# MINT709 CAPSTONE Project Report

# Performance comparisons of Internetwork Protocols

Prepared by: Haroun Yussuf Prepared for Dr. M.H. Macgregor

August 2011

# **Brief Introduction**

## Introduction

In the simplest of terms, network performance management is considered the second function of network management; the first being fault management. Managing the performance of anything implies the existence of a set of base criteria which represent the optimal way of operation that will be compared to the current operational attributes of the system in question. These are referred to as the performance metrics of the system.

The performance metrics of Internetworking protocols depend on the layer at which the subject protocol operates. In this study, the goal was to select a small number of these protocols – a few from each layer – as the subjects. Although the subtitles which have been used to group the protocols may not accurately classify the protocols under each section, the idea was and still remains to relate them in functionality. The data and resources for the study have been collected from secondary sources including papers written on the subject and observations from the traces of lab runs based on the lab setup shown in the network diagram below.



The importance of network performance measurement can never be emphasized enough; and is a subject area that hardware manufacturers and network administrators should give the attention it deserves. The process of network performance measurement, as any other performance measurement exercise, starts with capturing data that would be analyzed later to identify trends. There are many tools that facilitate this; and the tool of choice for this study was Wire shark (previously Ethereal) which provides an easy way to capture traffic on network interfaces and visualize it, while having the flexibility to dig deeper into the frame content and details at each layer of the Internetworking stack.

A study on network performance metrics and their composition by DANTE presented at TERENA (a regional research and education network) networking conference in 2006 discusses a Network Metric Composition Framework in which the performance metrics have been categorized into Layer 3 metrics and additional metrics. The first included the usual delay, loss, bandwidth and availability metrics; while the second included device specific data, netflow data and most importantly routing. The approach taken to this CAPSTONE project study takes a slightly different approach, and is based on the premise and assumption that because of the layered architecture of the network protocols imposed by the OSI and TCP/IP models, the protocols and technologies operating at each of the layers impact the overall performance of the networking system. As a result, the study looks at a sample of the protocols at each of these

layers and how they interact while eventually making the communication happen.

The goal behind performance measurement and specifying the metrics used in doing so is to outline traffic trends, identify anomalies and tune the performance by eliminating all bottlenecks. The report looks into the following protocols, tools and technologies to achieve this:

- Ping, traceroute, ICMP and DHCP
- TCP and UDP
- HTTP, SSH, Telnet and FTP
- ARP and RARP
- Unicast, Multicast and Ethernet
- RIP, OSPF, IS-IS, and BGP

The approach taken in each section is to provide an overview of the protocol in question discussing its functionality, issues and network performance metrics which vary depending on the protocol's functionality and role in the communication process. Next, the traces captured in the test runs are presented and commented on; and finally the whole exercise is summarized.

## **Network Protocols**

This section comprises of Ping and Traceroute - which both depend on the Internet Control Message Protocol, and the Dynamic Host Configuration Protocol (DHCP) whose performance characteristics and issues will be studied.

The analysis work is based on the configuration presented in the introduction of this report – the same lab configuration which will be used for the rest of this study. The real world performance factors belong to either one of three categories; the normal network overheard which accounts for 20 percent of the traffic under most circumstances, the external performance limiters such as the processing capabilities and memory capacity of the nodes, and finally – and most importantly – the network configuration problems which is the part we have more control over. The first two factors are mainly a matter of budget and availability of the suitable resources. The network configurations may include poor design issues and device misconfigurations.

Tools such as Ping and Traceroute have historically been used to pinpoint and troubleshoot network problems. There are various implementations of both tools by different vendors and it is not our goal to compare them; however, the goal is to look into their utility as performance measuring tools; and also look into the performance issues these tools themselves might create.

#### **Overview of Ping and Traceroute**

Ping is the most commonly used network diagnostics tool and performance evaluation in TCP/IP networks. It can be very useful in identifying network protocol problems that inhibit smooth communication between nodes, and the measure packet delay which is a great performance metric and indicator of faults in the network.

For security issues mostly involving target reconnaissance and more dangerously Denial of Service Attacks (especially DDoS), many of the ISPs filtered out the ICMP echo packets (message type 8) which is the foundation of Ping and Traceroute, rendering them less effective since 2003.

	ICMP pa	acket					
	Bit 0 - 7	Bit 8 - 15	Bit 16 - 31				
	Version/IHL	Type of service	Length				
	Identifica	flags and offset					
IP Header (20 bytes)	Time To Live (TTL)	Protocol	Checksum				
(20 bytes)	Source IP address						
	Destination IP address						
	Type of message	Code	Checksum				
ICMP Payload (8+ bytes)	Quench						
(0. 59003)	Data (optional)						

Figure 1 ICMP Packet

Ping works by sending an echo request message to the destination node; the destination node returns an echo reply. The packet loss is recorded, and the time between the transmission and reception of the ICMP packets is measured to be presented as the Round-Trip Time. The uses of the ping tool include:

- Testing the availability and reach-ability of a node
- Delay and round-trip times of packets

- Packet losses and high input queues drops by comparing the input queue drops and the actual output drops 0000

The 'debug ip packet' feature of Cisco routers helps provide even more detailed information about the ping results. It will give the details of the nature of the unreachable message returned by ICMP, for example.

Traceroute, like ping, has different implementations depending on the platform and operating system; this is exemplified by the variations in the command name where it is tracert in windows and traceroute in Unix and Unix-like operating systems.

Traceroute sends 3 UDP datagrams with their Time-to-live (TTL) field set to one; when it reaches its destination, it responds with an ICMP Time Exceeded Message (TEM) - which is message type 11 - indicating the expiration of the packet. The process continues in a recursive manner until the final destination is reached. The purpose is to give a trace of the path the packet took to reach that final destination.

#### **Issues with Ping and Traceroute in Performance Measuring**

The Round-Trip-Time actually only gives a rough idea of the delay in the network link as it considers the general picture of the time required to send an echo packet and get an answer. The problem is that this metric is not precise enough for performance evaluation; and the reason is that the node (a PC or a router) caries out some process-switching which most of the time considers the ping packet to have less priority. If the router, for example, is busy processing other tasks (process-oriented services), it will take longer to receive the ICMP echo reply.

Traffic Generation and Capture Process *Pinging across the internetwork (global)* 



**Figure 2 Test network** 

A node (laptop) attached to SW3 with IP address 192.168.3.3 attempts to ping another device connected to SW2 with IP address 192.168.1.2 in this scenario. This provides an example of pinging through the routers to ensure that the delay and related round-trip-time metric are not more than approximations since the intermediary routing devices will not consider the ping

traffic as being of less priority. Below is the detail of the captured packets:

86 17, 441660 192, 168, 3, 3	192.168.3.255	NBNS	Name query NB ISATAP<00>
87 17.596952 192.168.3.3	192.168.1.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=48/12288, ttl=128)
88 17.637471 192.168.1.2	192.168.3.3	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=48/12288, ttl=61)
89 18.205310 192.168.3.3	192.168.3.255	NBN5	Name query NB ISATAP<00>
90 18, 595256 192, 168, 3, 3	192.168.1.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=49/12544, ttl=128)
91 18.635740 192.168.1.2	192.168.3.3	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=49/12544, ttl=61)
92 18.674203 192.168.3.3	208.84.198.145	UDP	Source port: 37539 Destination port: 42784

## Detailed ICMP message

🛢 Frame 87: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)	
Arrival time: Jul 5, 2010 01:28:22.398339000 E. Africa standard time	
Epoch Time: 1278282502.398339000 seconds	
[Time delta from previous captured frame: 0.155292000 seconds]	
[Time delta from previous displayed frame: 0.155292000 seconds]	
[Time since reference or first frame: 17.596952000 seconds]	
Frame Number: 87	
Frame Length: 74 bytes (592 bits)	
Capture Length: 74 bytes (592 bits)	
[Frame is marked: False]	
[Frame is ignored: False]	
[Protocols in frame: eth:1p:icmp:data]	
[Coloring Rule Name: ICMP]	
[Coloring Rule String: icmp    icmpv6]	
Ethernet II, src: compalco_b3:c4:ab (00:16:d4:b3:c4:ab), Dst: cisco_bf:83:20 (00:08:21:bf:83:20)	
E Destination: Cisco_bf:83:20 (00:08:21:bf:83:20)	
Source: CompalCo_b3:c4:ab (00:16:d4:b3:c4:ab)	
Type: IP (0x0800)	
□ Internet Protocol, Src: 192.168.3.3 (192.168.3.3), Dst: 192.168.1.2 (192.168.1.2)	
version: 4	
Header Tength: 20 bytes	
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)	
Total Length: 60	
Identification: 0x0527 (1319)	
E Flags: 0x00	
Fragment offset: 0	
Time to live: 128	
Protocol: ICMP (1)	
⊕ Header checksum: 0xb044 [correct]	
Source: 192.168.3.3 (192.168.3.3)	
pestination: 192.168.1.2 (192.168.1.2)	
Internet Control Message Protocol	
Type: 8 (Echo (ping) request) code: 0	
cbde: 0 Checksum: 0x4d2b [correct]	
checksum; 0x4020 [COFFEC] Identifier: 0x0001	
identifier: 0x0001 Sequence number: 48 (0x0030)	
sequence number (LE): 12288 (0x300)	
B Data (32 bytes)	
E VALA (JE Vytes)	

Traceroute Scenario

C:\Users\haroun>tracert 192.168.1.2 Tracing route to TEAM4 [192.168.1.2] over a maximum of 30 hops: 1 192.168.3.1 1 ms 1 ms 1 ms 2 25 ms 25 ms 10.0.0.5 25 ms 3 49 ms 49 ms 10.0.0.1 49 ms TEAM4 [192.168.1.2] 4 59 ms 59 ms 59 ms

Trace complete.

As seen in the sample outputs for the ping program, the round-trip response time values for each ping packet sent are shown in the ping packet statistics:

64 bytes from 192.168.1.100: icmp\_seq=0 ttl=255 time=0.712 ms

The response time is shown in milliseconds. For internal LAN connections, the response times should be well within 1 or 2 milliseconds. For WAN connections, the response times can often be over 200 or 300 milliseconds, depending on WAN connectivity speeds. For VSAT connections it is approximately 1000 - 1400 ms round trip time according to Wikipedia entry on Satellite Internet access.

The tracert command is executed from router C, the interface with IP address 192.168.3.1, and the results of its execution is shown above. The captured packet trace is shown below:

		the second second second second second second second	subpress to the second		where the second s
11	47 23.709160	192.168.1.3	192.168.1.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=36/9216, ttl=1)
	48 23.709523	192.168.1.2	197.168.1.3	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=36/9216, ttl=64)
	49 23.710641	192.168.1.3	192.168.1.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=37/9472, ttl=1)
	50 23.710832	192.168.1.2	192.168.1.3	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=37/9472, ttl=64)
	51 23.711752	192.168.1.3	192.168.1.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=38/9728, ttl=1)
	52 23.711952	192.168.1.2	192.168.1.3	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=38/9728, ttl=64)
	Law of The set Law is the ballet of	A 49 10 10 10 10 10 10	The second second second second second	The state of the	residual company at a size and de adde and

#### **Performance Analysis**

In a Cisco network, as in any other networks based on other vendor's products, performance of the network is limited by the medium itself. In addition to the standard overheard that comes with TCP/IP protocols, turning on diagnostic and debugging tools will have a significant performance reduction on the network.

To ensure the accuracy of measuring performance attributes of a network, especially delay and throughput, either of two things are required:

- If the diagnostics are being done on a node that is not an intermediary router, to make sure that the same node is not involved in any process-intensive tasks. The suggestion here is to execute ping and traceroute from a standard computer

- If these commands are being executed on a router, most process intensive tasks need to be turned off, including debug and related diagnostic commands.

Some resources also suggest that Access-Control Lists may be used to control and filter the traffic that needs to be debugged if it is necessary to keep the debug commands on. Buffering debug messages to be viewed later using 'show log' command is also another option.

#### **Dynamic Host Configuration Protocol**

#### Protocol Overview

Dynamic Host Configuration Protocol (DHCP) is a client-server architecture protocol for automatically providing configuration parameters such as IP addresses, default gateways and subnet mask information to hosts on a network.

DHCP supports three mechanisms for IP address allocation. In automatic allocation, DHCP assigns a permanent IP address to a client. In dynamic allocation, DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address). In manual allocation, a client's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the client. A particular network will use one or more of these mechanisms, depending on the policies of the network administrator.



By using DHCP, dynamically configuring the host to the network is done by a simple handshake. In history, there are also many dynamic automatic configuration protocols. Other protocols that can also provide the mechanism of automatic configuration include RARP and BOOTP. These protocols use simple interaction; the client requests and the server replies. RARP (Reverse Address Resolution Protocol) is executed on Ethernet, and converts the Ethernet address to an IP address. RARP handshake is mainly used in the diskless workstations. RARP uses an Ethernet frame directly, meanwhile BOOTP uses UDP. BOOTP returns IP addresses with the subnet mask of a network, IP addresses of routers, etc. RARP and BOOTP have two defects. First, these protocols only support static allocation (conversion) of an IP address. RARP and BOOTP protocol do not solve the requirement of dynamic allocation. Secondly, these protocols can provide only few parameters.

### **Traffic Generation and Capture Process**

Using the same lab configuration as above, the following packets have been captured during the automatic IP assignment process that started once a laptop was connected to the network. The first step is to locate a DHCP server through broadcast to the segment.

133 31.207257 0.0.0.0 255.255.255.255 DHCP DHCP Discover - Transaction ID 0x438b960b

Following the transaction ID, it was possible to follow the rest of the process, as shown below.

140 33.030001	LEGALITOCOTOE/OTADE	11021110	TCWMAA	MUTLICASE L	. ISLER	ner	Keport N	1622	age va		
147 33.206440	192.168.1.1	255.255.255.255	DHCP	DHCP offer	-	TF	ansaction	I ID	0x438b960b		
148 33.207691	0.0.0.0	255.255.255.255	DHCP	DHCP Reques	it -	Tra	ansaction	I ID	0x438b960b		
149 33.210643	192.168.1.1	255.255.255.255	DHCP	DHCP ACK	-	Tra	ansaction	ID	0x438b960b		
150 33 379/33	Cisco Ser0h-85	Snanning_tree_(for-	STR	conf TC +	2not	-	32768/17/	0.1	8-18-6e-9h-00	Cost = 0	Port -

Once the DHCP server is located, the client sends the configuration information request directly to the server node, in which case the client will be assigned an IP address and other configuration details, with a specific lease time.

A detailed view of the parameter assignment is shown here as well.

```
⊞ Frame 147: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
∃ Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 255.255.255.255 (255.255.255.255)
Bootstrap Protocol
   Message type: Boot Reply (2)
   Hardware type: Ethernet
   Hardware address length: 6
   Hops: 0
   Transaction ID: 0x438b960b
   Seconds elapsed: 0

    Bootp flags: 0x8000 (Broadcast)

   Client IP address: 0.0.0.0 (0.0.0.0)
   Your (client) IP address: 192.168.1.3 (192.168.1.3)
   Next server IP address: 0.0.0.0 (0.0.0.0)
   Relay agent IP address: 0.0.0.0 (0.0.0.0)
   client MAC address: compalco_b3:c4:ab (00:16:d4:b3:c4:ab)
   Client hardware address padding: 000000000000000000000
   Server host name not given
   Boot file name not given
   Magic cookie: DHCP

    Option: (t=53,1=1) DHCP Message Type = DHCP Offer

    Option: (t=54,1=4) DHCP Server Identifier = 192.168.1.1
    Option: (t=51,1=4) IP Address Lease Time = 7 days

    Option: (t=58, l=4) Renewal Time Value = 3 days, 12 hours

    Option: (t=59,1=4) Rebinding Time Value = 6 days, 3 hours

    ⊕ Option: (t-3, l-4) Router - 192.168.1.1

   End Option
   Padding
```

#### **Performance Analysis of DHCP**

Bahlmann (2002) suggests an approach to testing carrier class DHCP and puts forth the

following performance parameters:

- Average transaction time: The current average of all completed DHCP transactions between server and client. This number is helpful and will gradually increase as the server and the network becomes increasingly taxed.

- Average overall cycle time: The current average of all completed DHCP cycles with the server (DISCOVER to ACK).

- Percentage of completed DHCP transactions: The percentage of the number of transactions with the server that have been successfully completed by the DHCP client generator (completed as opposed to timed out or dropped).

- Current transaction rate: The number of transactions currently being sent to the server per second.

As each client transaction is about to begin, it is helpful to obtain a snap shot of these average times, the last completed individual transaction, and the overall cycle time and then store these along with the record assigned to the impending transaction. The purpose of obtaining this snap shot is to be able to determine the overall performance of the DHCP server upon the last good transactions before it begins dropping packets (as finding this point should be the goal of any

quality DHCP testing). When stress testing, you want to find the spot at which the server fails, begins to drop packets, and/or does not complete requested DHCP transactions with clients. Note that each of these spots may take place at different times (if at all) as load is increased (failure of the server may or may not occur unless the incoming packets somehow overload the application, available resources [disk, connection, memory, etc.], or the operating system [swap/virtual memory, memory, disk, etc.]). If the server does not fail, it may just drop some packets while completing others – it all depends on the capability of the server to prioritize its processing capability and complete the work it has started. It is the duty of the client generator to determine this point as well as the performance of the server leading up to that point. The sweet spot of the server (how many DHCP clients it can effectively maintain during any given time) may well be the spot at which the server can no longer keep up with any additional load or potentially just beyond this point depending on what the server does upon reaching saturation as well as its ability to overcome these instances and catch back up with the incoming requests.

## **Transport Protocols**

## **Overview of TCP and UDP**

The Transmission Control Protocol and the User Datagram Protocol are the most commonly used transport layer protocols of today. Their performances, although affected by that of the other lower layer protocols on top of which they run, defines the overall performance of the communication link. This section attempts to look deeper into the two transport protocols and identify their performance metrics, while exploring the performance tuning approaches for the two protocols.

A key element in the performance of any communication link is the physical layer through which the actual transmission takes place. Several papers and literature have studied the performance of TCP and UDP on the various mediums commonly in use today including but not limited to wireless and optical networks. The focus of this section is to propose a holistic, more generic approach to the key performance metrics pertaining to the two protocols. While the two protocols have been designed to tackle the end to end transmission of the packets, the purposes of their design and hence their uses vary. Understanding the differences in their behaviors and their respective applications is crucial as they drive the communications and data transmission across the Internet. This will eventually contribute to understanding their performance characteristics.

The Transmission Control Protocol (TCP) is used to provide reliable transmission between two nodes, which is facilitated by mechanisms built into the protocol that ensure the establishment of a virtual connection (session) before transmission, and acknowledgment of the packets sent among other techniques. TCP also provides congestion control, meaning it reduces its frame sending rate if it detects that the network is overloaded. Most typical applications need the reliability and other services provided by TCP, and don't care about loss of a small amount of performance to overhead. For example, most applications that transfer files or important data between machines use TCP, because loss of any portion of the file renders the entire operation useless. Examples include such well-known applications as the Hypertext Transfer Protocol (HTTP) used by the World Wide Web (WWW), the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP).

On the other hand, the User Datagram Protocol (UDP) is a connection-less transport protocol that gives no guarantees on the success rate of the transmissions. That is to say that applications using UDP as the transport layer protocol do not require the guarantee that the data sent was received successfully. Although this might seem bad, it is important to note that no one protocol is better than the other, it is only that one is more suitable for certain situations than the other. The overhead that is typical of TCP might not be required for certain applications such as VOIP, while it is important that an FTP session has successfully completed despite the overhead/cost involved in establishing and maintaining a session over TCP.

