192.168.0.34

vs

2001:0db8:85a3:08d3:1319:8a2e:0370:7334

32 bits IPv4 vs 128 bit IPv6 address example

IPv6 address structure

- Divided into routing prefix, subnet identifier, and interface identifier

Subnet ID

X:X:X:X:X:X:X:X

Routing prefix Interface ID

2001:0db8:85a3:0000:0000:8a2e:0370:7334

Routing prefix Subnet ID Interface ID

IPv6 abbreviation

2001:0db8:85a3:0000:0000:8a2e:0370:7334

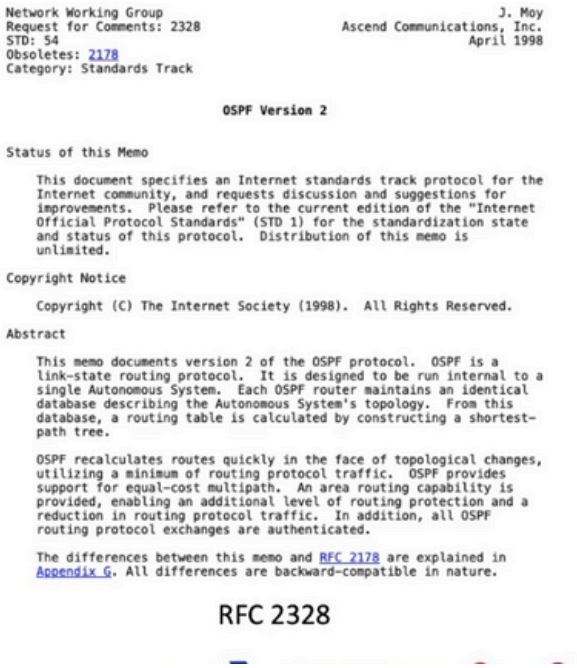
2001:db8:85a3::8a2e:370:7334

2001:0000:85a3:0000:0000:8a2e:0370:7334

2001:0:85a3::8a2e:370:7334

OSPF protocol

- Open Shortest Path First
- Interior Gateway Routing Protocol (IGP)
- Uses the Dijkstra algorithm to calculate the shortest paths
- Exchanges routing information through Link State Advertisement (LSA) packets
- Uses cost-based metrics to determine the best route



Network Working Group
Request for Comments: 2328
STD: 54
Obsoletes: 2178
Category: Standards Track

J. Moy
Ascend Communications, Inc.
April 1998

OSPF Version 2

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1998). All Rights Reserved.

Abstract

This memo documents version 2 of the OSPF protocol. OSPF is a link-state routing protocol. It is designed to be run internal to a single Autonomous System. Each OSPF router maintains an identical database describing the Autonomous System's topology. From this database, a routing table is calculated by constructing a shortest-path tree.

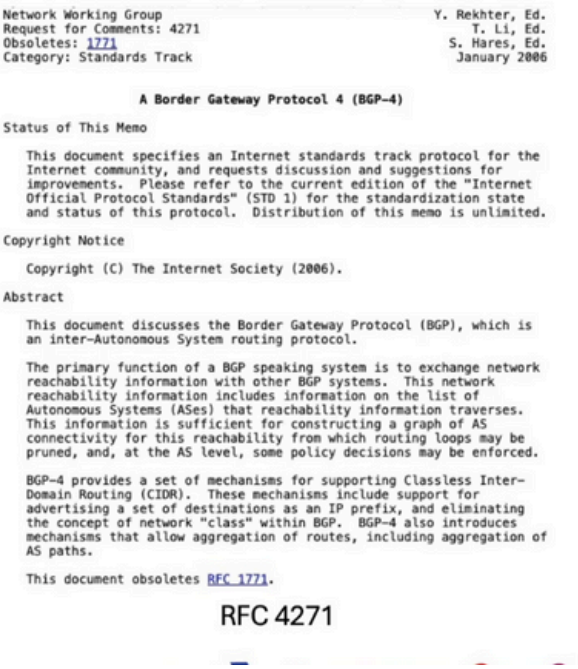
OSPF recalculates routes quickly in the face of topological changes, utilizing a minimum of routing protocol traffic. OSPF provides support for equal-cost multipath. An area routing capability is provided, enabling an additional level of routing protection and a reduction in routing protocol traffic. In addition, all OSPF routing protocol exchanges are authenticated.

