CH-2 IP Protocol Set

TFTP:

Trivial File Transfer Protocol, is a simple **high**-level protocol for transferring data servers use to boot diskless workstations, X-terminals, and routers by using *User Data Protocol* (UDP).

IT is one of the most essential technologies for client/server and computer network infrastructures.

Although it may sound similar, TFTP works differently than *FTP* (File Transfer Protocol) and *HTTP* (Hyper Text Transfer Protocol). Although TFTP is also based in FTP technology, TFTP is an entirely different protocol. Among the differences is that TFTP’s transport protocol uses UDP which is not secure while FTP uses **Transmission Control Protoco**l (TCP) to secure information.

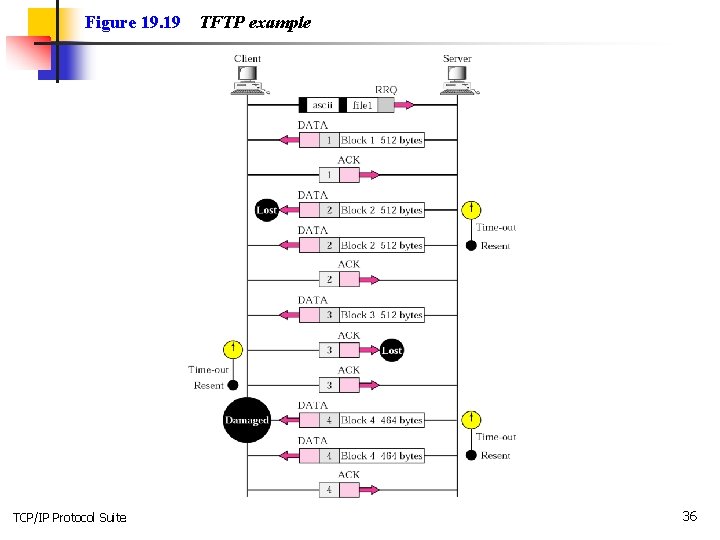
TFTP was primarily designed to read or write files by using a remote server. However, TFTP is a multi-purpose protocol that can be leveraged for an array of different tasks.

**TFTP Configuration Uses**

IT pros and Sys Admins typically use TFTP configuration for:

* Transferring files
* Remote-booting without hard drives
* Upgrading codes
* Backing up network configurations
* Backing up router configuration files
* Saving IOS images
* Booting PCs without a disk

After a workstation has been booted from a network card’s ROM, your TFTP installation will download a program and then run it from a central server.



**TFTP Protocol Transfer Modes**

There are three modes of transfer currently supported by TFTP protocol:

1. netascii
2. octet
3. mail

Additional modes can also be defined by pairs of cooperating hosts.

Using TFTP protocol, a transfer will start with a request to read or write a file while also requesting a connection. When a server grants this request, the connection is then opened up and the file is sent in fixed length blocks of 512 bytes.

**SNMP**:

Simple Network Management Protocol (*SNMP*) is a networking protocol used for the management and [monitoring of network-connected devices](https://www.thousandeyes.com/solutions/network-device-monitoring) in Internet Protocol networks. The SNMP protocol is embedded in multiple local devices such as routers, switches, servers, firewalls, and wireless access points accessible using their IP address.

Typically, the SNMP protocol is implemented using the User Datagram Protocol (UDP). UDP is a connectionless protocol that works like the Transmission Control Protocol (TCP) but assumes that error-checking and recovery services are not required. Instead, UDP continuously sends datagrams to the recipient whether they receive them or not.

There are three different versions of SNMP:

* **SNMP version 1 (SNMPv1)**—This was the first implementation, operating within the structure management information specification, and described in RFC 1157.
* **SNMP version 2 (SNMPv2)**—This version was improved to support more efficient error handling and is described in RFC 1901. It was first introduced as RFC 1441. It is often referred to as SNMPv2c.
* **SNMP version 3 (SNMPv3)**—This version improves security and privacy. It was introduced in RFC 3410.

SNMP version 2 is the most commonly deployed SNMP protocol version today. The most recent version, SNMP version 3, includes new security features that add support for authentication and encryption of SNMP messages as well as protecting packets during transit

Simple Network Management Protocol (SNMP) is an **application**–layer protocol defined by the Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices. It is a part of Transmission Control Protocol ⁄ Internet Protocol (TCP⁄IP) protocol suite.

SNMP is one of the widely accepted [network protocols](https://www.manageengine.com/network-monitoring/network-protocols.html) to manage and monitor network elements. Most of the professional–grade network elements come with bundled SNMP agent. These agents have to be enabled and configured to communicate with the [network monitoring tools](https://www.manageengine.com/network-monitoring/network-monitoring-tools.html) or network management system (NMS).

## SNMP tutorial

This tutorial is an effort to explain in brief about

* [What are the basic SNMP components and their functionalities?](https://www.manageengine.com/network-monitoring/what-is-snmp.html#snmp-functionalities)
* [SNMP basic commands](https://www.manageengine.com/network-monitoring/what-is-snmp.html#snmp-basic-commands)
* [How a typical SNMP communication happens?](https://www.manageengine.com/network-monitoring/what-is-snmp.html#typical-snmp-communication)
* [SNMP versions (SNMP v1, v2 and v3)](https://www.manageengine.com/network-monitoring/what-is-snmp.html#snmp-version)

## SNMP basic components and their functionalities

SNMP consists of

* [SNMP Manager](https://www.manageengine.com/network-monitoring/what-is-snmp.html#snmp-manager)
* [Managed devices](https://www.manageengine.com/network-monitoring/what-is-snmp.html#managed-devices)
* [SNMP agent](https://www.manageengine.com/network-monitoring/what-is-snmp.html#snmp-agent)
* [Management Information Database Otherwise called as Management Information Base (MIB)](https://www.manageengine.com/network-monitoring/what-is-snmp.html#mib)

### SNMP Manager:

A manager or management system is a separate entity that is responsible to communicate with the SNMP agent implemented network devices. This is typically a computer that is used to run one or more network management systems.