## IP, TCP and UDP Header Formats





The differences in frame and/or header structures indicates the differences in behavior, and hence

in performance requirements

### **Reliability**:

TCP: connection-oriented

#### UDP: connectionless

#### **Ordered**:

TCP: order of message receipt is guaranteed

UDP: order is not guaranteed

#### **Protocol weight:**

TCP: heavyweight, because of the connection/ordering overhead

UDP: lightweight, very few overhead

### Packets:

TCP: streaming, data is read as a stream, with nothing distinguishing where one packet ends and

another begins. There may be multiple packets per read call. UDP: datagrams, one packet per one read call.

More detailed header formats are presented below:



## **Traffic Capture Process/Methodology**

In the process of analyzing the performance of the two transport layer protocols, data from the previous captures has been perused. According to the test network design and the traffic captured during the test runs, TCP and UDP packets did not require any additional or specific traces. The ideal approach could have been the modeling of UDP and TCP packets using queuing theory to pinpoint opportunities for improved optimization and tuning.

## **Performance Metrics**



The Wireshark packet traces above show the TCP header structure of live traffic. The various sections in the header represent some key performance metrics that can be manipulated to enhance the performance of TCP including most importantly the Window Size. However, there are other elements that contribute to the performance of a TCP or a UDP transmission, some of those elements which have also been addressed by other literature include:

- 1. The physical layer aspects of the transmission link (the hardware and the medium)
- 2. The throughput including the maximum number of transactions per second, the MTU size
- 3. The adapter receive and transmit queues
- Device specific buffers which again involves the hardware I/O characteristics alluded to in number 1

## Performance Analysis of the Transport Layer Protocols

In general, it is known that TCP provides a reliable connection through its three-way handshake process, whereas UDP does not. In addition, the acknowledgement and retransmit features, TCP facilitates a more reliable link and is more suited to applications requiring the transmission of

large amounts of data.

This study and others before it show that TCP also offers higher throughput than UDP; however, when using UDP the end-to-end delay performance improves which makes it more suitable for delay sensitive applications such as VOIP, and other applications that require the transmission of information in small bursts such as those used for Telemetry and tele-operations.

# **Application Protocols**

## Introduction and Overview

This section of the CAPSTONE report deals with the performance metrics and issues of higher layer protocols with the goal of pinpointing the possible performance bottleneck areas. In this context, higher layer refers to the application layer protocols that are most commonly used in the TCP/IP protocol suite out of which four essential, very popular protocols have been selected to understand the performance issues surrounding the higher layer protocols.

These four protocols are:

- Hyper Text Transfer Protocol (HTTP): the ubiquitous protocol that made the World Wide Web and other Internet services possible.
- File Transfer Protocol (FTP): the protocol that makes it possible to transfer files between two nodes across networks.
- Telnet: is a protocol that facilitates bidirectional text based communication between two nodes using virtual terminals
- SSH: Secure Shell is Telnet's more secure cousin mostly used for out-of-band system administration

To understand the potential performance bottlenecks in the higher layer protocols, we need to first identify the underlying protocols in the stack that deal with the transport layer and data link layers. Looking down the OSI layer stack, higher layer protocols are susceptible to the weaknesses and performance issues of the lower layer protocols on which they depend for moving their data from one node to another destination node. By dissecting the structure of a higher layer data frame and identifying the various elements it contains that are critical for the performance of the protocols and their operations, it should be apparent as to what metrics are involved and how we can tweak that to squeeze the maximum performance out of the connections or sessions.

## **Performance Metrics and Measurement Issues**

## HyperText Transfer Protocol

HTTP protocol is what makes the World Wide Web possible. HTTP is a generic stateless object-

oriented protocol, which may be used for many similar tasks such as name servers, and distributed object-oriented systems, by extending the commands, or methods, used. A feature of HTTP is the negotiation of data representation, allowing systems to be built independently of the development of new advanced representations.

On the internet, the communication takes place over a TCP/IP connection. This does not preclude this protocol being implemented over any other protocol on the internet or other networks. In these cases, the mapping of the HTTP request and response structures onto the transport data units of the protocol in question is outside the scope of the specification of the protocol. However, it should not be that complicated specially considering the layered architecture of the networking models commonly used.

The protocol is basically stateless, a transaction consisting of:

**Connection:** The establishment of a connection by the client to the server - when using TCP/IP port 80 is the well-known port, but other non-reserved ports may be specified in the URL;

**Request:** The sending, by the client, of a request message to the server;

**Response:** The sending, by the server, of a response to the client;

**Close:** The closing of the connection by either both parties.

The format of the request and response parts is defined in RFC 2068 and related specifications.

Time	Source	Destination	Protocol	Info
1 0.000000	142.244.164.24	74.125.127.105	HTTP	GET /firefox?client=firefox-a&rls=org.mozilla:en-US:official HTTP/1.1
2 0.031603	74.125.127.105	142.244.164.24	HTTP	HTTP/1.1 302 Found (text/html)
3 0.098126	142.244.164.24	74.125.127.99	HTTP	GET /firefox?client=firefox-a&rls=org.mozilla:en-US:official HTTP/1.1
4 0.172179	142.244.164.24	74.125.127.99	HTTP	GET /images/firefox/redpandahead.png HTTP/1.1
5 0.203936	74.125.127.99	142.244.164.24	HTTP	HTTP/1.1 200 OK (PNG)
6 0.261444	74.125.127.105	142.244.164.24	HTTP	[TCP Retransmission] HTTP/1.1 302 Found (text/html)
7 0.436956	74.125.127.99	142.244.164.24	HTTP	[TCP Retransmission] HTTP/1.1 200 OK (PNG)
8 4.023482	142.244.164.24	74.125.127.99	HTTP	GET /imghp?client=firefox-a&rls=org.mozilla:en-US:official&hl=en&tab=wi HTTP/1.1
9 4.088369	74.125.127.99	142.244.164.24	HTTP	[TCP Previous segment lost] Continuation or non-HTTP traffic
10 4.092684	142.244.164.24	74.125.127.99	HTTP	[TCP ACKed lost segment] GET /intl/en_ALL/images/logos/images_logo_lg.gif HTTP/1.1

## Analysis of the HTTP Traces

The above screen capture of the trace in Wireshark demonstrates the request-response mechanism employed by the HTTP protocol. The request is sent by the browser using the GET message and indicating the browser and the version of supported HTTP; the first response is a confirmation that the request resource has been found; and it then goes about iteratively downloading the elements of the requested page including the images and then an OK acknowledgement in the form of the 200 code is sent back by the web server.

This simple structure of the request response mechanism is what makes it easy and straight forward to code browsers and web servers. A major issue in HTTP performance is the compression mechanism employed; this can affect the throughput and speed of the http protocol in any given scenario.

Most often, HTTP compression is implemented on the server side as a filter or module which applies the gzip algorithm to responses as the server sends them out. Any text based content can be compressed. In the case of purely static content, such as markup, style sheets, and JavaScript, it is usually possible to cache the compressed representation, sparing the CPU of the burden of repeatedly compressing the same file. When truly dynamic content is compressed, it usually must be recompressed each time it is requested (though there can be exceptions for quasi dynamic content, given a smart enough compression engine). This means that there is trade off to be considered between processor utilization and payload reduction. A highly configurable compression tool enables an administrator to adjust the tradeoff point between processor utilization and compressing CPU cycles on over compressing objects which might compress just as tightly with a lower level setting as with a higher one. This also allows for the exclusion of binary image files from HTTP compression, as most images are already optimized when they are created in an editor such as Illustrator. Avoid the needless recompression of images as this may actually increase their file size or introduce distortion.

All in all, HTTP performance comes down to the implementation and configuration of the web server. Focusing on tweaking the web server's performance by modifying its operating parameters would result in great returns in performance.

HTTP compression, otherwise known as content encoding, is a publicly defined way to compress textual content transferred from web servers to browsers. HTTP compression uses public domain compression algorithms, like gzip and compress, to compress XHTML, JavaScript, CSS, and other text files at the server. This standards-based method of delivering compressed content is built into HTTP 1.1, and most modern browsers that support HTTP 1.1 support ZLIB inflation of deflated documents. In other words, they can decompress compressed files automatically, which

saves time and bandwidth.

Tim	ne	Source	Destination	Protocol	Info			
1 0.	000000	2002:8ef4:a418::8ef4:	¿2002:c058:6301::c058:	(ICMPV6	Echo (ping) request id=0x0001, seq=129			
2 0.	996610	89.78.95.211	142.244.164.24	UDP	Source port: 65341 Destination port: 37539			
3 0.	997754	142.244.164.24	89.78.95.211	UDP	Source port: 37539 Destination port: 65341			
4 2.	517534	142.244.164.24	149.20.64.73	FTP	Request: PASV			
52.	569906	149.20.64.73	142.244.164.24	TCP	ftp > 49373 [ACK] Seq=1 Ack=7 Win=256 Len=0			
62.	570239	149.20.64.73	142.244.164.24	FTP	Response: 227 Entering Passive Mode (149,20,64,73,238,67).			
72.	570942	142.244.164.24	149.20.64.73	FTP	Request: SIZE /pub/FreeBSD/			
8 2.	571351	142.244.164.24	149.20.64.73	TCP	49377 > 60995 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2 SACK_PERM=1			
92.	623119	149.20.64.73	142.244.164.24	TCP	ftp > 49373 [ACK] Seq=51 Ack=27 Win=256 Len=0			
10 2.	623541	149.20.64.73	142.244.164.24	TCP	60995 > 49377 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460 WS=10 SACK_PERM=1			
11 2.	623655	142.244.164.24	149.20.64.73	TCP	49377 > 60995 [ACK] Seq=1 Ack=1 win=17520 Len=0			
12 2.	625861	149.20.64.73	142.244.164.24	FTP	Response: 550 Could not get file size.			
13 2.	626304	142.244.164.24	149.20.64.73	FTP	Request: MDTM /pub/FreeBSD/			
14 2.	675797	149.20.64.73	142.244.164.24	TCP	[TCP window Update] 60995 > 49377 [ACK] Seq=1 Ack=1 win=262144 Len=0			
15 2.	678972	149.20.64.73	142.244.164.24	TCP	ftp > 49373 [ACK] Seq=81 Ack=47 Win=256 Len=0			
		149.20.64.73	142.244.164.24	FTP	Response: 550 Could not get file modification time.			
		*** *** ***	140 00 64 70		and and the ferroes (			
	ame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) hernet II. Src: Intel.66:b5:ec (00:19:d2:66:b5:ec), Dst: Ditech.97:a8:00 (00:d0:02:97:a8:00)							
			(142.244.164.24), Dst		.99.1 (192.88.99.1) f4:a418::8af4:a418)			

## File Transfer Protocol

nternet Protocol, Src: 142.244.104.24 (142.244.104.24), DST: 192.80.99.1 (192.80.99.1) nternet Protocol Version 6, Src: 2002:8ef4:a418::8ef4:a418 (2002:8ef4:a418::8ef4:a418), DST: 2002:c058:6301::c058:6301 (2002:c058:6301::c058:6301) nternet Control Message Protocol V6

The FTP protocol follows the same request and response mechanism as the HTTP protocol show in the following diagram. The diagram below explains the above traces in more stark terms.



The factors that affect the performance metrics of an FTP server include:

- Mechanical elements such as the type of disks on the server and the nature of the IO operations needed to reply to the requests
- The file system type
- Any FTP caches in place
- Lower level protocols underlying the FTP protocol operations

The usual performance metrics apply to the FTP protocol as well as the HTTP protocol; most important of these is the throughput and the data transfer rate.

## Telnet

Telnet.pcap - Wireshark	Contract Contractory Contractory	Constitution will make total					
<u>File Edit View Go Capture Analyze Statistics T</u>	elephony <u>T</u> ools <u>H</u> elp						
$\blacksquare \blacksquare \boxtimes \boxtimes \boxtimes \boxtimes \models \blacksquare X \textcircled{=} =   < \cdot$	🗢 🛸 💫 7 🕹   🗐 🗐   O. Q. (	0. 🖆   🖉 🖄 %   💢					
Filter:	▼ Expression Clear Ap	pply					
No. Time Source	Destination Protocol In	info	-				
64 24.677563 192.168.186.128		Telnet Data					
65 24.934664 192.168.186.128		Telnet Data					
66 29.290899 192.168.186.1		Telnet Data					
67 29.291768 192.168.186.128		Telnet Data					
68 29.441437 192.168.186.1		Telnet Data Telnet Data					
69 29.442164 192.168.186.128		Telnet Data					
70 29.570593 192.168.186.1 71 29.571343 192.168.186.128		Telnet Data					
72 29.707309 192.168.186.1		Telnet Data					
73 29.718933 192.168.186.128		Telnet Data					
74 29.865544 192.168.186.1		Telnet Data					
75 29.866380 192.168.186.128		Telnet Data					
76 30.018197 192.168.186.1		Telnet Data					
77 30.018894 192.168.186.128		Telnet Data					
78 30.221065 192.168.186.128		Telnet Data					
79 33.093498 192.168.186.1		Telnet Data					
<pre>B Ethernet II, SrC: Vmware_e6:df:51 (00 B Internet Protocol, SrC: 192.168.186.12 B Transmission Control Protocol, SrC Por D Telnet</pre>	28 (192.168.186.128), Dst: 192.16 rt: telnet (23), Dst Port: 50397	68.186.1 (192.168.186.1)					
Data: \033]0;haroun@ubuntu904desktop: ~\aharoun@ubuntu904desktop:~\$							
0010 00 62 e6 8f 40 00 40 06 5e 23 c0 0020 ba 01 00 17 c4 dd a9 3e 1d ec eb 0030 00 b7 b9 c7 00 00 1b 5d 30 3b 68	0010 00 62 e6 6f 40 00 40 06 5e 23 c0 a8 ba 80 c0 a8 .b@.e. /#						
File: "C:\Users\abdullahi\Downloads\Telnet Packets		0	Profile: Default				

TELNET is a general protocol, meant to support logging in from almost any type of terminal to almost any type of computer. Its use and functionality, however, seems to be left with console connections to routers and computers in secure environments. It allows a user at one site to establish a TCP connection to a login server or terminal server at another site. A TELNET server generally listens on TCP Port 23.

The protocol is insecure by design as can be seen from the above figure where the submitted password is shown in the traces in plaintext. The protocol uses the concept of Network Virtual Terminals, and the connection between the two nodes is full duplex although it does not seem to be like that as the nature of the communication it is used for does not take full advantage of this capability.

The key performance metrics for the TELNET protocol are affected by the underlying TCP protocol's own performance.

## Secure Shell (SSH)

	race.pcap - Wiresh			-	Note Course for Read of Lot 1. Read of the read	
ile <u>t</u> i	lit <u>V</u> iew <u>G</u> o <u>C</u>	apture <u>A</u> nalyze <u>S</u> tatistics				
		🖻 🛃 🗶 🎜 🗏 🛛 🔍	🍬 🔿 🐼 🛣 📗		. 🔍 🛅   🔐 📧 🅵 %   💢	
ilter:			▼ Exp	pression Clear	Apply	
o.	Time	Source	Destination	Protocol	Info	
	1 0.000000	fe80::651a:978e:fc		SSDP	M-SEARCH * HTTP/1.1	
	2 3.000220	fe80::651a:978e:fc0		SSDP	M-SEARCH * HTTP/1.1	
	3 4.979160	fe80::651a:978e:fc		DHCPV6		
	4 7.000565	fe80::651a:978e:fc0		SSDP	M-SEARCH * HTTP/1.1	
	5 10.000504 6 13.000567	fe80::651a:978e:fc0 fe80::651a:978e:fc0		SSDP SSDP	M-SEARCH * HTTP/1.1 M-SEARCH * HTTP/1.1	
	7 14.769976	192.168.124.1	192.168.124.132	SSH	Encrypted request packet len=52	
	8 14.776481	192.168.124.132	192.168.124.1	SSH	Encrypted response packet len=52	
	9 14.979395	192.168.124.1	192.168.124.132	TCP	49365 > ssh [ACK] Seq=53 Ack=53 Win=253 Len=0	
	LO 15.092494	192.168.124.1	192.168.124.132	SSH	Encrypted request packet len=52	
	1 15.100497		192.168.124.1	SSH	Encrypted response packet len=52	
		192.168.124.1	192.168.124.132	SSH	Encrypted request packet len=52	
		192.168.124.132	192.168.124.1	SSH	Encrypted response packet len=52	
		192.168.124.1	192.168.124.132	SSH	Encrypted request packet len=52	
	15 15.356510	192.168.124.132	192.168.124.1	SSH	Encrypted response packet len=52	
	16 15.482311	192.168.124.1	192.168.124.132	SSH	Encrypted request packet len=52	
Ethe Inte	ernet II, Src ernet Protoco		0:50:56:c0:00:08), 80::651a:978e:fc06:	Dst: IPv6mcas dcO6 (fe80::6	t_00:00:00:0c (33:33:00:00:00:0c) 51a:978e:fc06:dc06), Dst: ff02::c)	
	rtext Transf		449 (54449), DST PO	rt: ssap (190	(0)	
нуре	rtext Iranst	er Protocol				
00	33 33 00 00 0	00 0c 00 50 56 c0 00	08 86 dd 60 00	33P V		
10 20	00 00 00 9a 1 07 80 fc 06 (	L1 01 fe 80 00 00 00 dc 06 ff 02 00 00 00	0000000651a .		e.	
30	00 00 00 00 0	00 0c d4 b1 07 6c 00	) 9a ed f6 4d 2d .			
	53 45 41 52 4	13 48 20 2a 20 48 54	54 50 2f 31 2e	SEARCH * HTT	P/1.	
40		F 72 74 25 56 46 46		HOCT · FEED		
50		\Downloads\SSH Tr Packe				0

SSH or Secure Shell is the most common remote login protocol and application in use today, as it offers the security protocols such as rlogin and telnet lack. The protocol is based on TCP; and in its simplest mode of operation, it connects to a server, negotiates a shared secret key using Diffie- Hellman, then begins encrypting the session (typically using the Blowfish cipher). A username and password are passed over the encrypted session and, if authenticated, the server starts a command shell over the encrypted session.

Using TCP at the Transport Layer poses some performance issues. A number of network applications make use of multiplexed channels inside of a single TCP connection to handle data transfer and/or control information. Because these channels cannot make use of the TCP windows for flow control they must implement their own. This means that a second window can be imposed on top of the existing TCP window. The result of this is that even if the TCP window is correctly sized for the current to produce exceptional FTP performance a user may still encounter dismal throughput under one of these applications. This is because the application window, which is often statically defined, is too small for many typical paths. This forces the connection to slow down to the limit of the smaller of the two windows. The best current example of this is the SSH2 protocol. It is not uncommon for a user to be sitting on a connection they can utilize less than 1% of because of this double window problem. While a user might not experience any issues in interactive sessions it's a very noticeable problem in bulk data transfers (e.g. SCP, rsync -essh, sftp, etc) and is common source of frustration – especially for users with access to high performance network connections.

## Data Link Protocols

## **Overview**

This section looks into the second layer among the OSI networking model, and the performance issues related to this layer. Although this study might not look into the low level mechanisms that define this layer's functions, it will focus more into a couple of protocols and concepts that are part of the layer's operations. The function of the data link layer is to take requests from the network layer and send requests to the physical layer below it. To be more specific, the data link layer has the following functions:

**Logical Link Control (LLC):** Logical link control refers to the functions required for the establishment and control of logical links between local devices on a network. As mentioned above, this is usually considered a DLL sub layer; it provides services to the network layer above it and hides the rest of the details of the data link layer to allow different technologies to work seamlessly with the higher layers. Most local area networking technologies use the IEEE 802.2 LLC protocol.

**Media Access Control (MAC):** This refers to the procedures used by devices to control access to the network medium. Since many networks use a shared medium (such as a single network cable, or a series of cables that are electrically connected into a single virtual medium) it is necessary to have rules for managing the medium to avoid conflicts. For example. Ethernet uses the CSMA/CD method of media access control, while Token Ring uses token passing.