The differences between this memo and RFC 2178 are explained in Appendix G. All differences are backward-compatible in nature.

RFC 2328

BGP protocol

- Border Gateway Protocol
- Exterior Gateway Routing Protocol (EGP)
- Interconnects Autonomous Systems (AS) on the Internet
- Uses a distance vector system and route attributes to select the best routes
- It is a policy-based protocol and allows manipulation of route attributes



Network Working Group
Request for Comments: 4271
Obsoletes: 1771
Category: Standards Track

Y. Rekhter, Ed.
T. Li, Ed.
S. Hares, Ed.
January 2006

A Border Gateway Protocol 4 (BGP-4)

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document discusses the Border Gateway Protocol (BGP), which is an inter-Autonomous System routing protocol.

The primary function of a BGP speaking system is to exchange network reachability information with other BGP systems. This network reachability information includes information on the list of Autonomous Systems (ASes) that reachability information traverses. This information is sufficient for constructing a graph of AS connectivity for this reachability from which routing loops may be pruned, and, at the AS level, some policy decisions may be enforced.

BGP-4 provides a set of mechanisms for supporting Classless Inter-Domain Routing (CIDR). These mechanisms include support for advertising a set of destinations as an IP prefix, and eliminating the concept of network "class" within BGP. BGP-4 also introduces mechanisms that allow aggregation of routes, including aggregation of AS paths.

This document obsoletes RFC 1771.

RFC 4271

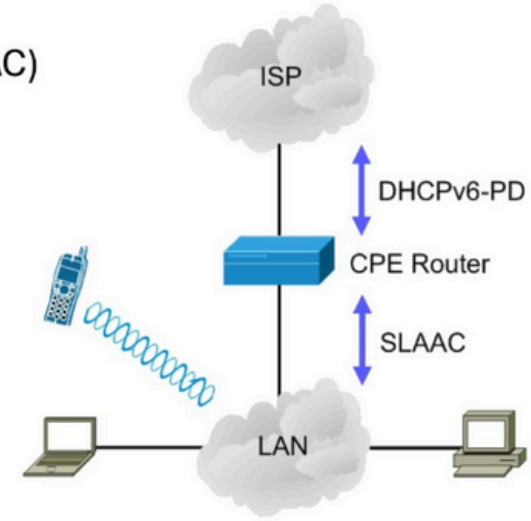
OSPF and BGP

- **Common characteristics:**
  - Both protocols are essential for efficient routing in IPv6 networks
  - OSPF operates within an Autonomous System (AS), while BGP operates between Autonomous Systems on the Internet
  - Both protocols aim to find optimal and reliable routes across the network, but they are applied in different contexts (within an AS vs. between ASes)

Autoconfiguration features

- Stateless autoconfiguration:
  - Stateless Address AutoConfiguration (SLAAC)
  - Automatic address generation

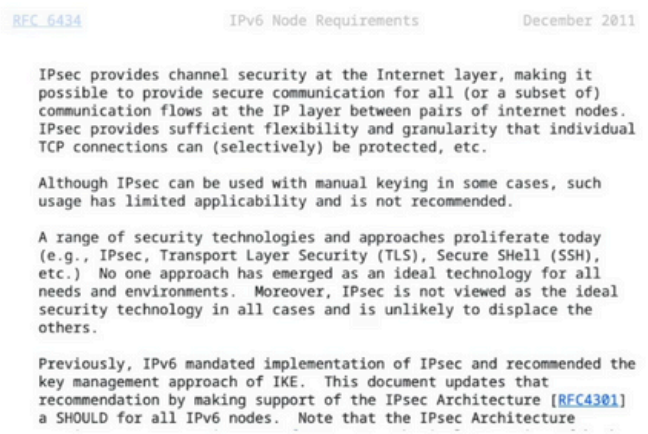
- Stateful autoconfiguration:
  - Address assignment via DHCPv6



Picture source: How IPv6 SLAAC Responds to Renumbering Events (internetsociety.org)

Enhanced security (IPsec)

- **Authentication:**
  - Verification of identity
- **Integrity:**
  - Assurance that data is not altered
- **Confidentiality:**
  - Encryption of transmitted data



RFC 6434 IPv6 Node Requirements December 2011

IPsec provides channel security at the Internet layer, making it possible to provide secure communication for all (or a subset of) communication flows at the IP layer between pairs of internet nodes. IPsec provides sufficient flexibility and granularity that individual TCP connections can (selectively) be protected, etc.