SNMP Manager’s key functions

* Queries agents
* Gets responses from agents
* Sets variables in agents
* Acknowledges asynchronous events from agents

**SNMP Agent:**

The agent is a program that is packaged within the network element. Enabling the agent allows it to collect the management information database from the device locally and makes it available to the SNMP manager, when it is queried for. These agents could be standard (e.g. Net-SNMP) or specific to a vendor (e.g. HP insight agent)

SNMP agent’s key functions

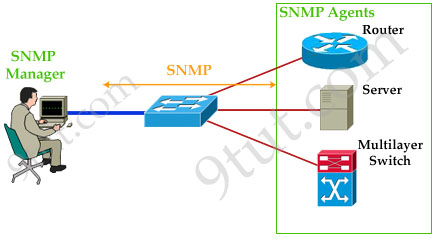
* Collects management information about its local environment
* Stores and retrieves management information as defined in the MIB.
* Signals an event to the manager.
* Acts as a proxy for some non–SNMP manageable network node.

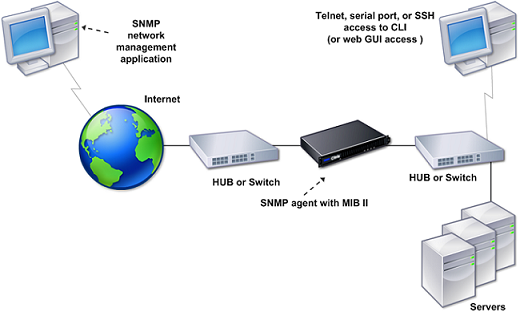
A mebibyte (MiB) is a unit of measurement used in computer data storage. The prefix mebi comes from the binary system of data measurement that is based on powers of two. A mebibyte equals 220 or 1,048,576 [bytes](https://searchstorage.techtarget.com/definition/byte).

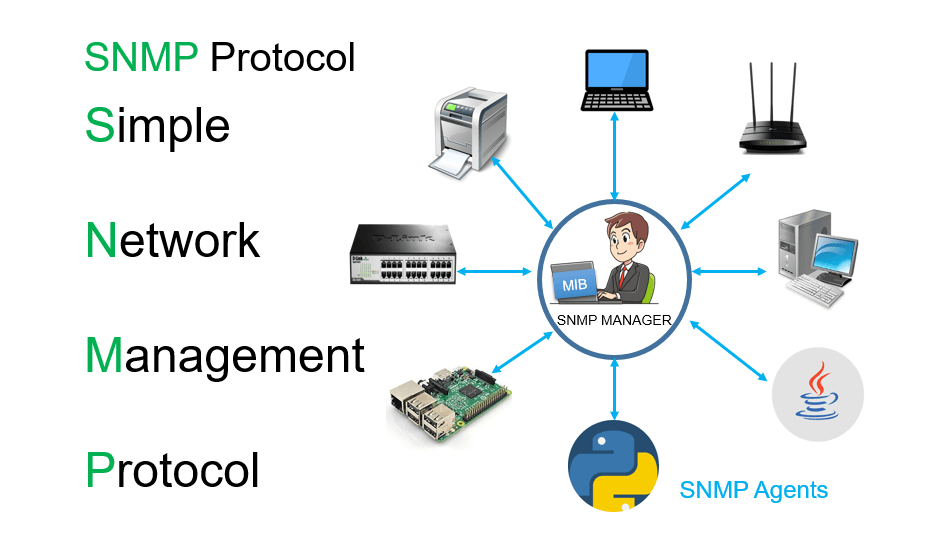


Simple Network Management Protocol (SNMP) is a networking protocol used for the management and [monitoring of network-connected devices](https://www.thousandeyes.com/solutions/network-device-monitoring) in Internet Protocol networks. The SNMP protocol is embedded in multiple local devices such as routers, switches, servers, firewalls, and wireless access points accessible using their IP address. SNMP provides a common mechanism for network devices to relay management information within single and multi-vendor LAN or WAN environments. It is an application layer protocol in the OSI model framework.

Typically, the SNMP protocol is implemented using the User Datagram Protocol (UDP). UDP is a connectionless protocol that works like the Transmission Control Protocol (TCP) but assumes that error-checking and recovery services are not required. Instead, UDP continuously sends datagrams to the recipient whether they receive them or not.







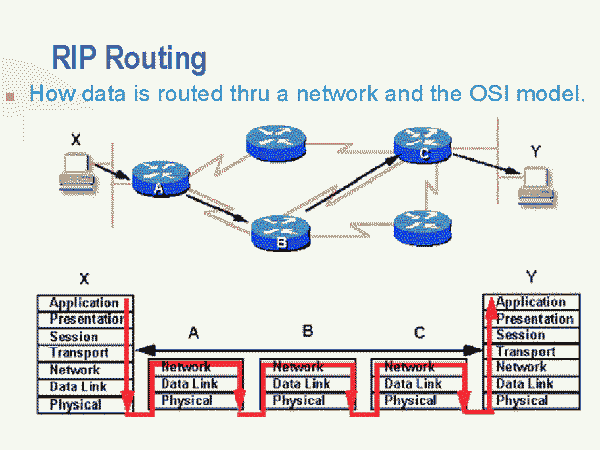
# Routing Information Protocol (RIP)

* Last Updated : 21 Oct, 2021

**Routing Information Protocol** (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance-vector routing protocol that has an AD (**Administrative Distance)** value of 120 and works on the application layer of the OSI model. RIP uses port number 520.

**Hop Count :**  
Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hops allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and a hop count of 16 is considered as network unreachable.