**Data Framing:** The data link layer is responsible for the final encapsulation of higher-level messages into *frames* that are sent over the network at the physical layer.

Addressing: The data link layer is the lowest layer in the OSI model that is concerned with addressing: labeling information with a particular destination location. Each device on a network has a unique number, usually called a *hardware address* or *MAC address*, which is used by the data link layer protocol to ensure that data intended for a specific machine gets to it properly.

**Error Detection and Handling:** The data link layer handles errors that occur at the lower levels of the network stack. For example, a cyclic redundancy check (CRC) field is often employed to allow the station receiving data to detect if it was received correctly.

Commonly used examples of Data Link Layer protocols are Ethernet, PPP and Token Ring. This layer is usually in the form of a software device driver for the network interface card (NIC

The layer itself is divided into two parts as mentioned above- MAC and LLC, which communicate with the layers above and below the data link layer. MAC (media access control) determines how data on a network meant for a specific computer reaches it and how a computer can transmit data. Every physical card has a unique MAC address and every frame sent on the network has both source and destination MAC addresses in the header. So the receiving DLL knows which frames on the network are meant for itself, and which computer sent the frame. In this category, the focus is on ARP, RARP, multicast, unicast and Ethernet. The objective is to point out the key performance issues and related factors, and will follow the format of the previous sections.

## ARP and RARP

Although included in this section, the ARP and RARP protocols are categorized as IP layer protocols. Address Resolution Protocol (ARP) is a required TCP/IP standard defined in RFC 826, Address Resolution Protocol (ARP). ARP resolves IP addresses used by TCP/IP-based software to media access control addresses used by LAN hardware. The Reverse ARP protocol is defined in RFC 903.

ARP provides the following protocol services to hosts located on the same physical network:

- Media access control addresses are obtained by using a network broadcast request in the form of the question what is the media access control address for a device that is configured with the enclosed IP address?
- When an ARP request is answered, both the sender of the ARP reply and the original ARP requester record each other's IP address and media access control address as an entry in a local table called the ARP cache for future reference.

RARP is described in Internet Engineering Task Force (IETF) publication RFC 903. [1] It has been rendered obsolete by the Bootstrap Protocol (BOOTP) and the modern Dynamic Host Configuration Protocol (DHCP), which both support a much greater feature set than RARP. This is most commonly used for products that use mass deployment of software (OSes).

RARP requires one or more server hosts to maintain a database of mappings of Link Layer addresses to their respective protocol addresses. Media Access Control (MAC) addresses needed to be individually configured on the servers by an administrator. RARP was limited to serving only IP addresses.

The Wireshark traces below show the operation of the Address Resolution Protocol in the test network.

 Time
 Source
 Destination
 Protocol
 Info

 6 22.156909
 Intel\_66:b5:ec
 Broadcast
 ARP
 who has 142.244.164.26?
 Tell 142.244.164.24

In the above diagram, a broadcast message is sent across the network segment as part of the ARP protocol operations. The goal is to get the MAC address of the machine interface with the IP address 142.244.164.26. The response to this will be a unicast message back to the node that initiated the ARP request.

## Unicast and Multicast

Unicast, Multicast and Broadcast are basically communication modes used in data transmission; the classification is based on the nature of what is on the receiving end of the transmission; and has many applications in the operations of the internets as will be seen in the upcoming sections.

Unicast packets are sent from host to host. The communication is from a single host to another single host. Broadcast (not included in this discussion) is used when a single device is transmitting a message to all other devices in a given address range. This broadcast could reach all hosts on the subnet, all subnets, or all hosts on all subnets. Broadcast packets have the host (and/or subnet) portion of the address set to all ones. By design, most modern routers block IP broadcast traffic and restrict it to the local subnet.

Multicast is a special protocol for use with IP. Multicast enables a single device to communicate with a specific set of hosts, not defined by any standard IP address and mask combination. This allows for communication that resembles a conference call. Anyone from anywhere can join the conference, and everyone at the conference hears what the speaker has to say. The speaker's

message isn't broadcasted everywhere, but only to those in the conference call itself. A special set of addresses is used for multicast communication. In the previous classification of IPv4 addresses, class D was reserved for multicast operations. If the operations of routing protocols are studied carefully, it would appear that protocols such as OSPF and EIGRP use multicast to share their routing tables and updates.

15 13.070093 169.254.178.12	224.0.0.252	IGMP	V2 Membership Report / Join group 224.0.0.252
16 13.161736 169.254.178.12	224.0.0.2	IGMP	V2 Leave Group 239.255.255.250
17 13.163414 169.254.178.12	239.255.255.250	IGMP	V2 Membership Report / Join group 239.255.255.250
18 13.292841 169.254.178.12	224.0.0.2	IGMP	V2 Leave Group 224.0.0.252
19 13.293151 169.254.178.12	224.0.0.252	IGMP	V2 Membership Report / Join group 224.0.0.252
20 13.570121 169.254.178.12	239.255.255.250	IGMP	V2 Membership Report / Join group 239.255.255.250
21 13.570273 169.254.178.12	224.0.0.252	IGMP	V2 Membership Report / Join group 224.0.0.252
22 16.156339 169.254.178.12	224.0.0.2	IGMP	V2 Leave Group 224.0.0.252

In the above trace capture, the highlighted line (17) indicates a multicast message to the address 239.255.255.250 (class D according to the now obsolete and irrelevant IP address classification system).

mile	Source	Destination	FIOLOCOI	1110
1 0.000000	85.73.34.205	142.244.164.24	UDP	Source port: 33203 Destination port: 37539
2 0.000441	142.244.164.24	85.73.34.205	UDP	Source port: 37539 Destination port: 33203
3 1.062953	24.196.201.203	142.244.164.24	UDP	Source port: 55005 Destination port: 37539
4 1.063389	142.244.164.24	24.196.201.203	UDP	Source port: 37539 Destination port: 55005
5 1.348945	190.203.161.103	142.244.164.24	UDP	Source port: 30610 Destination port: 37539
6 1.349368	142.244.164.24	190.203.161.103	UDP	Source port: 37539 Destination port: 30610
7 1.660453	186.45.85.185	142.244.164.24	UDP	Source port: 23825 Destination port: 37539
8 1.660877	142.244.164.24	186.45.85.185	UDP	Source port: 37539 Destination port: 23825
9 1.725722	2002:8ef4:a418::8ef4	:;2002:c058:6301::c058	:(ICMPV6	Echo (ping) request id=0x0001, seq=265
10 1.750210	142.244.164.24	129.128.5.233	DNS	Standard query A data2.wowzio.com
11 1.750581	142.244.164.24	129.128.76.233	DNS	Standard query A data2.wowzio.com
12 1.751373	129.128.5.233	142.244.164.24	DNS	Standard query response A 67.207.149.136
13 1.751483	129.128.76.233	142.244.164.24	DNS	Standard query response A 67.207.149.136
14 1.752206	142.244.164.24	129.128.5.233	DNS	Standard query AAAA data2.wowzio.com
15 1.753389	129.128.5.233	142.244.164.24	DNS	Standard query response
16 1.754598	142.244.164.24	67.207.149.136	TCP	49745 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2 SACK_PERM=1

## Ethernet

Like unicast, multicast and ARP; Ethernet is not restricted to the data link layer of the communication network model. Ethernet is defined in IEEE 802.3 standard, and has largely superseded other LAN networking protocols and technologies as of 1980. Systems communicating over Ethernet divide a stream of data into individual packets called frames. Each frame contains source and destination addresses and error-checking data so that damaged data can be detected and re-transmitted.

Ethernet is a family of protocols and techniques that operate at the physical and data link layers of the OSI reference model. Ethernet uses a protocol called CSMACD. This stands for Carrier

Sense, Multiple Access, and Collision Detection. The Multiple Access part means that every station is connected to a single copper wire (or a set of wires that are connected together to form a single data path). The Carrier Sense part says that before transmitting data, a station checks the wire to see if any other station is already sending something. If the LAN appears to be idle, then the station can begin to send data.

## **Common Performance Metrics**

The following are common metrics to most network and systems administrators.

**Latency:** It can take a long time for a packet to be delivered across intervening networks. In reliable protocols where a receiver acknowledges delivery of each chunk of data, it is possible to measure this as round-trip time.

**Packet loss:** In some cases, intermediate devices in a network will lose packets. This may be due to errors, to overloading of the intermediate network, or to intentional discarding of traffic in order to enforce a particular service level.

**Retransmission:** When packets are lost in a reliable network, they are retransmitted. This incurs two delays: First, the delay from re-sending the data; and second, the delay resulting from waiting until the data is received in the correct order before forwarding it up the protocol stack.

**Throughput:** The amount of traffic a network can carry is measured as throughput, usually in terms such as kilobits per second. Throughput is analogous to the number of lanes on a highway, whereas latency is analogous to its speed limit.

These factors, and others (such as the performance of the network signaling on the end nodes, compression, encryption, concurrency, and so on) all affect the effective performance of a network. In some cases, the network may not work at all; in others, it may be slow or unusable. And because applications run over these networks, application performance suffers. Various intelligent solutions are available to ensure that traffic over the network is effectively managed to optimize performance for all users.

In summary, the OSI layered model of communication imposes a systematic approach to data transmission and receipt. This dictates that any single transmission's performance is influenced

by the internal algorithms implemented at layer.

## **Routing Protocols**

Routing protocols are concerned with how the routers communicate with each other, and share routing information and approaches to select routes. This category of protocols are considered layer management protocols for the network layer, and may run over a variety of routed protocols such as TCP and UDP, and other non-transport layer protocols such as IS-IS which runs on CLNS.

This section explores the performance metrics and analysis of routing protocols; specifically, RIP, OSPF, IS IS and BGP will be addressed. Since the routing protocols differ in their philosophy, goals and applications than the routed protocols discusses in the previous sections, their performance metrics and complexities are more concerned with issues such as convergence times and overheads introduced by the control traffic.

To analyze the performance of the four protocols, the test lab setup introduced in the first section of this report has been used. The section begins with an overview of each of the four protocols to provide a clearer picture on their respective operations.

A dynamic routing protocol is responsible for path determination, routing updates and choosing the best path in a network (host node to destination node). Performance analysis of different routing protocols has been done based on different performance metrics like network convergence, router convergence, queuing delay and throughput and network bandwidth utilization, CPU utilization and routing traffic.

#### RIP

#### **Overview**

RIP (Routing Information Protocol) is categorized as an interior, distance vector routing protocol, and uses the Bellman-Ford single-source shortest path algorithm. One of the oldest routing protocols to be used, RIP has been in use for over 20 years; and currently has three versions: RIPv1, RIPv2 and RIPng.

It utilizes a mechanism known as routing by rumor in which each router broadcasts the whole of its routing table out of its active ports, and the receiving routers adopt that information and also pass it on to the others. One of the key performance issues with RIP is this periodic (30 second interval) update that includes the whole routing table; which, if it grows very large, can have dire consequences on bandwidth. Because of this and other reasons including the allowed 15 hops maximum, RIP is not a preferable routing protocol in today's network environments.

#### **Performance metrics**

The performance of the routing protocols is mainly based on the underlying algorithm it uses to select the best path. In this regard, RIP uses Bellman-Ford single-source shortest path algorithm, which has an algorithmic performance worst case scenario of O(|V|\*|E|), where V is akin to the number of routers and E the links between the routers. The inherent limitation of lack of scalability stems from the use of this algorithm.

In terms of bandwidth usage, the protocol sends routing updates every 30 seconds using UDP among other messages. Although the use of UDP eases the burden on the bandwidth (no acknowledgements and other overhead required as in TCP), the 30 second update intervals put an extra overhead on the available bandwidth. The severity of this is much felt on small bandwidth links such as serial connections. RIP is al so known for its slow convergence times and reliability issues due to the possibility of creating routing loops.

#### Traces

Time	Source	Destination	Protocol	Info
1 0.000000	CompalCo_b3:c4:ab	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.2
2 0.421563	fe80::78cd:8e70:a5b0:	ff02::1:2	DHCPV6	Solicit XID: 0xfb2c1e CID: 0001000112810aa80016d4b3c4ab
3 1.578935	Cisco_96:f2:41	Cisco_96:f2:41	LOOP	Reply
4 11.579014	Cisco_96:f2:41	Cisco_96:f2:41	LOOP	Reply
5 21.579301	Cisco_96:f2:41	Cisco_96:f2:41	LOOP	Reply
6 21.587774	Cisco_96:f2:41	CDP/VTP/DTP/PAgP/UDLD	CDP	Device ID: Router_A Port ID: FastEthernet0/1
7 24.900174	192.168.1.1	255.255.255.255	RIPV1	Response
8 31.579725	Cisco_96:f2:41	Cisco_96:f2:41	LOOP	Reply
9 32.432690	fe80::78cd:8e70:a5b0:	:ff02::1:2	DHCPV6	Solicit XID: 0xfb2c1e CID: 0001000112810aa80016d4b3c4ab
10 41.579647	Cisco_96:f2:41	Cisco_96:f2:41	LOOP	Reply
11 51.579897	Cisco_96:f2:41	Cisco_96:f2:41	LOOP	Reply
12 53.216619	CompalCo_b3:c4:ab	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.2
13 53.736620	192.168.1.1	255.255.255.255	RIPV1	Response
14 53.991627	CompalCo_b3:c4:ab	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.2
15 54.990047	CompalCo_b3:c4:ab	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.2
16 56.238436	CompalCo_b3:c4:ab	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.2
17 56.986904	CompalCo_b3:c4:ab	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.2
18 58.000859	CompalCo_b3:c4:ab	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.2
19 59.264862	CompalCo_b3:c4:ab	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.2
20 59.997702	CompalCo_b3:c4:ab	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.2
21 60.996065	CompalCo_b3:c4:ab	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.2
22 61.580014	cisco_96:f2:41	Cisco_96:f2:41	LOOP	Reply
23 71.580270	Cisco_96:f2:41	Cisco_96:f2:41	LOOP	Reply
24 81.580438	Cisco_96:f2:41	Cisco_96:f2:41	LOOP	Reply
25 81.588886	Cisco_96:f2:41	CDP/VTP/DTP/PAgP/UDLD	CDP	Device ID: Router_A Port ID: FastEthernet0/1
26 83.301303	192.168.1.1	255.255.255.255	RIPV1	Response
27 86.932724	Cisco_96:f2:41	DEC-MOP-Remote-Consol	0x6002	DEC DNA Remote Console
28 91.580644	Cisco_96:f2:41	Cisco_96:f2:41	LOOP	Reply
29 101.580826	Cisco_96:f2:41	Cisco_96:f2:41	LOOP	Reply

On startup, RIP broadcasts a packet carrying a Request message out each RIP-enabled interface. The RIP process then enters a loop, listening for RIP Request or Response messages from other routers. Neighbors receiving the Request send a Response containing their route table.

Line number 7 shows an interface with IP address 192.168.1.1 sending a response. The request broadcast capture was missed in this diagram, but we can at least see the loop. This broadcast mechanism (destination of 255.255.255.255) is what makes RIP inefficient and not suitable for scalable internetworks.

#### Analysis

The above figure represents the RIP traces captures during the lab tests. It shows the routing loop issues the RIP protocol faces, which also results in unnecessary overhead. Just by looking at the entries in this trace file, it is apparent that almost have of them refer to routing loops.

#### **OSPF**

#### **Overview**

OSPF is an interior routing protocol categorized as a link-state protocol as it uses a link state routing algorithm (shortest path first). OSPF routes IP packets within a single Autonomous System (AS) by gathering link state information from routers and building a topology map out of it. Based on the topology map, the routing table to be provided to the Internet Protocol is determined.

Since OSPF is aware of the network topology, it detects any changes in the topology, and converges quickly (in seconds) – a feature that makes it more stable and reliable than RIP. OSPF uses Dijkstra's algorithm for shortest paths to find the shortest path tree for each route.

The OSPD packet header has a structure that shows the use of the Area concept in simplifying the management of the resources and traffic. Every OSPF packet starts with a common 24 byte header. This header contains all the necessary information to determine whether the packet should be accepted for further processing. This determination is described in Section 8.2 of the specification.



Explanations of the header elements:

Version #

The OSPF version number. This specification documents version 2 of the protocol.

### Type

The OSPF packet types are as follows. The format of each of these packet types is described in a later section.

Type Description
- 1 Hello
- 2 Database Description
- 3 Link State Request
- 4 Link State Update
- 5 Link State Acknowledgment

#### Packet length

The length of the protocol packet in bytes. This length includes the standard OSPF header.

#### Router ID

The Router ID of the packet's source. In OSPF, the source and destination of a routing protocol packet are the two ends of an (potential) adjacency.

#### Area ID

A 32 bit number identifying the area that this packet belongs to. All OSPF packets are associated with a single area. Most travel a single hop only. Packets travelling over a virtual link are labeled with the backbone Area ID of 0.0.0.0.

#### Checksum

The standard IP checksum of the entire contents of the packet, starting with the OSPF packet header but excluding the 64-bit authentication field. This checksum is calculated as the 16-bit one's complement of the one's complement sum of all the 16-bit words in the packet, excepting the authentication field. If the packet's length is not an integral number of 16-bit words, the packet is padded with a byte of zero before check-summing.

#### AuType

Identifies the authentication scheme to be used for the packet. Authentication is discussed in Appendix D of the specification. Consult Appendix D for a list of the currently defined authentication types.

#### Authentication

A 64-bit field for use by the authentication scheme.

The protocol uses a data structure called the link-state database. A router has a separate link state database for every area to which it belongs. The link state database has been referred to elsewhere in the text as the topological database. All routers belonging to the same area have identical topological databases for the area.

#### Performance metrics and other features

OSPF has the following characteristics:

- (1) Fast detection of changes in the topology and very fast reestablishment of routes without
- Loops, which translates to fast convergence times.
- (2) Low overload, use updates that inform about changes on routes.
- (3) Division of traffic by several equivalent routes.
- (4) Routing according type of service.
- (5) Use of multi-send in local area networks.
- (6) Subnet and Super-net mask.
- (7) Authentication

#### Traces

Exchange of the Hello packets for neighbor discovery.

