to EUI-64 transform algorithm is also used to derive the interface identifier for the global unicast address.

eui-64allows the router to choose its own host identifier

SLA ID is the Site Level Aggregation Identifier that is used by individual organizations to identify subnets within their site. The SLA ID is 16 bits long.

TLA ID (0x2002) is the Top Level Identifiers are issued to local Internet registries. These IDs are administered by IANA **(http://www.iana.org/).** The TLA is used to identify the highest level in the routing hierarchy. The TLA ID is 13 bits long.

FPis the Format Prefix which is made up of the higher order bits. The **001** indicates that this is a global unicast address. The current list of the IPv6 address allocation can be viewed at http://www.iana.org/assignments/ipv6-unicast-address-assignments. Currently, IANA allocates 2000::/3 as an IPv6 global pool. 2000 can be written in binary as **001**0 0000 0000 0000. 001 is the 3 highest order bits, which correspond to the FP.



IPv6 Header Field Position

Domain 1.0
Virtualization Terminology
[Virtualization Terminology]
VT – Virtualization Technology

Host System - This is basically a computer on a network.

VSwitch- This stands for virtual switch and is used to signify networking devices connecting virtual machines at layer 2 (MAC address layer)

Type 1 Hypervisor – A Type 1 Hypervisor runs directly on the system hardware. It is also called a Virtual Machine Monitor (VMM). This provides the backgroung management for virtual management.

VMM – Virtual Machine Monitor or virtualization manager

Virtual desktop – Used to display images on an external monitor at a higher resolution than is typically supported by a flat-panel display.

Hypervisor – This is a VMM

Hardware Assistant – This virtualization changes access to the operating system and the operating system has direct access to resources without emulation or modification of the operating system.

.vmdk - VMware Image file

Type 2 Hypervisor – These run on a host operating system and provides virtualization services such as I/O devices and memory management. These are mainly used on client systrtems.

VM clone – This is a copy of an existing virtual machine.

.vhd - Virtual Hard Disk file

Paravirtualization – This is a communication method between the guest operating system and the hypervisor.

Unity – This provides the underlying operating system with a distinct and consistent look while maintaining functionality with applications within the operating system.

Snapshot – A snapshot is a picture in time of how the data was organized. The Snapshot can be used to provide a consistent view of a file system for the purposes of backup or recovery.

Domain 1.0
Virtualization Technology and Services
[Virtualization Technology and Services]

VoIP – Voice over IP

Virtual desktop – This is used to describe how the virtual space of a computer's desktop environment can be expanded beyond the physical limits of the existing system through the use of software.

Cloud Computing service – This incorporates the use of a network of online srtotage. The hosts are generally 3rd parties.

Virtual Private Network – This establishes a secure network connection

Virtual PBX- This is a business phone system that does not require any customer installed equipment.

Communication Service Provider - a company that provides telecommunication, wireless, and Internet service

Virtual Application Server – In this application, the server resources are hidden from the users. Software is used to divide the physical server into multiple virtual environments. This provides virtual applications on demand.

Parvirtualization – In this case, the Virtual Machine Interface is a communications mechanism between the guest operating system and the hypervisor.

Cloud storage service – In this case, data is stored outside the enterprise's home data storage.

Domain 2.0 Network Installation and Configuration
[Configuring InterVLAN Routing]

InterVLAN Routing Configuration

Each VLAN is its own broadcast domain. It cannot forward traffic across its VLAN boundaries. However, it is almost impractical in today's applications for a VLAN not to be able to communicate beyond itself. To enable communications among VLANs, InterVLAN routing is required.

The most logical solution to route traffic between different VLANs is to introduce or create a layer 3 routed network between them. One traditional way is to connect each VLAN to a router interface. Then, each router interface is configured as a different layer 3 network. This enables VLANs to communicate and pass traffic via the layer 3 IP network. For a few VLANs, this does not present an issue, but for a large number of VLANs this could create some issues. What this means is every VLAN will require a physical connection to a router port. Router ports are expensive and this design can be costly as the number of VLANs increases and more physical links are required.