Attention reader! Don’t stop learning now. Get hold of all the important CS Theory concepts for SDE interviews with the [**CS Theory Course**](https://practice.geeksforgeeks.org/courses/SDE-theory?vC=1) at a student-friendly price and become industry ready.



**Features of RIP :**   
1. Updates of the network are exchanged periodically.   
2. Updates (routing information) are always broadcast.   
3. Full routing tables are sent in updates.   
4. Routers always trust routing information received from neighbor routers. This is also known as *Routing on rumours*.

**RIP versions :**  
There are three versions of routing information protocol – **RIP Version1**, **RIP Version2**, and **RIPng**.

| **RIP v1** | **RIP v2** | **RIPng** |
| --- | --- | --- |
| Sends update as broadcast | Sends update as multicast | Sends update as multicast |
| Broadcast at 255.255.255.255 | Multicast at 224.0.0.9 | Multicast at FF02::9 (RIPng can only run on IPv6 networks) |
| Doesn’t support authentication of update messages | Supports authentication of RIPv2 update messages | – |
| Classful routing protocol | Classless protocol updated supports Classful | Classless updates are sent |

**RIP v1** is known as ***Classful*** Routing Protocol because it doesn’t send information of subnet mask in its routing update.   
**RIP v2** is known as *Classless* Routing Protocol because it sends information of subnet mask in its routing update.

**OSPF**: Open Shortest Path First Protocol

(Open Shortest Path First) protocol is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) for the Internet, used to distribute IP routing information throughout a single Autonomous System (AS) in an IP network.

*An* ***Autonomous system*** *is a collection of connected Internet Protocol routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain,*

*An interior gateway protocol is a type of routing protocol used for exchanging routing table information between gateways within an autonomous system. This routing information can then be used to route network-layer protocols*

*Routing protocols that route between autonomous systems or routing domains are referred to as Exterior Gateway Protocols (EGPs). (exterior gateway protocol).*

The OSPF protocol is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbors. The topology information is flooded throughout the AS, so that every router within the AS has a complete picture of the topology of the AS. This picture is then used to calculate end-to-end paths through the AS, normally using a variant of the ***Dijkstra*** algorithm. Therefore, in a link-state routing protocol, the next hop address to which data is forwarded is determined by choosing the best end-to-end path to the eventual destination.

The main advantage of a link state routing protocol like OSPF is that the complete knowledge of topology allows routers to calculate routes that satisfy particular criteria. This can be useful for traffic engineering purposes, where routes can be constrained to meet particular quality of service requirements. The main disadvantage of a link state routing protocol is that it does not scale well as more routers are added to the routing domain. Increasing the number of routers increases the size and frequency of the topology updates, and also the length of time it takes to calculate end-to-end routes. This lack of scalability means that a link state routing protocol is unsuitable for routing across the Internet at large, which is the reason why IGPs only route traffic within a single AS.

Each OSPF router distributes information about its local state (usable interfaces and reachable neighbors, and the cost of using each interface) to other routers using a Link State Advertisement (LSA) message. Each router uses the received messages to build up an identical database that describes the topology of the AS.

From this database, each router calculates its own routing table using a Shortest Path First (SPF) or Dijkstra algorithm. This routing table contains all the destinations the routing protocol knows about, associated with a next hop IP address and outgoing interface.

The formula to calculate the **cost** is Reference Bandwidth divided by interface bandwidth. For example, in the case of *10 Mbps Ethernet* (10Base2), OSPF Metric Cost value is 100 Mbps / 10 Mbps = 10.

This protocol uses the IP 224.0.0.5 for link state LSA. Then constructing **LSDB** link state **Data Base.**

For RIP it is recommended to use 15 routers not more. But in OSPF it is not recommended to use more than **50** routers.

The **cost** is equal to metric, but in RIP the metric = the no. of hops in the network, when in OSPF the following law is used metric= 108/ BW.

**Cost = Reference bandwidth / Interface bandwidth in bps.**

**So, Cost = 108 /interface bandwidth in bps**

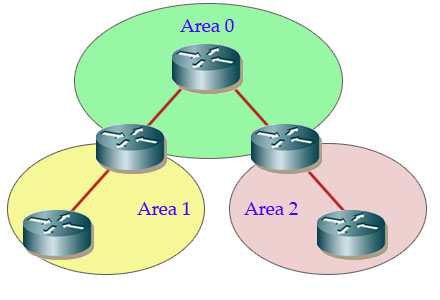
OSPF has 2 conditions to make the routing effective

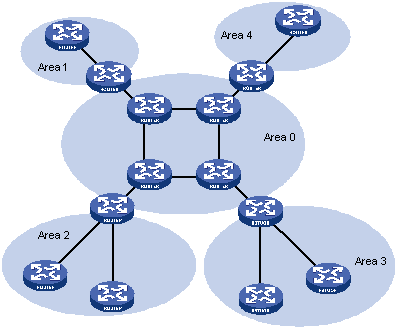
A- The overall network should be configured as areas, Area 0 (area0) must be the backbone.

B- All other areas must be connected to the area 0.

In any network if more than on routing protocol is used, the router will choose the less metric routing protocol to route the packets.

* The protocol recalculates routes when network topology changes, using the Dijkstra algorithm, and minimizes the routing protocol traffic that it generates.
* It provides support for multiple paths of equal cost.
* It provides a multi-level hierarchy (two-level for OSPF) called "area routing," so that information about the topology within a defined area of the AS is hidden from routers outside this area. This enables an additional level of routing protection and a reduction in routing protocol traffic.
* All protocol exchanges can be authenticated so that only trusted routers can join in the routing exchanges for the **AS**.





#### **OSPF Version 3 (OSPFv3)**

OSPF version 2 (OSPFv2) is used with IPv4. OSPFv3 has been updated for compatibility with IPv6's 128-bit address space. However, this is not the only difference between OSPFv2 and OSPFv3. Other changes in OSPFv3, as defined in RFC 2740, include

* protocol processing per-link not per-subnet
* addition of flooding scope, which may be link-local, area or AS-wide
* removal of opaque (unrecognized) LSAs
* support for multiple instances of OSPF per link
* Various packet and LSA format changes (including removal of addressing semantics).