Time	Source	Destination	Protocol	Info
1 0.000000	Cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
2 9.999964	<pre>cisco_96:f2:c0</pre>	Cisco_96:f2:c0	LOOP	Reply
3 19.999834	Cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
4 29.999780	Cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
5 33.623236	10.0.0.14	224.0.0.5	OSPF	Hello Packet
6 37.951955	Cisco_96:f2:c0	CDP/VTP/DTP/PAgP/UDLD	CDP	Device ID: Router_A Port ID: FastEthernet0/0
7 39.999612	Cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
8 43.619636	10.0.0.14	224.0.0.5	OSPF	Hello Packet
9 49.999605	Cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
10 53.619566	10.0.0.14	224.0.0.5	OSPF	Hello Packet
11 59.999387	Cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
12 63.619473	10.0.0.14	224.0.0.5	OSPF	Hello Packet
13 69.999398	<pre>Cisco_96:f2:c0</pre>	<pre>cisco_96:f2:c0</pre>	LOOP	Reply
14 73.619558	10.0.0.14	224.0.0.5	OSPF	Hello Packet
15 79.999205	<pre>cisco_96:f2:c0</pre>	Cisco_96:f2:c0	LOOP	Reply
16 83.619254	10.0.0.14	224.0.0.5	OSPF	Hello Packet
17 90.009494	Cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
18 93.619150	10.0.0.14	224.0.0.5	OSPF	Hello Packet
	Cisco_96:f2:c0	CDP/VTP/DTP/PAgP/UDLD	CDP	Device ID: Router_A Port ID: FastEthernet0/0
20 99.999012	Cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
21 103.619042	10.0.0.14	224.0.0.5	OSPF	Hello Packet
	Cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
23 113.618945	10.0.0.14	224.0.0.5	OSPF	Hello Packet
	<pre>Cisco_96:f2:c0</pre>	Cisco_96:f2:c0	LOOP	Reply
25 123.618829		224.0.0.5	OSPF	Hello Packet
	<pre>cisco_96:f2:c0</pre>	Cisco_96:f2:c0	LOOP	Reply
27 133.618743		224.0.0.5	OSPF	Hello Packet
	<pre>cisco_96:f2:c0</pre>	<pre>cisco_96:f2:c0</pre>	LOOP	Reply
29 142.163256		224.0.0.5	OSPF	Hello Packet
30 142.164661		10.0.0.13	OSPF	Hello Packet

Time	Source	Destination	Protocol	Info
28 139.998617	Cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
29 142.163256	10.0.0.13	224.0.0.5	OSPF	Hello Packet
30 142.164661	10.0.0.14	10.0.0.13	OSPF	Hello Packet
31 142.165311	10.0.0.13	10.0.0.14	OSPF	DB Description
32 142.165407	10.0.0.13	10.0.0.14	OSPF	Hello Packet
33 142.167120	10.0.0.14	10.0.0.13	OSPF	DB Description
34 142.167538		10.0.0.14	OSPF	DB Description
35 142.169317	10.0.0.14	10.0.0.13	OSPF	DB Description
36 142.169647	10.0.0.13	10.0.0.14	OSPF	DB Description
37 142.171171	10.0.0.14	10.0.0.13	OSPF	DB Description
38 142.171411		10.0.0.14	OSPF	LS Request
39 142.171555		10.0.0.14	OSPF	DB Description
40 142.173555		10.0.0.13	OSPF	LS Update
	10.0.0.13	224.0.0.5	OSPF	LS Update
42 142.699378		224.0.0.5	OSPF	LS Update
43 142.806583		224.0.0.5	OSPF	LS Update
44 143.618677		224.0.0.5	OSPF	Hello Packet
45 144.670158		224.0.0.5	OSPF	LS Acknowledge
46 145.162703		224.0.0.5	OSPF	LS Acknowledge
	Cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
48 152.162103		224.0.0.5	OSPF	Hello Packet
49 153.618577		224.0.0.5	OSPF	Hello Packet
	cisco_96:f2:c0	CDP/VTP/DTP/PAgP/UDLD		Device ID: Router_A Port ID: FastEthernet0/0
51 159.998414	<pre>cisco_96:f2:c0</pre>	Cisco_96:f2:c0	LOOP	Reply
52 162.162133		224.0.0.5	OSPF	Hello Packet
53 163.618502		224.0.0.5	OSPF	Hello Packet
	<pre>cisco_96:f2:c0</pre>	<pre>cisco_96:f2:c0</pre>	LOOP	Reply
55 172.162244		224.0.0.5	OSPF	Hello Packet
56 173.106252	192.168.3.2	224.0.0.22	IGMP	V3 Membership Report / Leave group 224.0.0.252

### LSA updates

Time	Source	Destination	Protocol	Info
79 184.399848	CompalCo_b3:c4:ab	Broadcast	ARP	Who has 192.168.3.1? Tell 192.168.3.2
80 189.998190	cisco_96:f2:c0	cisco_96:f2:c0	LOOP	Reply
81 192.167681	10.0.0.13	224.0.0.5	OSPF	Hello Packet
82 193.618204	10.0.0.14	224.0.0.5	OSPF	Hello Packet
83 200.006868	<pre>cisco_96:f2:c0</pre>	cisco_96:f2:c0	LOOP	Reply
84 202.162274	10.0.0.13	224.0.0.5	OSPF	Hello Packet
85 203.618070	10.0.0.14	224.0.0.5	OSPF	Hello Packet
86 209.998050	Cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
87 212.162307	10.0.0.13	224.0.0.5	OSPF	Hello Packet
88 213.617949	10.0.0.14	224.0.0.5	OSPF	Hello Packet
89 215.836150	10.0.0.13	224.0.0.5	OSPF	LS Update
90 217.802841	10.0.0.14	224.0.0.5	OSPF	LS Update
91 217.950196	Cisco_96:f2:c0	CDP/VTP/DTP/PAgP/UDLD	CDP	Device ID: Router_A Port ID: FastEthernet0/0
92 218.337956		224.0.0.5	OSPF	LS Acknowledge
	<pre>cisco_96:f2:c0</pre>	Cisco_96:f2:c0	LOOP	Reply
94 220.302384		224.0.0.5	OSPF	LS Acknowledge
95 222.162458		224.0.0.5	OSPF	Hello Packet
96 223.617927		224.0.0.5	OSPF	Hello Packet
	Cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
98 232.162491		224.0.0.5	OSPF	Hello Packet
99 233.617797		224.0.0.5	OSPF	Hello Packet
100 234.522857		224.0.0.5	OSPF	LS Update
101 234.557925		224.0.0.5	OSPF	LS Update
102 237.022351		224.0.0.5	OSPF	LS Acknowledge
	Cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
104 242.162512		224.0.0.5	OSPF	Hello Packet
105 243.618076		224.0.0.5	OSPF	Hello Packet
	Cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
107 252.162541		224.0.0.5	OSPF	Hello Packet
108 253.617589		224.0.0.5	OSPF	Hello Packet

#### Analysis

The first figure in this group shows the exchange of the Hello packets. Routers periodically send hello packets on all interfaces, including virtual links, to establish and maintain neighbor relationships. Hello packets are multicast on physical networks that have a multicast or broadcast capability, which enables dynamic discovery of neighboring routers. (On non-broadcast networks, dynamic neighbor discovery is not possible, so you must configure all neighbors statically using the neighbor statement.)

Hello packets consist of the OSPF header plus the following fields:

- Network mask—Network mask associated with the interface.
- Hello interval—how often the router sends hello packets. All routers on a shared network must use the same hello interval. You configure this interval with the hello-interval statement.
- Options—Optional capabilities of the router.
- Router priority—the router's priority to become the designated router. You can configure this value with the priority statement.
- Router dead interval—how long the router waits without receiving any OSPF packets from a router before declaring that router to be down. All routers on a shared network

must use the same router dead interval. You can configure this value with the deadinterval statement.

- Designated router—IP address of the designated router.
- Backup designated router—IP address of the backup designated router.
- Neighbor—IP addresses of the routers from which valid hello packets have been received within the time specified by the router dead interval.

The next two figures indicate the process of building the link state database and the exchange of LSAs. Database Description Packets

When initializing an adjacency, OSPF exchanges database description packets, which describe the contents of the topological database. These packets consist of the OSPF header, packet sequence number, and the link-state advertisement's header.

#### **Link-State Request Packets**

When a router detects that portions of its topological database are out of date, it sends a link-state request packet to a neighbor requesting a precise instance of the database. These packets consist of the OSPF header plus fields that uniquely identify the database information that the router is seeking.

#### Link-State Update Packets

Link-state update packets carry one or more link-state advertisements one hop farther from their origin. The router multicasts (floods) these packets on physical networks that support multicast or broadcast mode. The router acknowledges all link-state update packets and, if retransmission is necessary, sends the retransmitted advertisements unicast.

Link-state update packets consist of the OSPF header plus the following fields:

- Number of advertisements—Number of link-state advertisements included in this packet.
- Link-state advertisements—the link-state advertisements themselves.

#### Link-State Acknowledgment Packets

The router sends link-state acknowledgment packets in response to link-state update packets to verify that the update packets have been received successfully. A single acknowledgment packet can include responses to multiple update packets.

Link-state acknowledgment packets consist of the OSPF header plus the link-state advertisement header.

#### Link-State Advertisement Packet Types

Link-state request, link-state update, and link-state acknowledgment packets are used to reliably flood link-state advertisement packets. OSPF sends the following types of link-state advertisements:

- Router link advertisements—are sent by all routers to describe the state and cost of the router's links to the area. These link-state advertisements are flooded throughout a single area only.
- Network link advertisements—are sent by designated routers to describe all the routers attached to the network. These link-state advertisements are flooded throughout a single area only.
- Summary link advertisements—are sent by area border routers to describe the routes that they know about in other areas. There are two types of summary link advertisements: those used when the destination is an IP network, and those used when the destination is an AS boundary router. Summary link advertisements describe inter-area routes; that is, routes to destinations outside the area but within the AS. These link-state advertisements are flooded throughout the advertisement's associated areas.
- AS external link advertisement—are sent by AS boundary routers to describe external routes that they know about. These link-state advertisements are flooded throughout the AS (except for stub areas).

Each link-state advertisement type describes a portion of the OSPF routing domain. All link-state advertisements are flooded throughout the AS.

Each link-state advertisement packet begins with a common 20-byte header.

#### **OSPF** Metrics

The primary OSPF metric is *cost*, which Cisco and other manufacturers configure to be inversely proportional to the bandwidth of that interface. Lower cost means a faster interface and shorter end-to-end transmission times and thus the shortest path. The bandwidth of an interface is indirectly passed on with the OSPF route in the form of an additive 'cost' metric to indicate the speed of the entire path to the destination via the local interface link. Because OSPF is a link state protocol, higher speed links have a lower cost than low speed links.

#### IS-IS

#### **An Overview**

IS IS is the defacto standard for large service provider networks, and is defined in RFC 1142. It is an interior gateway protocol, which means it is designed for use within an administrative domain or network. IS-IS is a link-state routing protocol, operating by reliably flooding link state information throughout a network of routers. Each IS-IS router independently builds a database of the network's topology, aggregating the flooded network information. Like the OSPF protocol, IS-IS uses Dijkstra's algorithm for computing the best path through the network. Packets (datagrams) are then forwarded, based on the computed ideal path, through the network to the destination.

While OSPF is natively built to route IP and is itself a Layer 3 protocol that runs on top of IP, IS-IS is natively an OSI network layer protocol (it is at the same layer as CLNS). The widespread adoption of IP worldwide may have contributed to OSPF's popularity. IS-IS does not use IP to carry routing information messages. IS-IS is neutral regarding the type of network addresses for which it can route. OSPF, on the other hand, was designed for IPv4. This allowed IS-IS to be easily used to support IPv6. To operate with IPv6 networks, the OSPF protocol was rewritten in OSPF v3 (as specified in RFC 2740).

IS-IS routers build a topological representation of the network. This map indicates the subnets which each IS-IS router can reach, and the lowest-cost (shortest) path to a subnet is used to forward traffic.

OSPF has a larger set of extensions and optional features. However IS-IS is less chatty and can scale to support larger networks. Given the same set of resources, IS-IS can support more routers in an area than OSPF. This has contributed to IS-IS as an ISP-scale protocol.

#### **Performance metrics**

The IS-IS routing protocol is a link-state protocol, as opposed to distance-vector protocols such as Interior Gateway Routing Protocol (IGRP) and Routing Information Protocol (RIP). Linkstate offers several advantages over distance-vector protocols. It is faster converging, supports much larger internetworks, and is less susceptible to routing loops. Features of IS-IS include:

- Hierarchical routing
- Classless behavior
- Rapid flooding of new information
- Fast Convergence
- Very scalable
- Flexible timer tuning

IS IS uses the following metrics for its routing operations:

- Default metric (required): cost—No automatic calculation of the metric for IS-IS takes place, compared to some routing protocols that calculate the link metric automatically based on bandwidth (OSPF) or bandwidth/delay (EIGRP). Using narrow metrics (the default), an interface cost is between 1 and 63 (a 6-bit metric value). All links use the metric of 10 by default. The total cost to a destination is the sum of the costs on all outgoing interfaces along a particular path from the source to the destination, and the least-cost paths are preferred.
- Delay, expense, and error (optional)—these metrics are intended for use in type of service (ToS) routing. These could be used to calculate alternative routes referring to the DTR (delay, throughput, and reliability) bits in the IP ToS field.

#### Traces

Time	Source	Destination	Proto	ocol Info				
1 0.000000	Cisco_96:f2:c0		P/PAgP/UDLD CDP		ID: Router		ID: FastEthernet0/0	
2 1.264186	Cisco_96:f2:c0	ISIS-all-l	evel-1-IS's ISIS	S L1 HEL	🚽 0.0 kbps 1	0.0 kbps	.0000.0001	
3 2.047603	Cisco_96:f2:c0	Cisco_96:f						
4 4.652176	<pre>Cisco_96:f2:c0</pre>	ISIS-all-l	evel-2-IS'S ISIS	S L2 HEL	LO, System-	ID: 0000	.0000.0001	
5 10.112093	Cisco_96:f2:c0	ISIS-all-l	evel-1-IS'S ISIS	S L1 HEL	LO, System-	ID: 0000	.0000.0001	
6 12.047561	Cisco_96:f2:c0	Cisco_96:f	2:c0 L00	P Reply				
7 13.380026	Cisco_96:f2:c0	ISIS-all-l	evel-2-IS'S ISIS	S L2 HEL	LO, System-	ID: 0000	.0000.0001	
8 19.915987	<pre>Cisco_96:f2:c0</pre>	ISIS-all-l	evel-1-IS'S ISIS	S L1 HEL	LO, System-	ID: 0000	.0000.0001	
9 21.431962	<pre>Cisco_96:f2:c0</pre>	ISIS-all-l	evel-2-IS'S ISIS	S L2 HEL	LO, System-	ID: 0000	.0000.0001	
10 22.047397	Cisco_96:f2:c0	Cisco_96:f	2:c0 L00	P Reply				
11 29.155904	<pre>Cisco_96:f2:c0</pre>	ISIS-all-l	evel-1-IS'S ISIS	S L1 HEL	LO, System-	ID: 0000	.0000.0001	
12 29.940050	<pre>Cisco_96:f2:c0</pre>	ISIS-all-l	evel-2-IS'S ISI	S L2 HEL	LO, System-	ID: 0000	.0000.0001	
13 32.047341	Cisco_96:f2:c0	Cisco_96:f	2:c0 L00	P Reply				
14 37.491824	<pre>cisco_96:f2:c0</pre>	ISIS-all-l	evel-2-IS'S ISIS	S L2 HEL	LO, System-	ID: 0000	.0000.0001	
15 38.715801	cisco_96:f2:c0	ISIS-all-l	evel-1-IS'S ISIS	S L1 HEL	LO, System-	ID: 0000	.0000.0001	
16 42.047224	cisco_96:f2:c0	Cisco_96:f	2:c0 L00	P Reply				
17 46.379746	Cisco_96:f2:c0	ISIS-all-l	evel-1-IS'S ISIS	S L1 HEL	LO, System-	ID: 0000	.0000.0001	
18 47.179762	<pre>cisco_96:f2:c0</pre>	ISIS-all-l	evel-2-IS'S ISIS	S L2 HEL	LO, System-	ID: 0000	.0000.0001	
19 52.047181	cisco_96:f2:c0	cisco_96:f	2:c0 LOOF	P Reply				
20 54.863642	cisco_96:f2:c0	ISIS-all-l	evel-2-IS'S ISIS	S L2 HEL	LO, System-	ID: 0000	.0000.0001	
21 56.203630	<pre>cisco_96:f2:c0</pre>	ISIS-all-l	evel-1-IS'S ISIS	S L1 HEL	LO, System-	ID: 0000	.0000.0001	
22 59.999406	Cisco_96:f2:c0	CDP/VTP/DT	P/PAgP/UDLD CDP	Device	ID: Router	_A Port	ID: FastEthernet0/0	
23 62.046993	<pre>cisco_96:f2:c0</pre>	Cisco_96:f	2:c0 L00	P Reply				
24 64.643560	<pre>cisco_96:f2:c0</pre>	ISIS-all-l	evel-2-IS'S ISIS	S L2 HEL	LO, System-	ID: 0000	.0000.0001	
25 65.939670	<pre>cisco_96:f2:c0</pre>	ISIS-all-l	evel-1-IS'S ISIS	S L1 HEL	LO, System-	ID: 0000	.0000.0001	
26 72.046979	cisco_96:f2:c0	cisco_96:f	2:c0 LOOF	P Reply				
27 72.795462	cisco_96:f2:c0	ISIS-all-l	evel-2-IS'S ISIS	S L2 HEL	LO, System-	ID: 0000	.0000.0001	
28 74.395416	Cisco_96:f2:c0	ISIS-all-l	evel-1-IS'S ISIS	S L1 HEL	LO, System-	ID: 0000	.0000.0001	
29 82.046788	<pre>cisco_96:f2:c0</pre>	cisco_96:f	2:c0 LOOF	P Reply				
30 82.099371	cisco 96:f2:c0	ISIS-all-l	evel-2-IS'S ISIS	S L2 HEL	LO. Svstem-	ID: 0000	.0000.0001	
Time Sourc	e Destination	Protocol	Info					
90 180.192842 ciso	co_c0:16:78 ISIS-all-lev	el-2-IS'S ISIS	L2 HELLO System-TD.					
91 180.346392 ciso 92 180.888643 ciso			L2 HEL 🛃 0.4kbps 🏦 0.0k		Soquence: 0x0	0000005 Lif	otimo: 1100c	
93 180.905943 Cisc			L2 LSP, LSP-ID: 0000.0					G
94 181.849292 Cisc			L1 HELLO, System-ID:	0000.0000.0004				Ŀ
95 182.045811 cisc 96 183.092857 cisc			Reply L2 HELLO, System-ID: (	0000 0000 0004				
97 185.064904 ciso	co_c0:16:78 ISIS-all-lev	el-1-IS'S ISIS	L1 HELLO, System-ID: (	0000.0000.0004				
98 185.868696 Cisc					0, Start LSP-ID	: 0000.0000.	0000.00-00, End LSP-ID: ffff.ff	ĉf.
99 186.020978 ciso 100 186.568723 ciso			L2 HELLO, System-ID: ( L1 CSNP, Source-ID: ()		0, Start LSP-ID	: 0000.0000.	0000.00-00, End LSP-ID: ffff.ff	Ff.
101 188.332926 Cisc	co_c0:16:78 ISIS-all-lev	el-1-IS'S ISIS	L1 HELLO, System-ID: (	0000.0000.0004				
102 188.590322 ciso 103 188.726292 ciso			L2 HELLO, System-ID: ( L1 HELLO, System-ID: (					
104 189.224917 ciso	co_c0:16:78 ISIS-all-lev	el-2-IS'S ISIS	L2 HELLO, System-ID: (	0000.0000.0004				
105 191.468980 Ciso	co_c0:16:78 ISIS-all-lev	el-1-IS'S ISIS	L1 HELLO, System-ID:					
106 192.045773 cisc 107 192.544903 cisc			Reply L2 HELLO, System-ID: (	0000,0000,0004				
108 194.484929 ciso	co_c0:16:78 ISIS-all-lev	el-1-IS'S ISIS	L1 HELLO, System-ID: (	0000.0000.0004				
109 194.761192 ciso 110 195.120917 ciso			L2 CSNP, Source-ID: 0 L2 HELLO, System-ID:		00, Start LSP-ID	: 0000.0000.	0000.00-00, End LSP-ID: fff.ff	f.
TTO TAD'TTOAT\ C120								

105 191.468980	C15C0_C0:16:/8	ISIS-all-level-1-IS's	ISIS	L1 HELLO, System-ID: 0000.0000.0004
106 192.045773	cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
107 192.544903	cisco_c0:16:78	ISIS-all-level-2-IS's	ISIS	L2 HELLO, System-ID: 0000.0000.0004
108 194.484929	cisco_c0:16:78	ISIS-all-level-1-IS's	ISIS	L1 HELLO, System-ID: 0000.0000.0004
109 194.761192	cisco_c0:16:78	ISIS-all-level-2-IS's	ISIS	L2 CSNP, Source-ID: 0000.0000.0004.00, Start LSP-ID: 0000.0000.0
110 195.120917	cisco_c0:16:78	ISIS-all-level-2-IS's	ISIS	L2 HELLO, System-ID: 0000.0000.0004
111 195.355100	192.168.3.2	224.0.0.22	IGMP	V3 Membership Report / Leave group 224.0.0.252
112 195.393543	compalco_b3:c4:ab	Broadcast	ARP	who has 192.168.3.1? Tell 192.168.3.2
113 195.397190	192.168.3.2	224.0.0.22	IGMP	V3 Membership Report / Join group 224.0.0.252 for any sources
114 195.397570	192.168.3.2	224.0.0.22	IGMP	V3 Membership Report / Leave group 224.0.0.252
115 195.429978	192.168.3.2	224.0.0.22	IGMP	V3 Membership Report / Join group 224.0.0.252 for any sources
116 195.432474	192.168.3.2	224.0.0.252	LLMNR	Standard query ANY PHM780
117 195.465378	192.168.3.2	224.0.0.22	IGMP	V3 Membership Report / Join group 224.0.0.252 for any sources
118 195.532376	192.168.3.2	224.0.0.252	LLMNR	Standard query ANY PHM780
119 195 725979	compalco_b3:c4:ab	Broadcast	ARP	Who has 192 168 3 17 Tell 192 168 3 2

#### Analysis

The screen capture of the IS IS traces shows the exchange of the Hello packets in the process of forming adjacencies. The overhead involved in establishing the adjacencies and sharing the updates is part of the design of IS IS. The performance of the protocol may be improved by adopting the IS IS configuration best practices, and setting the update intervals in a way that does not compromise the integrity of the routing information.