Although IPsec can be used with manual keying in some cases, such usage has limited applicability and is not recommended.

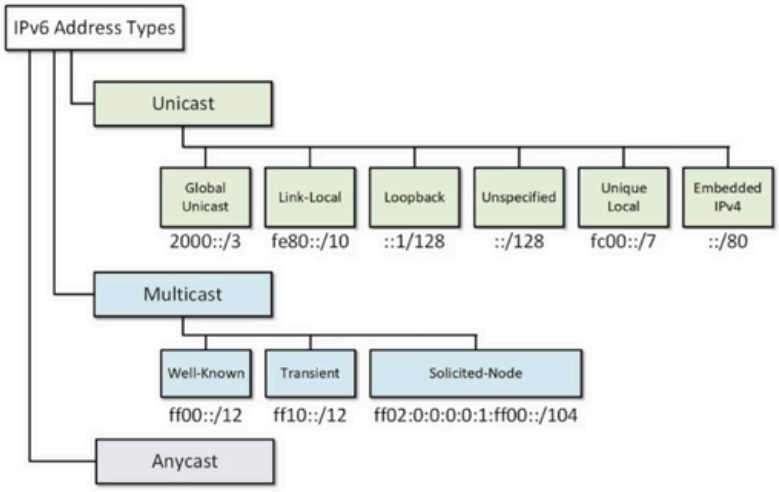
A range of security technologies and approaches proliferate today (e.g., IPsec, Transport Layer Security (TLS), Secure SHell (SSH), etc.) No one approach has emerged as an ideal technology for all needs and environments. Moreover, IPsec is not viewed as the ideal security technology in all cases and is unlikely to displace the others.

Previously, IPv6 mandated implementation of IPsec and recommended the key management approach of IKE. This document updates that recommendation by making support of the IPsec Architecture [RFC4301] a SHOULD for all IPv6 nodes. Note that the IPsec Architecture

IPsec in RFC 6434 (IPv6 Node Requirements)

Unicast

- One-to-one Communication
- Different types:
  - Global Unicast
  - Link-Local
  - Loopback
  - Unspecified
  - Unique Local
  - Embedded IPv4



Picture source: Types of IPv6 networks (networkacademy.io)

Link Local

- Communication between devices with a local link
- Typically used within subnets
- Are not routable
- The prefix is fe80::/10

```
fe80::1a2b:3c4d:5e6f:789a
```

Example of IPv6 Link-Local Address

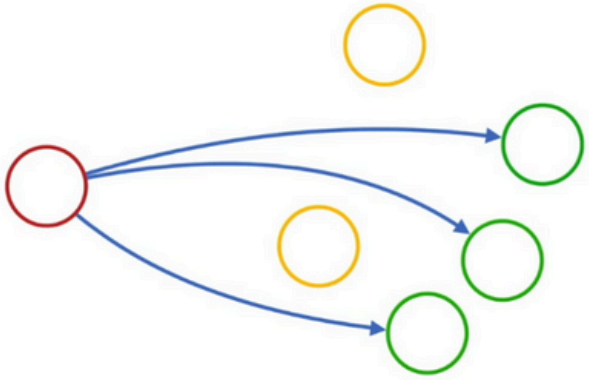
Loopback

- Address used for establishing internal communications within the device itself
- Loopback, as in IPv4

```
0000:0000:0000:0000:0000:0000:0000:0001/128
::1
```

Multicast

- Identify interfaces on the same or different host
- Sends packets to all interfaces belonging to the same multicast group
- Start with `ff`
  - `ff02::1` - All nodes on the local network segment
  - `ff02::2` - All routers on the local network segment
- Similar to IPv4 broadcast
- One-to-many communication



Anycast

- Addresses used to identify a group of devices offering a similar service
- Sending packets to one of the interfaces (usually the closest) associated with the address (not to all interfaces)
- One-to-nearest communication