Both OSPFv2 and OSPFv3 are fully supported by DC-OSPF.

* Interior Gateway Routing Protocol (IGRP):

IGRP does not actually use hops as a metric, although it does track hops and allows routes to be propagated up to 255 hops away. It was meant to be an enhancement on RIP which was limited to 16 hop networks. It was later modified and was adopted by the OSI to operate in ***CLNP*** (**connectionless Network protocol**) networks, so IGRP is not limited to IP networks.

IGRP uses IP directly, using protocol number 9; RIP uses UDP port 520. IGRP uses Autonomous System numbers to distinguish between routing domains.

IGRP sends updates every 90 seconds and uses a number of factors to determine the metric. Bandwidth is one factor used in determining this metric and this can be adjusted to fool the router if so desired.

Whereas RIP uses the metric of hops, IGRP uses the following metrics:

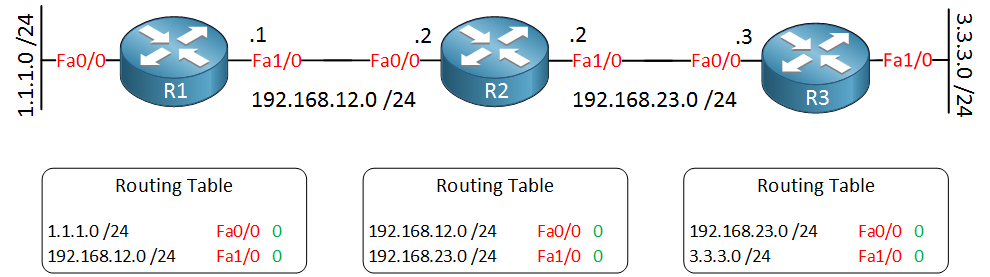
Internetwork **Delay** - this represents the delay on the medium in units of 10 microseconds e.g. for Ethernet this value is 100 microseconds i.e. 10ms, so the value of Delay is 100/10 = 10.

Bandwidth (BW) - this represents the speed of the link where the speed can range from 1200bps to 10Gbps. The value used is actually the inverse of the Bandwidth (in Kb/s) multiplied by 107 e.g. for a 64Kb/s link the value of BW is 107/64 = 156250.

Reliability - fractions of 255 where 255 means totally reliable.

Administrative Distance - can take a value between 1 and 255 and creates a load or weighting on that particular link, the higher the number the less attractive the link is.

The default metric is BW + Delay. You can change the weights if you want to. However note that these weights must be the same on all the routers!.



IGRP will only send routing updates to routers that are within the same Autonomous System. There are three types of routes:

Interior Routes - if there are subnets then these are advertised. These routes are subnets that are locally connected.

System Routes - routes to summarized networks within an AS.

Exterior Routes - routes to networks outside the AS and are called default networks.

RIP and OSPF advertise default networks as 0.0.0.0. IGRP and EIGRP can advertise more specific networks as default networks, and have a number of them. The default network is configured within the IGRP routing process with the command ip default-network.

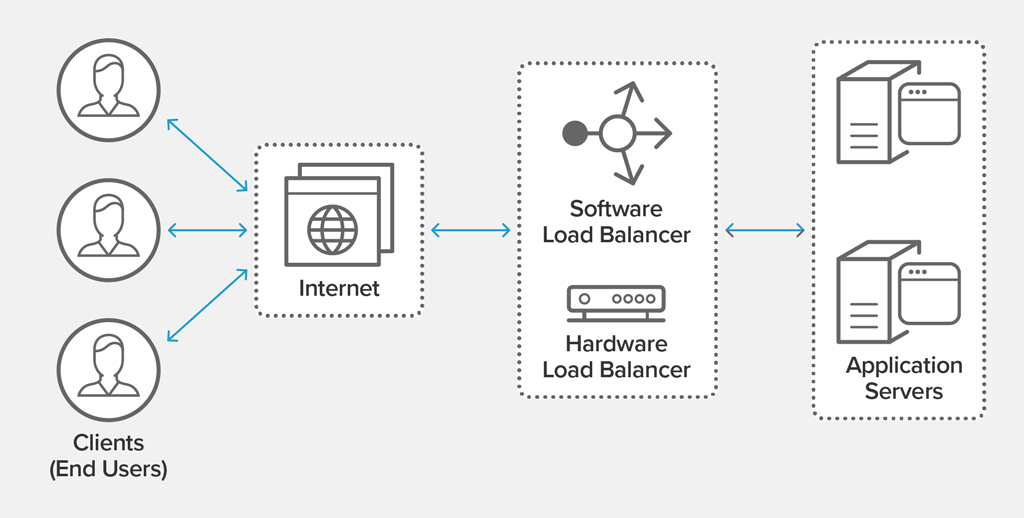
The default Update Timer is 90 seconds, the Invalid Timer is three times the update timer, 270 seconds. The Holddown Timer is the Invalid Timer plus 10 seconds and the Flush Timer is seven times the Update Timer i.e. 630 seconds. 20% jitter is added to the update timer to prevent waves of updates flooding a network where Jitter is the variation in the time between data packets arriving, caused by network congestion, or route changes. The longer data packets take to transmit, the more jitter affects audio quality. The standard jitter measurement is in milliseconds (ms). If receiving jitter is higher than 15-20ms, it can increase latency and result in packet loss, causing audio quality degradation.

**Load balancing** refers to efficiently distributing incoming network traffic across a group of backend servers, also known as a *server farm* or *server pool*.