#### BGP

#### **Overview**

The Border Gateway Protocol (BGP) is an exterior gateway protocol classified as a path vector routing protocol. It is the protocol used in the Internet backbone/core, and uses different set of criteria than interior gateway protocols to select routes including but not limited to path, routing policies and rules. Most Internet service providers must use BGP to establish routing between one another (especially if they are multi-homed). Therefore, even though most Internet users do not use it directly, BGP is one of the most important protocols of the Internet.

BGP neighbors, peers are established by manual configuration between routers to create a TCP session on port 179. A BGP speaker will periodically send 19-byte keep-alive messages to maintain the connection (every 60 seconds by default). Among routing protocols, BGP is unique in using TCP as its transport protocol. A BGP-enabled router uses a simple finite state machine to make its peering decisions with its neighbors.

#### Performance metrics and issues

#### Internal BGP scalability

An autonomous system with internal BGP (IBGP) must have all of its IBGP peers connect to each other in a full mesh (where everyone speaks to everyone directly). This full-mesh configuration requires that each router maintain a session to every other router. In large networks, this number of sessions may degrade performance of routers, due either to a lack of memory, or too much CPU process requirements.

Route reflectors and confederations both reduce the number of IBGP peers to each router and thus reduce processing overhead. Route reflectors are a pure performance-enhancing technique, while confederations also can be used to implement more fine-grained policy.

Route reflectors reduce the number of connections required in an AS. A single router (or two for redundancy) can be made a route reflector: other routers in the AS need only be configured as peers to them.

Confederations are sets of autonomous systems. In common practice, only one of the confederation AS numbers is seen by the Internet as a whole. Confederations are used in very large networks where a large AS can be configured to encompass smaller more manageable internal ASs.

Confederations can be used in conjunction with route reflectors. Both confederations and route reflectors can be subject to persistent oscillation unless specific design rules, affecting both BGP and the interior routing protocol, are followed.

However, these alternatives can introduce problems of their own, including the following:

- route oscillation
- sub-optimal routing
- increase of BGP convergence time

Additionally, route reflectors and BGP confederations were not designed to ease BGP router configuration. Nevertheless, these are common tools for experienced BGP network architects. These tools may be combined, for example, as a hierarchy of route reflectors.

#### Instability

The routing tables managed by a BGP implementation are adjusted continually to reflect actual changes in the network, such as links breaking and being restored or routers going down and coming back up. In the network as a whole it is normal for these changes to happen almost continuously, but for any particular router or link changes are supposed to be relatively infrequent. If a router is misconfigured or mismanaged then it may get into a rapid cycle between down and up states. This pattern of repeated withdrawal and re-announcement, known as route flapping, can cause excessive activity in all the other routers that know about the broken link, as the same route is continuously injected and withdrawn from the routing tables. The BGP design is such that delivery of traffic may not function while routes are being updated. On the Internet, a BGP routing change may cause outages for several minutes.

• Complexity (as compared to other protocols), overhead, convergence times, security.

- path attributes describe the characteristics of paths, and are used in the process of route selection
- Metrics to calculate shortest path
- Message types, Transport protocol (TCP), port number
- Fast Convergence time, timers
- Reliability (Routing loops)