Domain 2.0 Network Installation and Configuration
[Address Translation Technology]

local address

defines any IP address that is on the inside of or internal to the network.

global address

defines any IP address that is on the outside of or external to the network

Port Address Translation(PAT)

a technique that uses the port number to identify the computer that established the Internet connection, also called many-to-one NAT and NAT overload

Network Address Translation (NAT)

a technique used to translate an internal private IP address to a public IP address

static NAT

a fixed one-to-one mapping of an inside IP address to an outside IP address

dynamic NAT

this is a one-to-one mapping from an available global pool

NAT overload
another name for PAT

RFC 1918
This is address allocation for private internets. The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets: 10.0.0.0 - 10.255.255.255 (10/8 prefix) 172.16.0.0 - 172.31.255.255 (172.16/12 prefix) 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Domain 4.0 Network Management
Using traceroute Troubleshoot Connectivity
[Traceroute / Tracert]

Once your network is setup you can use the *traceroute<destination ip address>*command on your router to discover the routes the data packets (datagrams**)** actually take when traveling from the source to the destination. The command is issued from the Privileged EXEC mode on a router as shown.

R1#traceroute<destination ip address>

```
Router1#traceroute 10.10.5.250

Type escape sequence to abort.
Tracing the route to 34.0.0.4

  1 10.10.200.2   4 msec 4 msec 4 msec
  2 10.10.5.250  16msec *  16 msec
```

You can also trace packets from the PC by using the *tracert<destination ip address>*command.

Domain 4.0 Network Management
Explain the different methods and rationales for network performance optimization
[Network Performance Optimaztion]

QoS –Quality of Service

Latency sensitivity – the delay in data packet delivery

HSRP – This is a Cisco proprietary protocol that is used as a protocol for establishing a fault-tolerant gateway.

Traffic Shaping – This enables network traffic management and is used to optimize, improve latency, and increase usable bandwidth.

.
Caching Engine – This service is provided by a network server and is used to save Web pages or othe Internet content locally.

Load Balancing – a technique used to balance data through a router

High Availability – This has to do with the availability of resource in a computer system.

Uptime – indicates the amount of time has been running

Fault Tolerance – This has too do with how a systems responds to unexpected behavior or a software failure.

CARP – This stands for ***C****ommon* ***A****ddress* ***R****edundancy* ***P****rotocol* and is a free substitute for the Virtual Router Redundancy Protocol and the Hot Standby Protocol. The objective of this is to allow multiple hosts on the same network segment to share an IP address.

Domain 5.0

Explain common threats, vulnerabilities, and mitigation techniques

[Storage]

normal backup – This is the standard method of copying files to another medium in case of a failure.

Striping – This technique spreads data over multiple disks drives. This technique can be use to speed up data retrieval.

RAID 0 – This is short for redundandt array of independendent disks. RAID allows for the storage of data to redundant places.

Removable Storage – data storage that can be revoked from the computer. A typical example is the jump drive.

Differential Backup – This is a backup of the data files that have been modified since the last backup.

Incremental Backup – This provides a backup of only the information that has been modified since the last backup.

Storage Area Network- A SAN is a device that contains only disks for storing data..

Network Attached Storage –This is a device that is dedicated to only file sharing..

RAID 5 This level of RAID provides data striping at the byte level and it also contains stripe error correction. Level 5 is quite popular because it provides excellence performance and fault tolerance.

Cloud Storage – This is data storage online “in the cloud”. The data can be stored and be accessible from multiple distributed and connected resources.

RAID 1 – This provide disk mirroring thereby providing twice the read transaction rate of a single disk. The write transaction rate will e the same.

Parity – This is a method used to verify that data has been transmitted without errors. The parity bits are added to make the total number of 1’s received to be either an odd or even number.

Disaster Recovery Plan – This is a plan for a worst case scenario when all or part of the data records are destroyed. The objective of the disaster recovery plan is to get the system back online with minimal negative impact.

Offsite backup – a backup system that is located offsite, away from the influences (e.g. power failures, fire, theft) for the local site.