Modern high‑traffic websites must serve hundreds of thousands, if not millions, of concurrent requests from users or clients and return the correct text, images, video, or application data, all in a fast and reliable manner. To cost‑effectively scale to meet these high volumes, modern computing best practice generally requires adding more servers.

A [load balancer](https://www.nginx.com/solutions/adc) acts as the “traffic cop” sitting in front of your servers and routing client requests across all servers capable of fulfilling those requests in a manner that maximizes speed and capacity utilization and ensures that no one server is overworked, which could degrade performance. If a single server goes down, the load balancer redirects traffic to the remaining online servers. When a new server is added to the server group, the load balancer automatically starts to send requests to it. In this manner, a load balancer performs the following functions:

1. Distributes client requests or network load efficiently across multiple servers
2. Ensures high availability and reliability by sending requests only to servers that are online
3. Provides the flexibility to add or subtract servers as demand dictates.



load balancing diagram

Interior Gateway Routing Protocol (IGRP) uses bandwidth, delay, reliability, load, to find the *metric value*. By default, the algorithm uses only bandwidth and delay, but the other metric components can be enabled.

The following formula is used to calculate the composite metric of IGRP.

Metric = [K1 \* Bandwidth + (K2 \* Bandwidth) / (256-Load) + K3\*Delay] \* [K5/(Reliability + K4)]

The default constant values are K1 = K3 = 1 and K2 = K4 = K5 = 0.

If K5 = 0, the [K5/ (reliability + K4)] term is not used. So, given the default values for K1 through K5, the composite metric calculation used by IGRP reduces to Metric = Bandwidth + Delay.

• To find the bandwidth value, find the smallest of all the bandwidths in Kbps from outgoing interfaces and divide 10,000,000 by that number.

• Reliability and load are measured 1–255. A reliability of 1 is least reliable, while 255 is most reliable. A load of 1 is least utilized, while 255 is 100 percent utilized. The MTU maximum transfer unit refers to the size of the frame. If a route has lower metric value, then that route is preferred.

• In order to find the delay, add all of the delays (in microseconds) from the outgoing interfaces and divide this number by 10. (The delay is in tenths of microseconds.)

**SSL**:

Secure Sockets Layer (SSL) was the most widely deployed cryptographic protocol to provide security over internet communications before it was [succeeded by TLS](https://www.globalsign.com/en/blog/ssl-vs-tls-difference/) (Transport Layer Security) in 1999. Despite the deprecation of the SSL protocol and the adoption of TLS in its place, most people still refer to this type of technology as ‘SSL’.

SSL provides a secure channel between two machines or devices operating over the internet or an internal network. One common example is when SSL is used to secure communication between a web browser and a web server. This turns a website's address from HTTP to HTTPS, the ‘S’ standing for ‘secure’.

## Why Do I Need SSL?

With so much of our day to day transactions and communications happening online, there is very little reason for not using SSL. SSL supports the following information security principles:

* **Encryption**: protect data transmissions (e.g. browser to server, server to server, application to server, etc.)
* **Authentication**: ensure the server you’re connected to is actually the correct server
* **Data integrity**: ensure that the data that is requested or submitted is what is actually delivered.



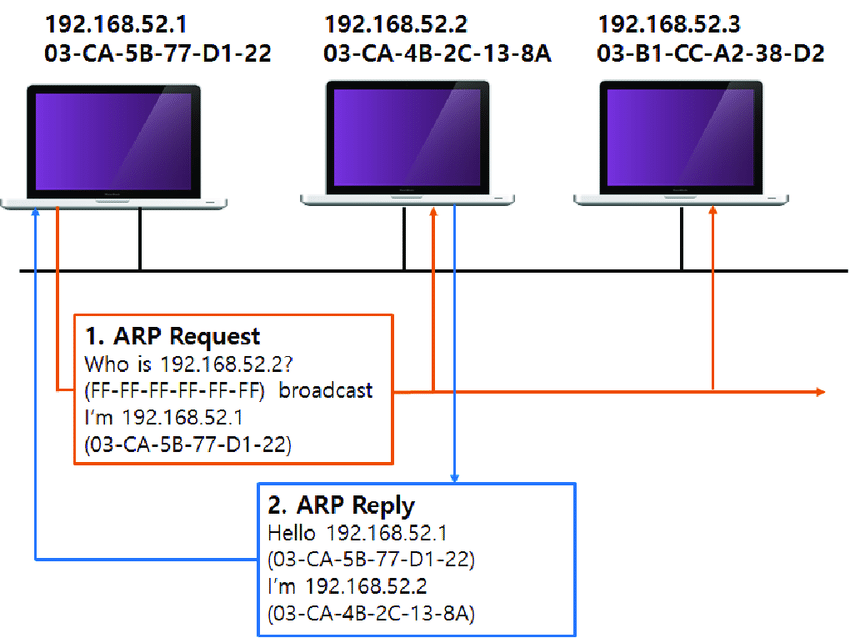
SSL can be used to secure:

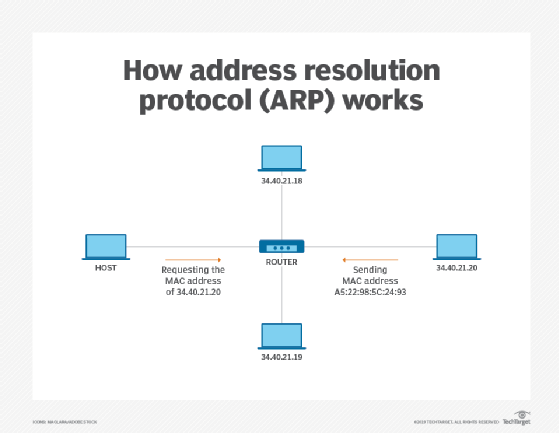
* Online credit card transactions or other online payments.
* Intranet-based traffic, such as internal networks, file sharing, extranets and database connections.
* Webmail servers like Outlook Web Access, Exchange and Office Communications Server.
* The connection between an email client such as Microsoft Outlook and an email server such as Microsoft Exchange.
* The transfer of files over HTTPS and FTP(s) services, such as website owners updating new pages to their websites or transferring large files.
* System logins to applications and control panels like Parallels, cPanel and others.
* Workflow and virtualization applications like Citrix Delivery Platforms or cloud-based computing platforms.
* Hosting control panel logins and activity like Parallels, cPanel and others.