#### Traces

276 1506.15603 Cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         275 1516.15643 Cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         276 1516.1563 Cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         285 1516.15644 Cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         286 1531.57084 Cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         286 1531.57113 10.0.0.14       10.0.0.14       TCP       bgp > 28621 Supg [StN] Seq.0 Ark-1 win-L6384 Len-0         286 1531.57314 10.0.0.13       10.0.0.14       TCP       bgp > 28621 Supg [StN] Seq.0 Ark-1 win-L6384 Len-0         286 1531.55315 10.0.0.14       10.0.0.13       BOP       PUPNITE Message       WDATE Message         287 15315 10.0.0.13       10.0.0.14       TCP       PUPNITE Message       WDATE Message         286 1531.15521 Cisco_96:f2:c0       COP/VTP//PAP/VUDL COP       Device 1D: Router_A Port.10: FastEthernet0/0       28621 Supg [StS1       Conton-16125 Len-0         271 1538.90287 10.0.0.13       10.0.0.14       BOP       WDATE Message       WDATE Message       WDATE Message         271 1538.90287 10.0.0.14       10.0.0.13       TCP       MDATE Message       VEACK Seq.96 72:CO       LOOP         271 1538.90281 10.0.0.13       10.0.0.14       BOP	Time	Source	Destination	Protocol	Info
275 1316.1364.25 C (150.0.96:17:00       C (150.0.96:17:00       L 000 P Ref)       D 0.0.043         253 1356.1364.12 C (150.0.96:17:00       C (150.0.96:17:00       C (150.0.96:17:00       C (150.0.96:17:00         253 1356.1364.12 C (150.0.96:17:00       100.0.0.14       TCP       260.1 > bigs (150.1) Scient Min-10:354.1400         253 135.5731.17 10.0.0.13       100.0.0.14       TCP       260.1 > bigs (150.0.96:17.100       D (150.0.14         263 135.5731.17 10.0.0.13       100.0.0.14       BCP       OPEN MESSage       D (150.0.17.100       D (150.0.17.100         263 135.1.5731.10 0.0.0.13       100.0.0.14       BCP       OPEN MESSage       D (150.0.17.100       D (150.0.17.100         263 135.1.5731.10 0.0.0.13       100.0.0.14       BCP       OPEN MESSage       D (150.0.17.100       D (150.0.17.100         263 135.1.5731.10 0.0.0.13       100.0.0.14       BCP       OPEN MESSage       UPDATE MESSage       D (150.0.17.100       D (150.0.17.100         273 1353.90033.1 (150.0.96:17:00       C (150.0.96:17:00       C (150.0.96:17:00       D (170.0.17.100       D (150.0.11.100       D (150.0.11.					
258 1256.136414 Cisco_09:f2:c0       Cisco_00:f2:c0       Loop       rep1/         269 1333.05098 100.01.41       100.0.014       TCP       260:131.010.013       Loop         260 133.07098 100.01.41       100.0.014       TCP       260:131.010.013       Loop         261 133.07098 100.01.41       100.0.014       TCP       260:131.010.013       Loop         263 133.07093 100.00.141       100.0.013       ECP       260:131.000.013       Loop         263 133.010.00.131       100.0.014       ECP       260:131.000.013       Loop       Loop         263 133.010.00.131       100.0.0.13       ECP       Loop       Loop <t< td=""><td></td><td></td><td></td><td></td><td></td></t<>					
239       133.155387       10.0.0.13       10.0.0.14       TCP       25621       Stag. Cost, Seq0. Acc.1. win-16384 Lem-0. MSS-1460         261       133.157113       10.0.0.13       10.0.0.14       TCP       2622.1       Stag. Cost, Seq1. Acc.1. win-16384 Lem-0. MSS-1460         261       133.157113       10.0.0.13       10.0.0.14       TCP       262.1       Stag. Cost, Seq1. Acc.1. win-16384 Lem-0. MSS-1460         261       133.157113       10.0.0.14       10.0.0.14       TCP       262.1       Nin. Acc.1. Win-16384 Lem-0. MSS-1460         261       133.157113       10.0.0.14       TCP       262.1       Nin. Acc.1. Win-16384 Lem-0. MSS-1460         261       133.157114       10.0.0.13       TCP       266.1       Stag. MSS-10.0.0.14       TCP         261       133.157114       10.0.0.14       TCP       PCR       PCR       PCR       PCR         271       133.9       10.0.0.14       TCP       PCR					
260 1331.570688 10.0.0.14       10.0.0.13       TCP       bgp > 28621 [SVN, ACK) Seq1 AC-L win-16384 Lem-0         261 331.572113 10.0.0.13       10.0.0.14       FCP       26821 > bgp [ACK] Seq1 AC-L win-16384 Lem-0         262 133.57213 10.0.0.14       10.0.0.13       60.0.14       60.0.14         263 133.57213 10.0.0.14       10.0.0.13       60.0.14       60.0.14         263 133.57213 10.0.0.14       10.0.0.13       60.0.14       60.0.14         263 133.57213 10.0.0.13       10.0.0.13       60.0.0.14       60.0.14         264 1333.1000 (Sig. Cap.672:0)       CDP/VTP/CPP/App/UDD COP       Dev/Ce 10. Bouter A Fort 10: FastEthernet0/0         266 1333.00393 Cisc06:72:0       CDP/VTP/CPP/App/UDD COP       Dev/Ce 10: Bouter A Fort 10: FastEthernet0/0         267 1333.75141 10.0.0.13       10.0.0.0.13       BOP       UPNATE Message, UPAATE Message       UPAATE Message         273 1333.003093 Cisc06:72:0       10.0.0.0.13       BOP       UPNATE Message, MERALIVE Message       UPDATE Message         273 1335.01030 10.0.0.14       10.0.0.0.13       BOP       UPNATE Message, MERALIVE Message       UPAATE Message         273 1335.01030 10.0.0.14       10.0.0.0.13       BOP       UPDATE Message       Win-16051 Lem-0         274 1354.0102 10.0.0.0.14       10.0.0.0.13       BOP       EEPALIVE Message <t< td=""><td></td><td></td><td></td><td></td><td></td></t<>					
761       133.57113       10.0.0.13       10.0.0.0.14       TC       72623 > bgp [ArX] Seq1.4.KS.3       Seq1.2.KS.3					
762 133.572117 10.0.0.0.13       10.0.0.14       BGF       OPEN MESSage.         763 133.572417 10.0.0.13       10.0.0.14       BGF       OPEN MESSage. KEEPALTVE MESSage         764 133.1.57841 10.0.0.13       10.0.0.14       BGF       OPEN MESSage. KEEPALTVE MESSage         764 133.1.57843 10.0.0.13       10.0.0.14       BGF       OPEN MESSage. KEEPALTVE MESSage         764 133.3.57211 10.0.0.13       10.0.0.14       BGF       OPEN MESSage. KEEPALTVE MESSage         764 133.3.670311 10.0.0.13       10.0.0.14       BGF       OPENT MESSage.       DPATE MESSage         771 133.80037 10.0.0.13       10.0.0.14       BGF       UPDATE MESSage.       UPDATE MESSage.       UPDATE MESSage         771 133.80037 10.0.0.13       10.0.0.13       TGF       MSG       MSG       MSG       MSG         771 133.80037 10.0.0.14       10.0.0.13       TGF       MSG					
263       263       253       2					
764 1531.578926 10.0.0.13       10.0.0.14       BOP       KEEPALTUE Message       UPDATE Message, UPDATE Me					
265       100.0.0.14       10.0.0.13       BCP       UPDATE MESSAGE, UPDAT					
266 1531.08.0337 10.0.0.13       10.0.0.14       TCP       28621 > bgp [AcX] seque50 xkc302 win=16083 Lin=0         266 1533.09.039 Cisc.0.96:f2:c0       Clx/CP/TD/PT/PA/DV/DUDC CDP       Perkic 1D: Router_A Port DD: FastEthernet/0         268 1533.09.039 Cisc.0.96:f2:c0       Clx/CP/TD/PT/PA/DV/DV/DV/DV/DV/DV/DV/DV/DV/DV/DV/DV/DV/	264 1531.578	926 10.0.0.13	10.0.0.14	BGP	KEEPALIVE Message
267       1333.900394       CTP./TP./PARP/UDL CDP       Dev/ce TD: Router_A Port ID: FastEthernet0/0         268       1333.75811       10.0.0.13       10.0.0.14       DOP         270       1339.78181       10.0.0.13       10.0.0.14       DOP         271       1339.78181       10.0.0.14       DOP       UPDATE Message.       DOPATE Message         271       1339.78181       10.0.0.14       10.0.0.13       TCP       DSP 2621       [AcX] Seque 202 Ack-200 win-16125 Len-0         271       1339.78181       10.0.0.14       10.0.0.13       DOP       WPDATE Message       REPALVE Message       REPALVE Message         273       1336.15017       Cisco_96172:00       Cisco_96172:00       LOP       Reply         275       1535.50163       10.0.0.14       TCP       SEC1 > DSP [Ack] Seque320 Ack-220 win-16056 Len-0         276       1566.156027       Cisco_96172:00       LOP       Reply         276       1566.156027       Cisco_96172:00       LOP       Reply         280       1358.5031610.0.0.13       DO       DO       Reply         281       1359.50128       DO       Cisco_96172:00       LOP       Reply         281       1359.501728       DO       DO       DO	265 1531.682	734 10.0.0.14	10.0.0.13	BGP	UPDATE Message, UPDATE Message, UPDATE Message, UPDATE Message, KEEPALIVE Message, KEEPA
271       1333, 000593 (15cc.0, 96:12:c0       COP/VTP//DTP/AgAP/LOLD COP 280 1333, 76821 (15c.0, 96:12:c0       LCOP/VTP/COP/LOP/COP 280 1333, 76821 (15c.0, 96:12:c0       LCOP/VTP/COP/LOP/COP 270 1339, 46823 (15c.0, 96:12:c0       LCOP/VTP/COP 270 1359, 46823 (15c.0, 96:12:c0       LCOP 270 1358, 40153 (15c.0, 96:12:c0       LCOP 270 1357, 41538 (15c.0, 96:12:c0       LCOP 2	266 1531.881	337 10.0.0.13	10.0.0.14	ТСР	28621 > bgp [ACK] Sea=65 Ack=302 win=16083 Len=0
268 1336.15629 (1sco_96:f2:c0       LOOP       Reply         270 1339.85129 10.0.0.13       10.0.0.14       BOP       UPDATE Message, UPDATE Message         270 1339.85129 10.0.0.13       10.0.0.14       BOP       UPDATE Message, UPDATE Message         271 1339.85129 10.0.0.14       10.0.0.13       10.0.0.14       BOP         271 1339.8513 10.0.0.14       10.0.0.13       TCP       Bop > 2861 [AcK] Seq=302 Ack-200 win=16057 Len=0         271 1340.1503 (15co_95:f2:c0       Clsco_95:f2:c0       LOOP       Reply         271 1353.8502 (15co_95:f2:c0       Clsco_95:f2:c0       LOOP       Reply         271 1353.61058 10.0.0.0.13       10.0.0.0.14       TCP       2561 > bpg [AcK] seq=302 Ack=209 win=16056 Len=0         277 1355.10158 10.0.0.0.14       10.0.0.0.14       TCP       25621 > bpg [AcK] seq=298 Ack=329 win=16056 Len=0         277 1355.10158 10.0.0.0.13       10.0.0.0.14       TCP       2561 > bpg [AcK] seq=202 Ack=329 win=16056 Len=0         278 1356.1538 11 (sco_95:f2:c0       Clsco_95:f2:c0       LOOP       Reply         281 1392.30156 10.0.0.13       10.0.0.14       TCP       2561 > bgg [AcK] seq=317 Ack-348 win=16057 Len=0         281 1392.30158 10.0.0.14       10.0.0.14       BCP       VEEPALTVE Message         281 1392.30158 10.0.0.14       10.0.0.14       BCP       VEEPALTVE Me			CDP/VTP/DTP/PAgP/	UDLD CDP	
269 1339, 78181 10.0.0.13       10.0.0.14       BOP       UPDATE Message, UPDATE Message         271 1338, 980287 10.0.0.14       10.0.0.13       TCP       bgp > 28621 [AcK] Seq=302 Ack=260 win=16125 Len-0         272 1339, 980287 10.0.0.14       10.0.0.13       TCP       bgp > 28621 [AcK] Seq=302 Ack=260 win=16087 Len-0         273 1330, 1557 (550.96;f2:0)       Cisco.96;f2:0       Lioco.95;f2:0       Lioco.95;f2:0       Cisco.96;f2:0         273 1356, 15502 (fisco.96;f2:0)       Cisco.96;f2:0       Liop Reply       Reply       Reply         273 1356, 155102 (fisco.96;f2:0)       Cisco.96;f2:0       Liop Reply       Reply       Reply         273 1556, 15512 (fisco.96;f2:0)       Cisco.96;f2:0       Liop Reply       Reply       Reply         273 1556, 15512 (fisco.96;f2:0)       Cisco.96;f2:0       Liop Reply       Reply       Reply         281 1592, 20238 (fisco.96;f2:0)       Cisco.96;f2:0       Liop Reply       Reply       Reply         281 1592, 20238 (fisco.96;f2:0)       Cisco.96;f2:0       Liop Reply       Reply </td <td></td> <td></td> <td></td> <td></td> <td></td>					
270 1339. 881/24 10. 0. 0. 1.1       10. 0. 0. 1.4       100. 0. 0. 1.3       TCP         271 1339. 881/24 10. 0. 0. 1.1       10. 0. 0. 1.1       TCP       bgp > 2862/1 [ACK] Seg=302 ACK=260 Win=16125 Lem=0         272 1339. 881/91 10. 0. 0. 1.3       10. 0. 0. 1.3       TCP       bgp > 2862/1 [ACK] Seg=302 ACK=260 Win=16025 Lem=0         274 1350. 880/00 10. 0. 0. 1.4       10. 0. 0. 1.3       TCP       bgp > 2862/1 [ACK] Seg=302 ACK=280 Win=16057 Lem=0         274 1354. 156137 Cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         275 13556. 15602 Cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         276 1358. 70163 10. 0. 0.14       10. 0. 0.14       TCP       2862/1 Seg=298 ACK=329 Win=16056 Len=0         277 1356. 15602 Cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         280 1356. 15830 Cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         281 1359. 20131 01 00. 0. 0.14       10. 0. 0.14       GGP       KEEPALIVE Message         281 1359. 20131 01 00. 0. 0.14       10. 0. 0.14       GGP       KEEPALIVE Message         281 1359. 20130 01 0. 0. 14       10. 0. 0.14       GGP       KEEPALIVE Message         281 1359. 20130 01 0. 0. 14       10. 0. 0.14       GGP       KEEPALIVE Message         281 1359. 20130 01 0. 0. 14       10. 0. 0.14 </td <td></td> <td></td> <td></td> <td></td> <td></td>					
271 1339. 80287 10.0.0.14 10.0.0.13 172 bg > 28621 [ACK] Seq=302 ACk=20 Win=16125 Lemo 272 1339. 80127 10.0.0.13 10.0.0.13 10.0.0.13 10.0.0.13 10.0.0.14 10.0.0.13 172 bg > 28621 [ACK] Seq=302 ACk=208 Win=16125 Lemo 273 1340. 186005 10.0.0.14 10.0.0.13 174 bg > 28621 [ACK] Seq=302 ACk=208 Win=16087 Lemo 274 1346. 158157 Cisco_96f72:0 Ci					
272 1339.981191 10.0.0.13       10.0.0.14       DGP       KEEPALTVE Message         273 1540.156157 Cisco_96;f2:c0       Cisco_96;f2:c0       LOOP       Reply         274 1550.156157 Cisco_96;f2:c0       Cisco_96;f2:c0       LOOP       Reply         275 1556.156157 Cisco_96;f2:c0       Cisco_96;f2:c0       LOOP       Reply         276 1556.156127 Cisco_96;f2:c0       Cisco_96;f2:c0       LOOP       Reply         278 1556.15602 Cisco_96;f2:c0       Cisco_96;f2:c0       LOOP       Reply         278 1556.15602 Cisco_96;f2:c0       Cisco_96;f2:c0       LOOP       Reply         280 1586.15587 Cisco_96;f2:c0       Cisco_96;f2:c0       LOOP       Reply         281 1592.30235 10.0.0.14       10.0.0.14       BGP       WPATE Message         281 1592.30256 10.0.0.14       10.0.0.14       BGP       KEEPALIVE Message         281 1592.30256 10.0.0.14       10.0.0.14       BGP       KEEPALIVE Message         281 1592.30258 10.0.0.14       10.0.0.14       BGP       KEEPALIVE Message         281 1592.30256 10.0.0.14       10.0.0.14       BGP       KEEPALIVE Message         281 1767.30386 Cisco_96;f2:c0       Cisco_96;f2:c0       LOOP       Reply         281 1767.30397 10.0.0.14       255.255.255.255       DNS       Standard query PR 1.4.168.19					
273 1540.180405 10.0.0.14       10.0.0.13       TCP       bdp > 28621 [ACC] Seq=302 ACC=298 win=16087 Len=0         274 1546.156137 (510.0.96;f2:c0       Cisco_96;f2:c0       LOOP       Reply         275 1556.156102 (510.0.96;f2:c0       Cisco_96;f2:c0       LOOP       Reply         275 1556.156102 (510.0.96;f2:c0       Cisco_96;f2:c0       LOOP       Reply         275 1556.156102 (510.0.96;f2:c0       Cisco_96;f2:c0       LOOP       Reply         275 1556.15587 6 (510.0.96;f2:c0       Cisco_96;f2:c0       LOOP       Reply         281 1592.302381 0.0.0.13       10.0.0.14       BGP       KEEPALTVE Message         281 1592.30238 10.0.0.13       10.0.0.14       TCP       28621 > bgp [ACK] Seq=317 AcK=348 win=16037 Len=0         281 1592.30238 10.0.0.14       10.0.0.14       TCP       28621 > bgp [ACK] Seq=317 AcK=348 win=16037 Len=0         281 1592.30238 10.0.0.14       250.0.96;f2:c0       LOOP Device 10: Router A Port 10: FastEthernet0/0         1mm       Sware       Detination       Protoci       Inf       Sagaa         11 261.15388 cisco_96;f2:c0       Cico_96;f2:c0       LOOP       Reply       Standard query PTR 1.4.166.192, in-addr.arpa         151 276.15386 cisco_96;f2:c0       Cico_96;f2:c0       LOOP       Reply       Standard query PTR 2.0.0.10.1.n-addr.arpa         152					
274       1546.156137 C1502.965(72:00       C1552.995(72:00       LOOP       Reply         275       1555.156102 C1552.965(72:00       C1552.995(72:00       LOOP       Reply         276       1556.15602 C1552.965(72:00       C1552.995(72:00       LOOP       Reply         275       1556.156022 C1552.965(72:00       C1552.995(72:00       LOOP       Reply         278       1556.15582 C1552.965(72:00       C1552.995(72:00       LOOP       Reply         281       1552.301816 10:0.0.13       10:0.0.14       BGP       KEEPALTVE Message         281       1552.301816 10:0.0.13       10:0.0.14       BGP       KEEPALTVE Message         281       1552.301816 10:0.0.13       10:0.0.14       T0       286(72:00       LOOP       Reply         284       1592.30233 10:0.0.13       10:0.0.14       T0       285(72:00       LOOP       Reply					
275       1556.156102 cisco_96:f2:c0       LOOP       Reply         277       1558.40308 10.0.0.14       10.0.0.13       BCP       UPDATE Message         277       1558.10502 cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         278       1556.155876 cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         281       1558.15581 cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         281       1592.301810 10.0.0.13       10.0.0.14       BCP       KEEPALIVE Message         281       1592.302381 10.0.0.14       10.0.0.14       BCP       KEEPALIVE Message         281       1592.302381 10.0.0.14       10.0.0.14       TCP       286C1 > bpg f.ckl 59c-917 Ack = 348 win=16037 Len=0         281       1593.2558 cisco.96:f2:c0       COP /TP/TP/PAP/UDL COP       Device 10: Router A Port 10: FastEthernet0/0         1mm       Survet       Pethoden       Protoci       Info         15126.15388 cisco.96:f2:c0       Cisco.96:f2:c0       Loop       Reply         351278.730897 10.0.0.14       255.255.255       DNS       Standard query PTR 1.4.166.192.fn-addr.arpa         351278.730897 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.1n-addr.arpa         351279.730410 10.0.0.14       255.255					
276 1558.201163 10.0.0.14       10.0.0.13       DCP       UPDATE Message         277 1558.401163 10.0.0.13       10.0.0.14       TCP       2860.15022 C1sco_96:f2:c0       C1sco_96:f2:c0         278 1556.15576 c1sco_96:f2:c0       C1sco_96:f2:c0       LOOP       Reply         281 1592.30253 10.0.0.13       10.0.0.13       DCP       KEFPALTVE Message         281 1592.30253 10.0.0.13       10.0.0.13       DCP       KEFPALTVE Message         281 1592.30253 10.0.0.13       10.0.0.14       TCP       2861.1523       Seq=317 Ack=348 win=16037 Len=0         281 1592.302553 10.0.0.13       10.0.0.14       TCP       2861.1523       Seq=317 Ack=348 win=16037 Len=0         281 1592.30256 C1sco_96:f2:c0       CCP/VTP/OTP/PAAP/UDLD CCP       Device 10: Router A Port ID: FastEthernet0/0         Imme       Source       Detmation       Protocol       Into         350 1276.13356 C1sco_96:f2:c0       CCDP/VTP/OTP/PAAP       Seq=317 Ack=348 win=16037 Len=0         351 1276.13358 C1sco_96:f2:c0       CCDP/VTP/OTP/PAAP       Reply         351 1276.73397 10.0.0.14       255.255.255.255       DNS       Standard query PTR 1.4.168.192.1n=addr.arpa         351 1276.73097 10.0.0.14       255.255.255.255       DNS       Standard query PTR 2.0.0.10.1n=addr.arpa         357 1276.75017 10.0.0.14       255.255.255.255 </td <td></td> <td></td> <td></td> <td></td> <td></td>					
277       1558.401308 10.0.0.12       10.0.0.14       TCP       28621 > bgp (ACK) Seq=298 AcK=329 win=16056 Len=0         278       1566.15602 c1(sc.0.966f2:c0       C1(sc.0.96f2:c0       LOOP       Reply         280       1586.15587 c1(sc.0.96f2:c0       C1(sc.0.96f2:c0       LOOP       Reply         281       1592.301816 510.0.0.13       10.0.0.14       BCP       KEEPALTVE Message         283       1592.301816 510.0.0.13       10.0.0.14       ECP       KEEPALTVE Message         284       1592.301816 510.0.0.13       10.0.0.14       TCP       28621 > bgp (ACK) Seq=317 AcK=348 win=16037 Len=0         284       1593.89997 c1/sco.96f2:c0       C1(sc.0.96f2:c0       LOP Reply         1me       Source       Detination       Protocl Inte       Source       Detination         349       1776.153956 c1/sco.96f2:c0       C1(sc.0.96f2:c0       LOP Reply       Source       Sour					
277 1558.403308 10.0.0.13       100.0.0.14       TCP       28621 > bpp [ACK] Seq=298 ACK=329 win=16056 Len=0         278 1566.15602 cisc_0.6672:00       Cisc_0.96:f2:00       LOOP       Reply         280 1586.155876 cisc_0.96:f2:00       LOOP       Reply         281 1592.301816 10.0.0.13       10.0.0.14       BGP       KEEPALTVE Message         281 1592.301816 10.0.0.14       10.0.0.14       BGP       KEEPALTVE Message         283 1592.301816 10.0.0.13       10.0.0.14       TCP       28621 > bpg [ACK] Seq=317 Ack=348 win=16037 Len=0         284 1593.89977 cisco 96:f2:c0       CDP/VTP/DTP/ADP/UDLD CDP       Device ID: Router A Port ID: FastEthernet0/0         Imm       Source       Uestination       Protocol       Inte         349 1776.153956 cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         351 1786.15388 cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         351 1796.75397 10.0.0.14       255.255.255       DNS       Standard query PTR 1.4.168.192; in-addr.arpa         351 1796.75397 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10. in-addr.arpa         351 1796.750170 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10. in-addr.arpa         351 1796.750170 10.0.0.14       255.255.255       DNS       Standard query P	276 1558.201	163 10.0.0.14	10.0.0.13	BGP	UPDATE Message