**ARP**

The [Address Resolution Protocol(ARP)](https://en.wikipedia.org/wiki/Address_Resolution_Protocol) is a communication protocol used to discover the data-link layer address(Layer 2 address like Media Access Control(MAC) address) associated with an Internet layer address(Layer 3 address like IPv4 address). ARP was defined in 1982 by [RFC 826](https://tools.ietf.org/html/rfc826).

ARP is a request-response or request-reply protocol in which one device sends a request to another device asking for some information, to which the other device will reply with the required information. It is a message exchange pattern. ARP packets are encapsulated by link layer and are distributed only in a particular network. As a result, ARP is said to be a link layer protocol.





### Why do we need ARP?

Devices in a Local Area Network(LAN) are programmed to communicate using link layer addresses. Switches are not configured for a standard that will allow destination decisions to be based on IP within the same broadcast domain. A device that is not connected to the internet will not have an IP address. In that case, the network has to resort to using MAC addresses for communication. If a device wants to communicate with another device in the same LAN, it needs to know the MAC address of the other device’s network interface. This allows for the communication between the two end devices to be unicast.

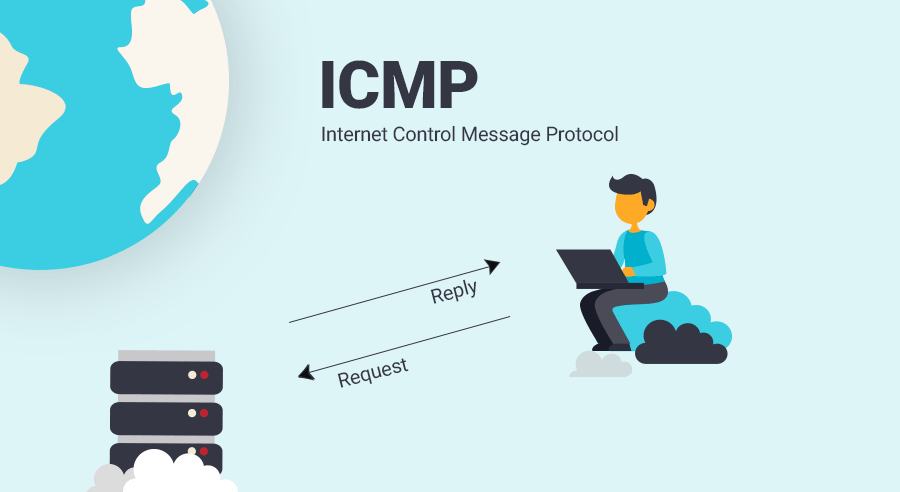
**ICMP**

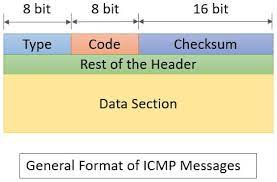
The Internet Control Message Protocol (ICMP) is a [network layer](https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/) protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. Commonly, the ICMP [protocol](https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/) is used on network devices, such as routers. ICMP is crucial for error reporting and testing, but it can also be used in [distributed denial-of-service (DDoS) attacks](https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/).

## How is ICMP used in DDoS attacks?

**ICMP flood attack**

A ping flood or ICMP flood is when the attacker attempts to overwhelm a targeted device with ICMP echo-request packets. The target has to process and respond to each packet, consuming its computing resources until legitimate users cannot receive service.





ICMP flood attack:

Reverse Address Resolution Protocol (RARP) is a network-specific standard protocol. It is described in RFC 903. Some network hosts, such as a diskless workstation, do not know their own IP address when they are booted. To determine their own IP address, they use a mechanism

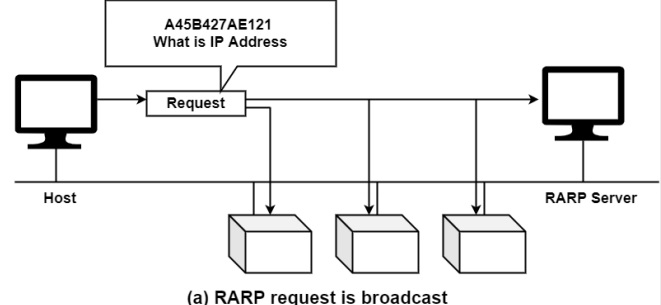
similar to ARP, but now the hardware address of the host is the known parameter, and the IP address is the queried parameter.

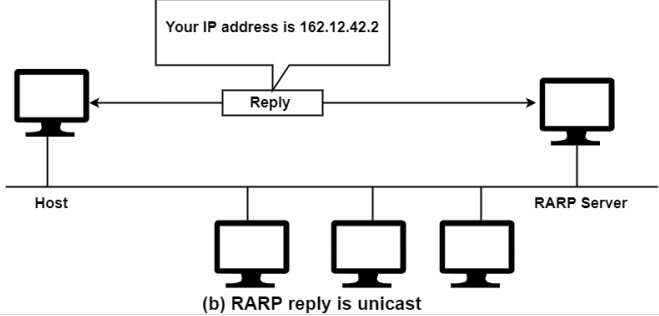
The reverse address resolution is performed the same way as the ARP address resolution. The same packet format is used for the ARP.

An exception is the operation code field that now takes the following values−

* 3 for RARP request
* 4 for RARP reply

The physical header of the frame will now indicate RARP as the higher-level protocol (8035 hex) instead of ARP (0806 hex) or IP-(0800 hex) in the Ether type field.





When a framework with a local disk is bootstrapped, it generally accepts its IP address from a configuration document that's read from a disk file. But a system without a disk, including an X terminal or a diskless workstation, needs some other way to accept its IP address.

The feature of RARP is for the diskless framework to read its specific hardware address from the interface card and send a RARP request asking for someone to reply with the diskless systems IP address.

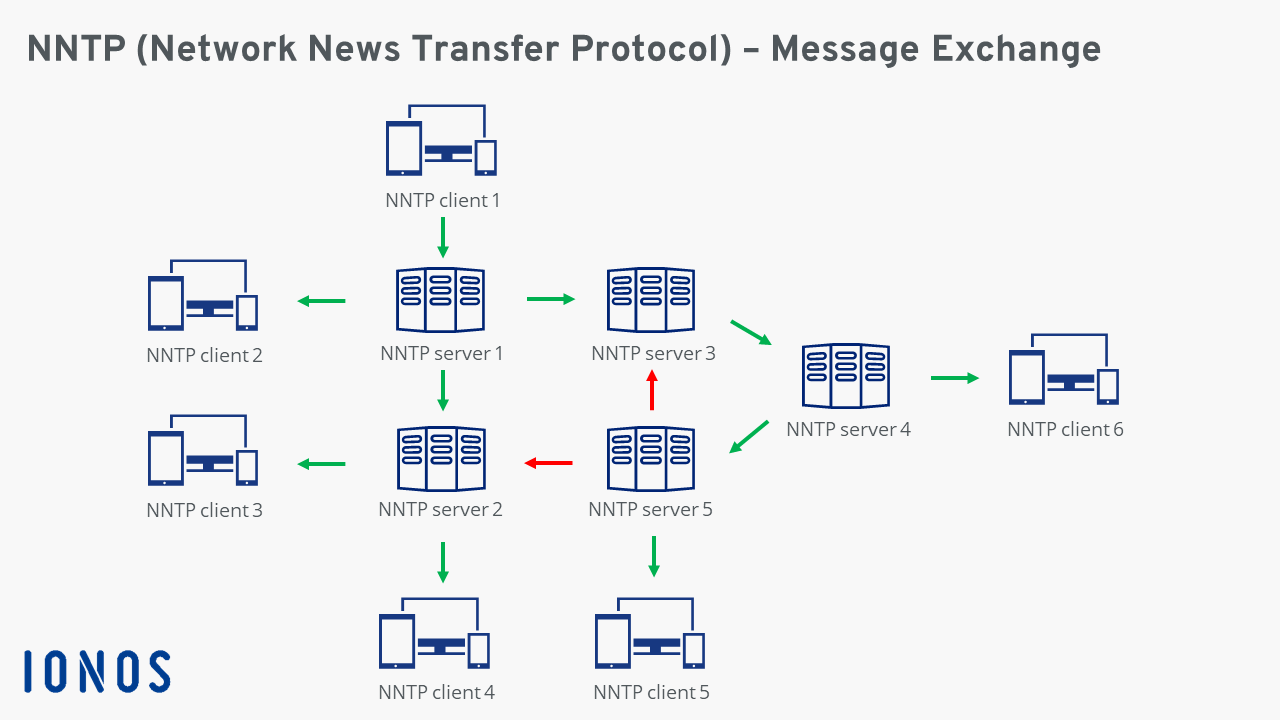
**8083**

TCP port **8083** uses the Transmission Control Protocol. TCP is one of the main protocols in TCP/IP networks. TCP is a connection-oriented protocol, it requires handshaking to set up end-to-end communications. Only when a connection is set up user's data can be sent bi-directionally over the connection.   
Attention! TCP guarantees delivery of data packets on port **8083** in the same order in which they were sent. Guaranteed communication over TCP port **8083** is the main difference between TCP and UDP. UDP port **8083** would not have guaranteed communication as TCP.

UDP on port **8083** provides an unreliable service and datagrams may arrive duplicated, out of order, or missing without notice. UDP on port **8083** thinks that error checking and correction is not necessary or performed in the application, avoiding the overhead of such processing at the network interface level.   
UDP (User Datagram Protocol) is a minimal message-oriented Transport Layer protocol (protocol is documented in IETF RFC 768).   
Application examples that often use UDP: voice over IP (VoIP), streaming media and real-time multiplayer games. Many web applications use UDP, e.g. the Domain Name System (DNS), the Routing Information Protocol (RIP), the Dynamic Host Configuration Protocol (DHCP), the Simple Network Management Protocol (SNMP).   
TCP vs UDP - TCP: reliable, ordered, heavyweight, streaming; UDP - unreliable, not ordered, lightweight, datagrams.

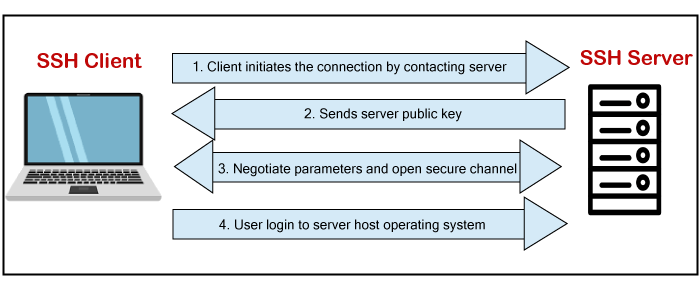
NNTP

**Network News Transfer Protocol (NNTP)** is the underlying protocol of UseNet, which is a worldwide discussion system which contains posts or articles which are known as news. Network News Transfer Protocol is used to transfer news from one network to another. It is designed specifically to transfer news/articles. A NNTP client is included in browsers like Netscape, Opera and Internet Explorer or a special application named newsreader can be used as a NNTP client. NNTP servers manages the global network of news groups.