278 1566.156022 (sico_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         278 1576.155876 (sico_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         281 1592.303165 10.0.0.13       10.0.0.14       BGP       KEEPALTVE Message         282 1592.303253 10.0.0.14       10.0.0.13       BGP       KEEPALTVE Message         283 1592.303253 10.0.0.13       10.0.0.14       BGP       KEEPALTVE Message         284 1593.303977 Cisco 96:f2:c0       CDP/VTP/DTP/PADP/UDD COP       Device 1D: Router A Port ID: FastEthernet0/0         10m       Source       Device 1D: Router A Port ID: FastEthernet0/0         11766.15388 (sico_96:f2:c0       CDP/VTP/DTP/PADP/UDD COP       Reply         1350 1274.723057 10.0.0.14       255.255.255.255       pss       standat 40 uery PTR 1.4.165.192.1n-addr.arpa         1351 1276.15388 (sico_96:f2:c0       Cisco_96:f2:c0       LooP       Reply         1351 1276.15388 (sico_96:f2:c0       Cisco_96:f2:c0       LooP       Perly         1351 1276.15388 (sico_96:f2:c0       Cisco_96:f2:c0       LooP       Reply         1571 757.7471010.0.0.14       255.255.255.255       pss standard query PTR 1.4.165.192.1n-addr.arpa         1571 757.7471010.0.0.14       255.255.255.255       ps standard query PTR 2.0.0.10.1n-addr.arpa         1571 757.74701010.0.0.14       255.25	277 1558.401	308 10.0.0.13	10.0.0.14	TCP	
279 1376.153876 (cisco_96:f2:c)       Cloop       Reply         281 1366.155881 (cisco_96:f2:c)       Cloop       Reply         281 1392.301816 (10.0.0.13)       10.0.0.14       BCP       KEEPALTVE Message         282 1392.30233 10.0.0.13       10.0.0.13       BCP       KEEPALTVE Message         283 1392.30233 10.0.0.14       10.0.0.0.14       TCP       28621 > Dpg [ACK] seq=17 ACK=348 win=16037 Len=0         284 1593.89977 (cisco 96:f2:c0       CDP/VTP/OTP/PAOP/UDLD CDP       Device ID: Router A Port ID: FastEthernet0/0         1mm       Source       Detination       Prodoce       Info         350 1784.728267 10.0.0.14       255.255.255 255       NS       Standard query PTR 1.4.168.192.in-addr.arpa         351 1786.153886 (cisco_96:f2:c0       Cisco_96:f2:c0       Loop       Reply         352 1787.73093 10.0.0.14       255.255.255 255       DNS       Standard query PTR 1.4.168.192.in-addr.arpa         351 1796.750170 10.0.0.14       255.255.255 255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         351 1796.750170 10.0.0.14       255.255.255 255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         351 1796.750170 10.0.0.14       255.255.255 255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         351 1995.794110 (cisco_96:f2:c0       CDP/VTP/DTP/PAOP/UDLO       DP </td <td>278 1566,156</td> <td>022 cisco_96:f2:c0</td> <td>Cisco_96:f2:c0</td> <td>LOOP</td> <td>Reply</td>	278 1566,156	022 cisco_96:f2:c0	Cisco_96:f2:c0	LOOP	Reply
280       1586       15581       15581       15581       15581       15581       15581       15581       100.0.0.13       BGP       KEEPALTVE Message         282       1592       30225       310.0.0.14       100.0.0.13       BGP       KEEPALTVE Message         283       1592       30225       310.0.0.13       10.0.0.0.14       TCP       25611 > big / Sce=217 Ack=348 win=16037 Len=0         284       1593       899977       Cisco_96:f2:c0       CDP/VTP/DTP/PACP/UDLD CDP       Device ID: ROUTE A Port ID: FastEthernet0/0         1mm       Source       Uetmaton       Protocol       Hot       Source       Cisco_96:f2:c0       Cop Reply         151       1766.15388       Cisco_96:f2:c0       Cisco_96:f2:c0       Nos       Standard query PTR 1.4.168.192.1n-addr.arpa         152       1787.730597       10.0.0.14       255.255.255.255       DNS       Standard query PTR 2.0.0.10.1n-addr.arpa         153       1797.749110       Cisco_96:f2:c0       Cisco_96:f2:c0       Dop Ver/Pr/PACPUDLD COP       Pevice ID: Router_A Port ID: FastEthernet0/0         151       1795.75917       10.0.0.14       255.255.255.255       DNS       Standard query PTR 2.0.0.10.1n-addr.arpa         153       1796.759017       10.0.0.14       255.255.255.255       DNS<					
281       1592, 301816       10.0.0.13       10.0.0.14       BGP       KEEPALTVE Message         282       1592, 501238       10.0.0.0.13       10.0.0.13       BGP       KEEPALTVE Message         284       1593, 899977       Cisco 96:f2:c0       CDP/VTP/DTP/PAGP/UDL COP       Device ID: Router A Port ID: FastEthernet0/0         Imm       Source       Uethation       Protocol       Imm       Fortice Into         350       1784, 72967       10.0.0.14       255, 255, 255, 255       DNS       Standard query PTR 1.4.168, 192, in-addr. arpa         351       1786, 15388       Cisco, 96:f2:c0       COP/VTP/DTP/AgP/UDL COP       Standard query PTR 1.4.168, 192, in-addr. arpa         351       1786, 15388       Cisco, 96:f2:c0       COP/VTP/DTP/AgP/UDL COP       Standard query PTR 1.4.168, 192, in-addr. arpa         351       1790, 720180       10.0.0.14       255, 255, 255       DNS       Standard query PTR 2.0.0.10.in-addr. arpa         351       1790, 720180       10.0.0.14       255, 255, 255       DNS       Standard query PTR 2.0.0.10.in-addr. arpa         351       1790, 720180       10.0.0.14       255, 255, 255       DNS       Standard query PTR 2.0.0.10.in-addr. arpa         351       1795, 730170       10.0.0.14       255, 255, 255       DNS       Standard query PTR					
282       1592. 30223       10.0.0.14       10.0.0.13       BCP       KEEPALIVE Message         283       1592. 50228       10.0.0.13       TCP       28621.5       bgp [AcK] Seq=37.Ack=348 win=16037_Len=0         284       1593.899977       Cisco 96:f2:c0       CDP/VTP/DTP/PAdP/UDLD CDP       Device ID: Router A Port ID: FastEthernet0/0         1me       Source       Device ID: Router A Port ID: FastEthernet0/0       Reply         349       1766.15396       Cisco_96:f2:c0       Lico_96:f2:c0       Lico_96:f2:c0       Lico         151       1786.15388       Cisco_96:f2:c0       Lico       Reply       14.168.192.in-addr.arpa         351       1796.75097       10.0.0.14       255.255.255       DNS       Standard query PTR 1.4.168.192.in-addr.arpa         351       1796.750170       10.0.0.14       255.255.255       DNS       Standard query PTR 1.4.168.192.in-addr.arpa         355       1796.750170       10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         358       109.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.0.10.in-addr.arpa         359       100.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.0.10.in-addr.arpa         359       100.0.0.13       10.0.0.14					
283       1592.501238       10.0.0.0.13       10.0.0.0.14       TCP       286/12 > bgp [AcK]       Seq=317       Ack=348 win=16037       Len-0         284       1593.899977       Cisco 96:f2:c0       CDP/VTP/DTP/PADP/VDLD COP       Device ID: Router A Port ID: FastEthernet0/0         1me       Source       Detination       Protocol       Info         349       1776.153956       Cisco.96:f2:c0       LOOP       Reply       Reply <td< td=""><td></td><td></td><td></td><td></td><td></td></td<>					
284 1593.899977 cisco 96:f2:c0         CDP/VTP/DTP/PAGP/UDLD CDP         Device ID: Router A Port ID: FastEthernet0/0           Imme         Source         Detimation         Protocol         Info           94 1776.153956 cisco_96:f2:c0         Cisco_96:f2:c0         LOOP         Reply         1 0.0014           251 1786.153888 cisco_96:f2:c0         Cisco_96:f2:c0         LOOP         Reply         1 0.0014           251 1786.153886 cisco_96:f2:c0         Cisco_96:f2:c0         Device ID: Router A Port ID: FastEthernet0/0           351 1786.153886 cisco_96:f2:c0         Cisco_96:f2:c0         Device ID: Router A Port ID: FastEthernet0/0           351 1796.750170 10.0.0.14         255.255.255.255         DNS         Standard query PTR 1.4.168.192.in-addr.arpa           355 1796.750170 10.0.0.14         255.255.255.255         DNS         Standard query PTR 2.0.0.10.in-addr.arpa           358 1799.750170 10.0.0.14         255.255.255.255         DNS         Standard query PTR 2.0.0.10.1n-addr.arpa           358 1799.750177 10.0.0.14         255.255.255.255         DNS         Standard query PTR 2.0.0.10.1n-addr.arpa           358 1809.97077 10.0.0.14         10.0.0.14         TCP         45063 S Spg [SvK] Seq=0 kin=16384 Len=0 MSS=1460           361 1804.90779 10.0.0.13         10.0.0.14         TCP         45063 S Spg [SvK] Seq=1 Ack-1 win=16384 Len=0 MSS=1460					
Imme         Source         Destination         Protocol         Info           149         1776.153956         Cisco96:f2:c0         Cisco96:f2:c0         LOOP         Reply           350         1784.732867         10.0.0.14         255.255.255.255         DNS         standaf         1.0.180p         1.0.180p <td></td> <td></td> <td></td> <td></td> <td></td>					
349 1776.153956 Cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         350 1784.729267 10.0.0.14       255.255.255       DNS       Standard query PTR 1.4.168.192.in-addr.arpa         351 1786.730587 10.0.0.14       255.255.255       DNS       Standard query PTR 1.4.168.192.in-addr.arpa         351 1786.730180 10.0.0.14       255.255.255       DNS       Standard query PTR 1.4.168.192.in-addr.arpa         355 1795.750170 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         355 1795.750170 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         356 1796.750170 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         358 1799.750177 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         359 1804.907452 10.0.0.14       10.0.0.13       TCP       bgp > 45063 SNN, AcK Seq=0 Ack=1 Win=16384 Len=0 MSS=1460         361 1804.907452 10.0.0.14       10.0.0.14       TCP       45063 > bgp [AcK] Seq=1 Ack=1 Win=16384 Len=0         361 1804.907452 10.0.0.14       10.0.0.13       BCP       PEN Message         361 1804.907452 10.0.0.14       10.0.0.13       BCP       VEDATE Message, VEDATE Message, UPDATE Message, UP	204 1093.899	977 CISCO 90:12:CO	CDP/VTP/DTP/PAdP/	UDED CDP	Device ID. Router A POrt ID: Fasternernet0/0
150       1784.729267       10.0.0.14       255.255.255       DNS       Standard <ul> <li>0.0 Hbps</li> <li>8.192. in-addr.arpa</li> </ul> 351       1786.15388       Cisco_96:f2:c0       LOOP       Reply         351       1786.15388       Cisco_96:f2:c0       LOOP       Reply         351       1790.730180       10.0.0.14       255.255.255       DNS       Standard query PTR 1.4.168.192. in-addr.arpa         351       1793.747939       10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         355       1795.750170       10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         358       1790.750170       10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         358       1790.750170       10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         358       1790.750170       10.0.0.14       TCP       45063 > bgp [SVN] Seq=0 Win=16384 Len=0 MSS=1460         361       1804.907497       10.0.0.13       10.0.0.14       TCP       45063 > bgp [SVN] Seq=0 Win=16384 Len=0       MSS=1460         361       1804.907497       10.0.0.13       10.0.0.14       TCP	Lime	Source	Destination	Protocol Info	2
1311 1786.153888 c1sco.96:f2:c0       c1sco.96:f2:c0       LOOP       Reply         1351 1787.730597 10.0.0.14       255.255.255.255       DNS       Standard query PTR 1.4.168.192, in-addr.arpa         1351 1797.747939 10.0.0.14       255.255.255.255       DNS       Standard query PTR 1.4.168.192, in-addr.arpa         1351 1795.750170 10.0.0.14       255.255.255.255       DNS       Standard query PTR 2.0.0.10.1n-addr.arpa         1351 1795.750170 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         1351 1795.750170 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         1358 1799.750177 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         1351 1365.907451.00.0.13       10.0.0.14       TCP       bgp 34064392 bgg (FX) Seq-0 Min-16384 Len=0 MSS-1460         160 1804.907397 10.0.0.13       10.0.0.14       TCP       bgp 45063 Styp, (FK) Seq-1 Ack=1 win=16384 Len=0 MSS-1460         161 1804.907397 10.0.0.13       10.0.0.14       TCP       bgp 45063 Styp, (FK) Seq-2 Ack=1 win=16384 Len=0         162 1804.907397 10.0.0.13       10.0.0.14       BCP       OPEN MESsage         163 1804.907397 10.0.0.13       10.0.0.14       BCP       OPEN MESsage         164 1805.13510 01.0.0.13       10.0.0.14       BCP       OPEN MESsage <td>349 1776.1539</td> <td></td> <td></td> <td></td> <td></td>	349 1776.1539				
511 1786.153888 cisco_96:f2:c0       cisco_96:f2:c0       LOOP       Reply         521 1787.73097 10.0.0.14       255.255.255.255       DNS       Standard query PTR 1.4.168.192, in-addr.arpa         353 1790.730180 10.0.0.14       255.255.255.255       DNS       Standard query PTR 1.4.168.192, in-addr.arpa         354 1793.74793 10.0.0.14       255.255.255.255       DNS       Standard query PTR 2.0.0.10.1n-addr.arpa         351 1795.750170 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         355 1795.750170 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         358 1804.902455 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         358 1804.902455 10.0.0.14       10.0.0.14       TCP       bg 54063 > bgg [StN] Seq-0 Ack=1 win=16384 Len=0 MSS=1460         360 1804.907397 10.0.0.13       10.0.0.14       TCP       bg7 > 45063 > bgg [CKL] Seq-1 Ack=1 win=16384 Len=0         361 1804.907397 10.0.0.13       10.0.0.14       BCP       OPEN MESsage         361 1804.907397 10.0.0.13       10.0.0.14       BCP       OPEN MESsage         361 1804.907397 10.0.0.13       10.0.0.14       BCP       OPEN MESsage         363 1804 91524 10.0.0.13       10.0.0.14       BCP       OPEN MESsage         364 1805.02000		56 cisco_96:f2:c0	cisco_96:f2:c0	LOOP Rep	
152       1787.730597       10.0.0.14       255.255.255       DNS       Standard query PTR 1.4.168.192, in-addr.arpa         153       1790.73080       10.0.0.14       255.255.255       DNS       Standard query PTR 1.4.168.192, in-addr.arpa         153       1790.73080       10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         155       1795.794110       cisc				LOOP Rep	
153       1790.7301&0 10.0.0.14       252.255.255.255       DNS       Standard querý PTR 1.4.168.192.in-addr.arpa         153       1793.7301&0 10.0.0.14       255.255.255.255       DNS       Standard querý PTR 2.0.0.10.in-addr.arpa         155       1795.794110       Cisco_96:f2:c0       CDP/VTP/DTP/PAgP/UDLD CDP       Device ID: Router_A Port ID: FastEthernet0/0         155       1795.794110       Cisco_96:f2:c0       CDP/VTP/DTP/PAgP/UDLD CDP       Reply         157       1796.750170       10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         158       1799.750177       10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         150       1804.907397       10.0.0.14       10.0.0.14       TCP       bg7 45063 > bg7 [CK] Seq-0 Ack=1 win=16384 Len=0 MSS=1460         160       1804.907397       10.0.0.13       TCP       bg7 45063 > bg7 [CK] Seq-0 Ack=1 win=16384 Len=0         161       10.0.0.13       10.0.0.14       TCP       bg7 PM MSSage       Seq-1 Ack=1 win=16384 Len=0         162       1804.907797       10.0.0.13       10.0.0.14       TCP       bg7 PM MSSage       VEEPALIVE Message         163       1804.907797       10.0.0.13       10.0.0.13       BGP       VEEPALIVE Message, UPDATE Message, UPDATE M	350 1784.7292	67 10.0.0.14	255.255.255.255	LOOP Rep DNS Star	da 🛃 0.1kbps 1 0.0 kbps 8.192. in-addr.arpa
154       1793.747939       10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         355       1795.794110       Cisco_96:f2:c0       CDP/VTP/DTP/PAgP/UDLD CDP       Device ID: Router_A Port ID: FastEthernet0/0         356       1796.750170       10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         358       1799.750177       10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         358       1799.750177       10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         359       1804.902645       10.0.0.13       10.0.0.14       TCP       45063 >> bgp [SVN] Seq=0 Atk=1 win=16384 Len=0 MSS=1460         361       1804.90797       10.0.0.13       10.0.0.14       TCP       45063 >> bgp [Atk] Seq=1 Atk=1 win=16384 Len=0 MSS=1460         361       1804.90797 10.0.0.13       10.0.0.14       TCP       45063 >> bgp [Atk] Seq=1 Atk=1 win=16384 Len=0         361       1804.907354       10.0.0.13       10.0.0.14       BGP       OPEN Message         361       1804.907354       10.0.0.13       10.0.0.14       BGP       PDET Message, UPDATE Message         361       1804.906754       10.0.0.13       10.0.0.14       BGP       VEDATE	350 1784.7292 351 1786.1538	67 10.0.0.14 88 Cisco_96:f2:c0	255.255.255.255 Cisco_96:f2:c0	LOOP Rep DNS Star LOOP Rep	da <u>≹ 0.0 kbps</u> <b>8.192. in-addr. arpa</b>
355       1795.794110 (isco_96:f2:c0       CDP/VTP/DTP/PApP/UDLO CDP       Device TD: Router_A Port ID: FastEthernet0/0         356       1796.750170 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.1n-addr.arpa         358       1796.750170 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.1n-addr.arpa         358       1799.750177 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.1n-addr.arpa         358       1799.750177 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.1n-addr.arpa         358       100.0.14       TCP       bg7 Standard query PTR 2.0.0.10.1n-addr.arpa         360       1804.907397 10.0.0.13       10.0.0.14       TCP       bg7 45063 > bgr [ck] Seq-1 Ack-1 win-16384 Len-0 MSS-1460         361       1804.907397 10.0.0.13       10.0.0.14       TCP       bg7 OPEN Message       Seq-1 Ack-1 win-16384 Len-0         361       1804.907397 10.0.0.13       10.0.0.14       BGP       OPEN Message, WEEPALTVE Message       366         364       1804.907397 10.0.0.14       10.0.0.13       BGP       UPDATE Message, UPDATE Message, UPDATE Message, UPDATE Message, WEPALTVE Message       366         364       1804.91522 10.0.0.13       10.0.0.14       TCP       45063 > bgr [AcK] Seq-362 Ack=302 win-16083 Len-0       367 <td>350 1784.7292 351 1786.1538 352 1787.7305</td> <td>67 10.0.0.14 88 Cisco_96:f2:c0 97 10.0.0.14</td> <td>255.255.255.255 Cisco_96:f2:c0 255.255.255.255</td> <td>LOOP Rep DNS Star LOOP Rep DNS Star</td> <td>da * 0.1kbps 1 0.0kbps 8.192.in-addr.arpa Y dard query PTR 1.4.168.192.in-addr.arpa</td>	350 1784.7292 351 1786.1538 352 1787.7305	67 10.0.0.14 88 Cisco_96:f2:c0 97 10.0.0.14	255.255.255.255 Cisco_96:f2:c0 255.255.255.255	LOOP Rep DNS Star LOOP Rep DNS Star	da * 0.1kbps 1 0.0kbps 8.192.in-addr.arpa Y dard query PTR 1.4.168.192.in-addr.arpa
356 1796.153689 cisco_96:f2:c0       cisco_96:f2:c0       LOOP       Reply         358 1799.750170 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.1n-addr.arpa         358 1799.750177 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         358 1799.750177 10.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         359 1804.907451 20.0.0.13       10.0.0.14       TCP       45063 > bgp [KcN] Seq-0 Ack=1 Win=16384 Len=0 MSS=1460         361 1804.907797 10.0.0.13       10.0.0.14       TCP       45063 > bgp [AcK] Seq-1 Ack=1 Win=16384 Len=0         361 1804.907797 10.0.0.13       10.0.0.14       TCP       45063 > bgp [AcK] Seq-1 Ack=1 Win=16384 Len=0         361 1804.907797 10.0.0.13       10.0.0.14       TCP       45063 > bgp [AcK] Seq-1 Ack=1 Win=16384 Len=0         361 1804.915529 10.0.0.13       10.0.0.14       BGP       OPEN Message         361 1805.020003 10.0.0.14       10.0.0.13       BGP       UPDATE Message, UPDATE Message         361 1805.153619 cisc0.96:f2:c0       cisc0.96:f2:c0       LOOP       Reply         361 1816.153619 cisc0.96:f2:c0       cisc0.96:f2:c0       LOOP       Reply	350 1784.72920 351 1786.15380 352 1787.73059 353 1790.73010	67 10.0.0.14 88 Cisco_96:f2:c0 97 10.0.0.14 80 10.0.0.14	255.255.255.255 Cisco_96:f2:c0 255.255.255.255 255.255.255.255	LOOP Rep DNS Star LOOP Rep DNS Star DNS Star	da <u>≹ 0.1kbps</u> <u></u> <b>1</b> 0.0kbps <b>8.192.in-addr.arpa</b> y dard query PTR 1.4.168.192.in-addr.arpa dard query PTR 1.4.168.192.in-addr.arpa
357       1796.750170       0.0.0.14       255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         358       1799.750177       10.0.0.14       255.255.255.255       DNS       Standard query PTR 2.0.0.10.in-addr.arpa         359       1804.902645       10.0.0.13       10.0.0.14       TCP       45063 > bgp [SVN] Seq=0 win=16384 Len=0 MSS=1460         360       1804.907497       10.0.0.14       TCP       bgp 74053       Styn Ack1 Seq=0 Ack=1 win=16384 Len=0         361       1804.907497       10.0.0.13       10.0.0.14       TCP       bgp 74053       Styn Ack1 Seq=0 Ack=1 win=16384 Len=0         361       1804.907497       10.0.0.13       10.0.0.14       TCP       45063 > bgp [AcK] Seq=0 Ack=1 win=16384 Len=0         361       1804.907457       10.0.0.13       10.0.0.14       BGP       OPEN Message         364       1804.91552       10.0.0.13       10.0.0.14       BGP       VEPATE Message, UPDATE Message         364       1804.91552       10.0.0.13       10.0.0.14       TCP       45063 > bgp [AcK] Seq=65 Ack=302 win=16083 Len=0         365       1805.218010       10.0.0.13       10.0.0.14       TCP       45063 > bgp [AcK] Seq=65 Ack=302 win=16083 Len=0         367       1806.153194       Cisc.96:F2:c0       LoOP       Reply	350 1784.7292 351 1786.1538 352 1787.73059 353 1790.7301 354 1793.7479	67 10.0.0.14 88 Cisco_96:f2:c0 97 10.0.0.14 80 10.0.0.14 39 10.0.0.14	255.255.255.255 Cisco_96:f2:c0 255.255.255.255 255.255.255.255 255.255.	LOOP Rep DNS Star LOOP Rep DNS Star DNS Star DNS Star	nda € 0.1kbps 1 0.0kbps 8.192.in-addr.arpa y dard query PTR 1.4.168.192.in-addr.arpa ndard query PTR 1.4.168.192.in-addr.arpa ndard query PTR 2.0.0.10.in-addr. arpa