SSH

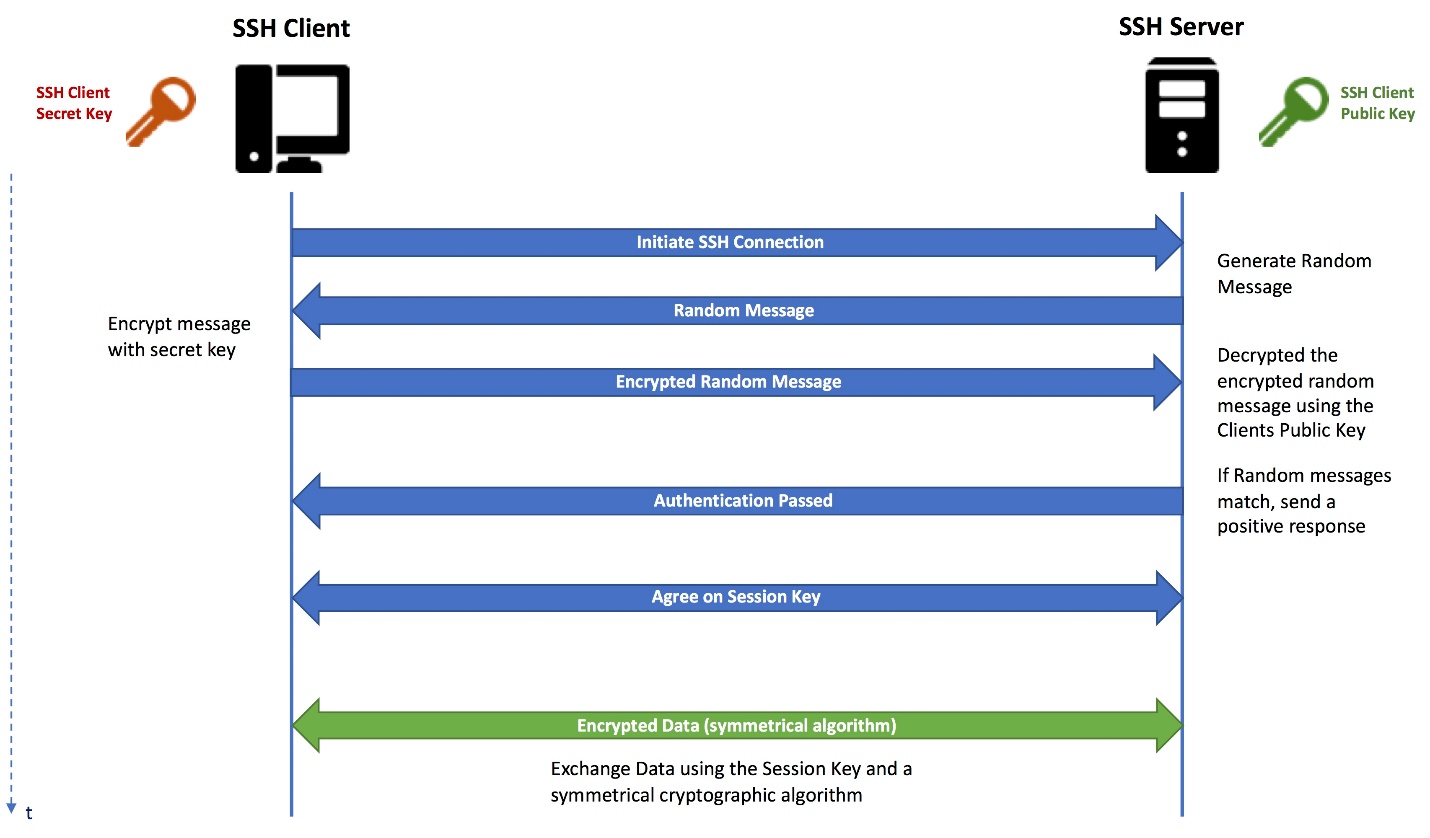
Secure shell (SSH), also called secure socket shell, is a networking protocol for securely and remotely accessing computers, routers, servers, and other devices over an unsecured network.





SSH provides password or public-key based authentication and encrypts connections between two network endpoints. It is a secure alternative to legacy login protocols (such as telnet, rlogin) and insecure file transfer methods (such as FTP).

In addition to providing strong encryption, SSH is widely used by network administrators to manage systems and applications remotely, deliver software patches, or execute commands and move files.



SSH use cases include:

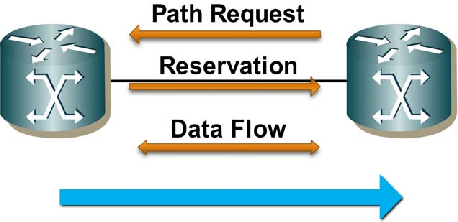
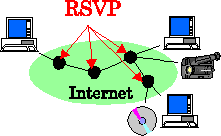
* Interactive use
* File transfers
* Point-to-point tunneling

# RSVP (Resource Reservation Protocol)?

RSVP is a transport layer protocol that is used to reserve resources in a computer network to get different quality of services (QoS) while accessing Internet applications. It operates over Internet protocol (IP) and initiates resource reservations from the receiver’s end.

## Features

* RSVP is a receiver oriented signalling protocol. The receiver initiates and maintains resource reservation.
* It is used both for unicasting (sending data from one source to one destination) and multicasting (sending data simultaneously to a group of destination computers).
* RSVP supports dynamic automatic adaptation to changes in network.
* It provides a number of reservation styles. It also provides support for addition of future styles.



## RSVP Messages

There are two types of RSVP messages −

* **Path Messages (path):** A path message is sent by the sender to all receivers by multicasting storing the path state at each node in its path. It stores the necessary information so that the receivers can make the reservation.
* **Reservation messages (resv):**The resv message is sent by the receiver to the sender along the reverse path of the path message. It identifies the resources that is requires by the data flow.