158       1799.750177       10.0.0.14       255.255.255       DNS       Standard guery       PTR 2.0.0.10.in-addr.arpa         159       100.0.0.13       10.0.0.14       TCP       45063 > bgp [KVN] Seq-0 win-16384 Len-0 MSS=1460         160       1804.907432       10.0.0.13       TCP       bgp 34061 [SVN] Ack] Seq-0 Ack=1 win=16384 Len-0 MSS=1460         161       1804.907797       10.0.0.13       10.0.0.14       TCP       45063 > bgp [ACK] Seq-1 Ack=1 win=16384 Len-0         161       1804.907797       10.0.0.13       10.0.0.14       TCP       45063 > bgp [ACK] Seq-1 Ack=1 win=16384 Len-0         161       1804.908754       10.0.0.14       10.0.0.14       BGP       OPEN MESsage         161       1804.908754       10.0.0.14       10.0.0.13       BGP       OPEN MESsage, VEDATE Message, UPDATE Message         161       1804.915529       10.0.0.13       10.0.0.14       TCP       45063 > bgp [ACK] Seq-65 Ack=302 win-16083 Len-0         165       1805.020003       10.0.0.13       10.0.0.14       TCP       45063 > bgp [ACK] Seq-65 Ack=302 win-16083 Len-0         166       1805.15519       Cisc.0.96172:c0       LOOP       Reply       10.0.0.14       FCP         167       1806.153619       cisc.0.96172:c0       LOOP       Reply       10.0.0.14	350 1784.7292 351 1786.1538 352 1787.7305 353 1790.7301 354 1793.7479 355 1795.7941	67 10.0.0.14 88 Cisco_96:f2:c0 97 10.0.0.14 80 10.0.0.14 39 10.0.0.14 10 Cisco_96:f2:c0	255.255.255.255 Cisco_96:f2:c0 255.255.255.255 255.255.255.255 CDP/VTP/DTP/PAgP/UDLD	LOOP Rep DNS Star LOOP Rep DNS Star DNS Star DNS Star CDP Dev	da ± 0.1kbps   1 0.0kbps   8.192.in-addr.arpa y dard query PTR 1.4.168.192.in-addr.arpa dard query PTR 1.4.168.192.in-addr.arpa idard query PTR 2.0.0.10.in-addr.arpa (c ID: Router_A Port ID: FastEthernet0/0
359 1804.902645 10.0.0.13       10.0.0.14       TCP       45063 > bgp       [\$vx] seq=0 win=16384 Len=0 MSS=1460         360 1804.907432 10.0.0.14       10.0.0.13       TCP       45063 > bgp       [\$xx] seq=0 Ack=1 win=16384 Len=0 MSS=1460         361 1804.907432 10.0.0.13       10.0.0.14       TCP       45063 > bgp       [\$xx] seq=0 Ack=1 win=16384 Len=0         361 1804.907432 10.0.0.13       10.0.0.14       TCP       45063 > bgp       [\$xx] seq=1 Ack=1 win=16384 Len=0         361 1804.907437 10.0.0.13       10.0.0.14       BCP       OPEN Message       message         361 1804.915529 10.0.0.14       10.0.0.13       BCP       OPEN Message, UPDATE Message       UPDATE Message         361 1804.915529 10.0.0.13       10.0.0.14       BCP       UPDATE Message, UPDATE Message       UPDATE Message, UPDATE Message, UPDATE Message, KEEPALIVE Message, KEEPALIVE Message         361 1805.218010 10.0.0.13       10.0.0.14       TCP       45063 > bgp [ACK] seq=65 Ack=302 win=16083 Len=0         367 1806.15359 cisc_0.96:f2:c0       Cisc_0.96:f2:c0       LOOP       Reply         368 1816.153593 cisc_0.96:f2:c0       Cisc_0.96:f2:c0       LOOP       Reply         367 1834.218051 0.0.0.13       10.0.0.14       BCP       UPDATE Message         371 1834.318053 10.0.0.13       10.0.0.14       BCP       UPDATE Message	350 1784.72920 351 1786.15380 352 1787.73059 353 1790.73010 354 1793.7479 355 1795.79411 356 1796.15360	67 10.0.0.14 88 cisco_96:f2:c0 97 10.0.0.14 80 10.0.0.14 39 10.0.0.14 10 cisco_96:f2:c0 89 cisco_96:f2:c0	255.255.255.255 Cisco_96:f2:c0 255.255.255.255 255.255.255.255 CDP/VTP/DTP/PAgP/UDLD Cisco_96:f2:c0	LOOP Rep DNS Star LOOP Rep DNS Star DNS Star DNS Star CDP Dev LOOP Rep	yda ≜ 0.1kbps 1 € 0.0 kbps 8,192.in-addr.arpa jy idard query PTR 1.4.168.192.in-addr.arpa idard query PTR 1.4.168.192.in-addr.arpa idard query PTR 2.0.0.10.in-addr.arpa idard query PTR 2.0.0.10.in-addr.arpa jy
160 1804.907492 10.0.0.14       10.0.0.13       TCP       bgp > 45063 > bgp (EXK) Seq-0 Ack-1 win-16384 Len-0 MSS=1460         161 1804.90797 10.0.0.13       10.0.0.14       TCP       45063 > bgp (EXK) Seq-1 Ack-1 win-16384 Len-0         161 1804.906754 10.0.0.13       10.0.0.14       TCP       45063 > bgp (EXK) Seq-1 Ack-1 win-16384 Len-0         161 1804.906754 10.0.0.13       10.0.0.14       BCP       OPEN Message         163 1804.91529 10.0.0.13       10.0.0.14       BCP       OPEN Message, UEDATE Message, UPDATE Message, UPDATE Message, UPDATE Message, UPDATE Message, KEEPALIVE Message, KEEPALIVE Message, Compare Message, UPDATE Message, UPDATE Message, UPDATE Message, KEEPALIVE Message, KEEPALIVE Message, Cisco.96:172:00         166 1805.153619 (cisco.96:172:00       Cisco.96:172:00       LOOP       Reply         369 1806.153619 (cisco.96:172:00       Cisco.96:172:00       LOOP       Reply         369 1806.153619 (cisco.96:172:00       Cisco.96:172:00       LOOP       Reply         369 1826.153474 (cisco.96:172:00       Cisco.96:172:00       LOOP       Reply         369 1834.318651 10.0.0.13       10.0.0.14       BCP       UPDATE Message       UPDATE Message         371 1834.218198 10.0.0.13       10.0.0.14       BCP       UPDATE Message       UPDATE Message         373 1834.318053 10.0.0.14       10.0.0.13       TCP       Bgp > 45063 [ACK] Seq-302 Ack-260 wi	350 1784.72920 351 1786.15380 352 1787.73050 353 1790.73010 354 1793.74790 355 1795.79410 356 1796.15360 357 1796.75010	67 10.0.0.14 88 cisco_96;f2:c0 97 10.0.0.14 80 10.0.0.14 39 10.0.0.14 10 Cisco_96;f2:c0 89 cisco_96;f2:c0 70 10.0.0.14	255.255.255.255 Cisco_96:f2:c0 255.255.255.255 255.255.255.255 255.255.	LOOP Rep DNS Star LOOP Rep DNS Star DNS Star DNS Star CDP Dev LOOP Rep DNS Star	da   0.1kbps
361       1804.907797       10.0.0.13       10.0.0.14       TCP       45063.> bgg [AcK] Seq-1 Ack-1 win=16384 Len=0         362       1804.90754       10.0.0.13       10.0.0.14       BCP       OPEN Message         361       1804.914524       10.0.0.14       10.0.0.13       BCP       OPEN Message         364       1804.914524       10.0.0.14       10.0.0.14       BCP       OPEN Message       UPDATE Message         364       1804.915529       10.0.0.14       10.0.0.13       BCP       UPDATE Message, UPDATE Message       UPDATE Message, UPDATE Message, UPDATE Message, UPDATE Message, KEEPALIVE Message         366       1805.218010       10.0.0.014       TCP       45063       Seq=65       Ack=302 win=16083 Len=0         367       1806.153619       Cisco.96:f2:cO       Cisco.96:f2:cO       LOOP       Reply         368       1816.153593       Cisco.96:f2:cO       LOOP       Reply         369       1826.153474       Cisco.96:f2:cO       LOOP       Reply         370       1834.18661       10.0.0.14       BCP       UPDATE Message       UPDATE Message         371       1834.317461       10.0.0.14       BCP       UPDATE	350 1784.72920 351 1786.15380 352 1787.73059 353 1790.73011 354 1793.74799 355 1795.79411 356 1796.15360 357 1796.75011 358 1799.75011	67 10.0.0.14 88 Cisco_96:f2:c0 97 10.0.0.14 80 10.0.0.14 99 10.0.0.14 10 Cisco_96:f2:c0 89 Cisco_96:f2:c0 70 10.0.0.14 77 10.0.0.14	255.255.255.255 C15co_96:f2:c0 255.255.255.255 255.255.255.255 255.255.255.255 CDP/VTP/0TP/PAgP/UDLD C15co_96:f2:c0 255.255.255 255.255.255 255.255.255	LOOP Rep DNS Star LOOP Rep DNS Star DNS Star DNS Star CDP Dev LOOP Rep DNS Star DNS Star	rda ≜ 0.1kbpc 1 0.0 kbpc 8,192.in-addr.arpa jv dard query PTR 1.4.168.192.in-addr.arpa dard query PTR 1.4.168.192.in-addr.arpa dard query PTR 2.0.0.10.in-addr.arpa (ce ID: ROUTE_A Port ID: FastEthernetO/0 y dard query PTR 2.0.0.10.in-addr.arpa dard query PTR 2.0.0.10.in-addr.arpa
362       1804.908754       10.0.0.13       10.0.0.14       BGP       OPEN Message         363       1804.914524       10.0.0.14       10.0.0.13       BGP       OPEN Message, KEEPALTVE Message         364       1804.914524       10.0.0.14       10.0.0.13       BGP       UPDATE Message, CEPALTVE Message, KEEPALTVE Message, UPDATE Message, UPDATE Message, UPDATE Message, KEEPALTVE Message, KEEPALTVE Message, UPDATE Message, Cesage         367       1806.153619       cisc.0.96:f2:c0       cisc.0.96:f2:c0       LOOP       Reply         368       1816.153619       cisc.0.96:f2:c0       cisc.0.96:f2:c0       LOOP       Reply         369       1826.153474       cisc.0.96:f2:c0       LOOP       Reply         369       1806.13619       0.0.0.13       10.0.0.14       BGP       UPDATE Message         370       1834.218061       0.0.0.13       10.0.0.14       BGP       UPDATE Message         371       1834.318053       10.0.0.13       TOP       bgp > 45063       CisC = 3602       Ack=360       Min=16125       Len=0         373       1834.318053       10.0.0.13       TOP       bgp > 45063       CisC = 3629	350 1784.72920 351 1786.15380 352 1787.73059 353 1790.73010 354 1793.7479 355 1795.79411 356 1796.15366 357 1796.7501 358 1799.7501 359 1804.9026	57 10.0.0.14 88 Cisco_96:f2:c0 97 10.0.0.14 80 10.0.0.14 10 Cisco_96:f2:c0 89 Cisco_96:f2:c0 70 10.0.0.14 77 10.0.0.14 75 10.0.0.13	255, 255, 255, 255 Cisco_96: F2: c0 255, 255, 255, 255 255, 255, 255, 255 255, 255, 255, 255 CDP/VTP/DTP/PAgP/UDLD Cisco_96: F2: c0 255, 255, 255, 255 255, 255, 255, 255 255, 255, 255, 255	LOOP Rep DNS Star LOOP Rep DNS Star DNS Star DNS Star CDP Dev LOOP Rep DNS Star DNS Star DNS Star	yda € 0.1kbps 1 0.0 kbps 8.192.in-addr.arpa yda query PTR 1.4.168.192.in-addr.arpa ddard query PTR 1.4.168.192.in-addr.arpa ddard query PTR 2.0.0.10.in-addr.arpa ice ID: Router_A Port ID: FastEthernetO/O y ddard query PTR 2.0.0.10.in-addr.arpa ddard query PTR 2.0.0.10.in-addr.arpa ddard query PTR 2.0.0.10.in-addr.arpa
363       1804.914524       10.0.0.14       10.0.0.13       BCP       OPEN Wessage, KEEPALIVE Message         364       1804.914529       10.0.0.13       10.0.0.14       BCP       VEEPALIVE Message         365       1805.02003       10.0.0.13       10.0.0.13       BCP       UPDATE Message, UPDATE Message, UPDATE Message, UPDATE Message, UPDATE Message, KEEPALIVE Message         366       1805.218010       0.0.0.13       10.0.0.14       BCP       UPDATE Message, UPDATE Message       UPDATE Message         370       1834.118661       10.0.0.13       10.0.0.14       BCP       UPDATE Message, UPDATE Message       UPDATE Message         371       1834.218198       10.0.0.13       10.0.0.14       BCP       UPDATE Message       UPDATE Message         372       1834.318053       10.0.0.14       10.0.0.14       BCP       UPDATE Message       UPDATE Message         373       1834.318053       10.0.0.13       10.0.0.14       BCP       UPDAT	350 1784.7292 351 1786.1538 352 1787.7305 353 1790.7301 354 1793.74791 355 1795.7941 356 1796.15361 357 1796.7501 358 1799.7501 359 1804.9074	67 10.0.0.14 88 cisc_96:f2:c0 97 10.0.0.14 80 10.0.0.14 93 10.0.0.14 10 cisc_96:f2:c0 89 cisc_96:f2:c0 70 10.0.0.14 45 10.0.0.14 45 20.0.0.14	255.255.255.255 C15co_96:f2:c0 255.255.255.255 255.255.255.255 255.255.255.255 CDP/VTP/DTP/PAgP/UDLD C15co_96:f2:c0 255.255.255.255 255.255.255.255 10.0.0.13	LOOP Rep DNS Star LOOP Rep DNS Star DNS Star DNS Star CDP Dev LOOP Rep DNS Star DNS Star TCP 4500	da       0.0 kbps       8.192. in-addr.arpa         y       y         dard query PTR 1.4.168.192. in-addr.arpa         dard query PTR 1.4.168.192. in-addr.arpa         dard query PTR 1.4.168.192. in-addr.arpa         idard query PTR 2.0.0.10.in-addr.arpa         idard query PTR 2.0.0.10.in-6184 Len=0 MSS=1460
364       1804, 915529       10.0,0,0.13       10.0,0,14       BCP       KEEPALIVE Vessage         365       1805, 020033       10.0,0,0.13       10.0,0,0.13       BCP       UPDATE Message, UPDATE Message, UPDATE Message, UPDATE Message, UPDATE Message, KEEPALIVE Message, Cisco_96:f2:c0       LOOP       Reply         369       1806, 153649       Cisco_96:f2:c0       LOOP       Reply       KeepAutine Message, UPDATE Message, UPDATE Message         369       1836, 153474       Cisco_96:f2:c0       LOOP       Reply         369       1836, 153474       Cisco_96:f2:c0       LOOP       Reply         369       1836, 153474       Cisco_96:f2:c0       LOOP       Reply         369       1806, 0.13       10.0, 0.14       BGP       UPDATE Message       UPDATE Message         371       1834, 218198       10.0, 0.13       10.0, 0.14       BGP       UPDATE Message, KEEPALIVE Message         374       1834, 31805       10.0, 0.13       10.0, 0.13       BGP       UPDATE Message, KEEPALIVE Message	350 1784.7292 351 1786.1538 352 1787.7305 353 1790.7301 354 1793.7479 355 1795.7941 356 1796.15366 357 1796.7501 358 1799.7501 359 1804.9026 360 1804.9077	67         10.0         14           88         Cisco_96:f2:c0         97           97         10.0         0.14           80         10.0         0.14           93         10.0         0.14           93         10.0         0.14           95         0.50         6:f2:c0           95         Cisco_96:f2:c0         95           95         Cisco_96:f2:c0         10           95         Cisco_96:f2:c0         10           97         Cisco_96:f3:c0         13	255, 255, 255, 255, 255 Cisco_96:F2:C0 255, 255, 255, 255, 255 255, 255, 255, 255 CDP/VTP/DTP/PAgP/VDLD Cisco_96:F2:C0 255, 255, 255, 255 255, 255, 255, 255 10.0, 0, 14 10.0, 0, 14	LOOP Rep DNS Star LOOP Rep DNS Star DNS Star DNS Star DNS Star LOOP Rep DNS Star DNS Star DNS Star DNS Star TCP 4500	ya <u>0.1kbps</u> <u>↑ 0.0kbps</u> <u>8.192.in-addr.arpa</u> yad <u>0.1kbps</u> <u>1 0.0kbps</u> <u>8.192.in-addr.arpa</u> tdard query PTR 1.4.168.192.in-addr.arpa tdard query PTR 2.0.0.10.in-addr.arpa ice ID: Router_A Port ID: FastEthernet0/0 y ndard query PTR 2.0.0.10.in-addr.arpa tdard query PTR 2.0.0.10.in-addr.arpa tdard query PTR 2.0.0.10.in-addr.arpa tdard query PTR 2.0.0.10.in-addr.arpa tdard query PTR 2.0.0.10.in-addr.arpa 3> bpg [SYN] Scq-0 win-13384 Len=0 MSS=1460 >3 bbg [SKN] Seq-0 Ack=1 win=16384 Len=0 MSS=1460
165       100.0.0.14       10.0.0.13       BCP       UPDATE Message       UPDATE Message, UPDATE Message, UPDATE Message, UPDATE Message, KEEPALIVE Message, VPDATE VPDATE Message, VPDATE Message, VPDATE Message, VPDATE Messag	350 1784.7292 351 1786.15388 352 1787.7305 353 1790.7301 354 1793.7479 355 1795.7941 356 1796.1536 357 1796.7501 358 1799.7501 359 1804.9026 360 1804.9074 361 1804.9077	67         10.0.0.14           88         Cisco_96:f2:c0           97         10.0.0.14           80         10.0.0.14           10         Cisco_96:f2:c0           89         Cisco_96:f2:c0           70         10.0.0.14           10         Cisco_96:f2:c0           70         10.0.0.14           13         10.0.0.14           14         10.0.0.13           15         10.0.0.13           10         Cisco_94:f2:c0	255, 255, 255, 255, 255 Cisco_96; F2:c0 255, 255, 255, 255, 255 255, 255, 255,	LOOP         Rep           DNS         Star           LOOP         Rep           DNS         Star           TCP         4500           TCP         4500           TCP         4500           TCP         4500           TCP         90PE	da       0.1kbps       0.0kbps       8.192.in-addr.arpa         y       y       y         dard query PTR 1.4.168.192.in-addr.arpa       y         dard query PTR 1.4.168.192.in-addr.arpa       y         dard query PTR 1.4.168.192.in-addr.arpa       y         idard query PTR 2.0.0.10.in-addr.arpa
366 1805.218010 10.0.0.13       10.0.0.14       TCP       45063 > bgp [AcK] Seq=65 AcK=302 win=16083 Len=0         367 1806.153593 Cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         368 1816.153593 Cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         368 1816.153593 Cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         368 1816.153593 Acisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         369 1826.153474 (cisco_96:f2:c0       Cisco_96:f2:c0       LOOP       Reply         371 1834.318661 10.0.0.13       10.0.0.0.14       BGP       UPDATE Message         372 1834.317456 10.0.0.13       10.0.0.14       BGP       VEPATE Message         373 1834.318053 10.0.0.14       10.0.0.13       BGP       VEPATE Message         375 1834.517523 10.0.0.14       10.0.0.13       TCP       bgp > 45063 [ACK] Seq=329 Ack=298 win=16087 Len=0         375 1834.51801 10.0.0.14       10.0.0.14       TCP       bgp > 45063 [ACK] Seq=228 Ack=329 win=16087 Len=0         376 1834.5180	350 1784.7292 351 1786.1538 352 1787.7305 353 1790.7301 354 1793.7479 355 1795.7941 356 1795.7941 357 1796.7501 357 1796.7501 358 1799.7501 358 1799.7501 361 1804.9074 361 1804.9077 363 1804.9145	67         10.0.0.14           88         Cisco_96:f2:c0           97         10.0.0.14           80         10.0.0.14           10         Cisco_96:f2:c0           98         Cisco_96:f2:c0           90         Cisco_96:f2:c0           90         Cisco_96:f2:c0           90         Cisco_96:f2:c0           90         Cisco_96:f2:c0           70         Cisco_10:f2:c0           90         Cisco_96:f2:c0           91         Cisco_96:f2:c0           92         Cisco_96:f2:c0	255, 255, 255, 255, 255 Cisco, 96; 72:00 255, 255, 255, 255 255, 255, 255, 255 255, 255, 255, 255 CDP/VTP/DTP/PAgP/UDLD Cisco_96; 72:00 255, 255, 255, 255 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 13	LOOP Rep DNS Star LOOP Rep DNS Star DNS Star DNS Star CDP Dev LOOP Rep DNS Star DNS Star TCP 4500 BGP OPEN BGP OPEN	yda € 0.8 kbps 1 € 0.0 kbps 8, 192. in-addr. arpa y idard query PTR 1.4.168.192. in-addr. arpa idard query PTR 1.4.168.192. in-addr. arpa idard query PTR 2.0.0.10. in-addr. arpa (cc ID: Router_A Port ID: FastEthernetO/0 y idard query PTR 2.0.0.10. in-addr. arpa idard query PTR 2.0.0.10. in-addr. arpa 35 > bgp (SVW) Seq=0 Win=16384 Len=0 MSS=1460 35 > bgp (ACK) Seq=0 Ack=1 Win=16384 Len=0 Wessage Wessage
367       1806.153619       cisco_96:f2:c0       cisco_96:f2:c0       LOOP       Reply         368       1816.153593       cisco_96:f2:c0       LOOP       Reply         369       1826.153474       cisco_96:f2:c0       LOOP       Reply         370       1834.118661       10.0.0.13       10.0.0.14       BGP       UPDATE       Message, UPDATE       Message         372       1834.118661       10.0.0.14       10.0.0.14       BGP       UPDATE       Message       372         372       1834.317486       10.0.0.14       10.0.0.13       TCP       bgp > 45063       [ACK]       Seq=302       Ack=260       win=16125       Len=0         373       1834.318053       10.0.0.14       10.0.0.13       BGP       UPDATE       Message       374       133.13919       10.0.0.14       BGP       NPDATE       Message       374       133.13919       10.0.0.14       BGP       NPDATE       Message       375       1374       133.10.0.0.14       10.0.0.13       BGP       NPDATE       Message       375       1374       10.0.0.14       TCP       bgp > 45063       Ack       Seq=329       Ack=280       win=16057       Len=0       376       1834.518014       10.0.0.13       TCP       b	350         1784.7292           351         1786.1538           352         1787.7305           353         1790.7301           354         1793.7479           355         1796.7501           356         1796.7501           358         1797.7501           358         1796.7501           359         1804.9024           361         1804.9074           361         1804.9077           361         1804.9077           361         1804.9077           361         1804.9074           364         1804.9155	67         10.0.0.14           88         Cisco_96:f2:c0           97         10.0.0.14           80         10.0.0.14           10         Cisco_96:f2:c0           89         Cisco_96:f2:c0           70         10.0.0.14           10         Cisco_96:f2:c0           70         10.0.0.14           15         10.0.0.13           32         10.0.0.13           54         10.0.0.13           54         10.0.0.13           24         10.0.0.13	255, 255, 255, 255, 255 Cisco_96: F2: c0 255, 255, 255, 255, 255 255, 255, 255,	LOOP Rep DNS Star LOOP Rep DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star TCP AS00 TCP 4500 TCP 4500 BGP OPEN BGP OPEN BGP KEEF	ida       0.1kbps       1 0.0kbps       8.192.in-addr.arpa         idard query PTR 1.4.168.192.in-addr.arpa       idard query PTR 1.4.168.192.in-addr.arpa         idard query PTR 1.4.168.192.in-addr.arpa       idard query PTR 2.0.0.10.in-addr.arpa         idard query PTR 2.0.0.10.in-addr.arpa       idard query PTR 2.0.0.10.in-addr.arpa         idard query PTR 2.0.0.10.in-idadr.arpa       idard query PTR 2.0.0.10.in-idadr.arpa
368 1816.153593 c/scc_96:f2:c0       c/scc_96:f2:c0       LOOP       Reply         369 1826.153474 c/scc_96:f2:c0       c/scc_96:f2:c0       LOOP       Reply         370 1834.118661 10.0.0.13       10.0.0.14       BGP       UPDATE Message         371 1834.218198 10.0.0.13       10.0.0.14       BGP       UPDATE Message         372 1834.317465 10.0.0.13       10.0.0.14       BGP       UPDATE Message         373 1834.318053 10.0.0.13       10.0.0.14       BGP       UPDATE Message         373 1834.318053 10.0.0.13       10.0.0.14       BGP       VERALIVE Message         373 1834.318053 10.0.0.13       10.0.0.14       BGP       VERALIVE Message         375 1834.517523 10.0.0.14       10.0.0.13       TCP       bgp > 45063 [ACK] Seq=329 Ack=298 kin=16087 Len=0         376 1834.518014 10.0.0.13       10.0.0.14       TCP       bgp > 45063 [ACK] Seq=239 Ack=298 kin=16087 Len=0         376 1834.518014 10.0.0.13       10.0.0.14       TCP       bgp > 45063 [ACK] Seq=239 Ack=298 kin=16087 Len=0         377 1835.781501 10.0.0.14       102.0.614       TCP       bgp > 45063 [ACK] Seq=239 Ack=239 kin=16087 Len=0         376 1834.518014 10.0.0.14       TCP       bgp > source port: 3105       bestination port: 33448	350 17.84,7292 351 17.86,15.38 352 17.87,7305 353 17.90,7301 354 17.93,7479 355 17.96,15.36 357 17.96,7341 358 17.96,15.36 357 17.96,7341 359 18.04,9024 359 18.04,9024 361 18.04,9074 361 18.04,9074 361 18.04,9073 364 18.04,9153 364 18.04,9153	67         10.0.0.14           88         clsc.0.6f72:c0           97         10.0.0.14           80         10.0.0.14           10         clsc.0.96:f2:c0           98         clsc.0.96:f2:c0           98         clsc.0.96:f2:c0           98         clsc.0.014           77         10.0.0.14           23         21.0.0.0.13           24         10.0.0.13           24         10.0.0.14           27         10.0.0.14           27         10.0.0.14           20         0.0.0.14           21         0.0.0.14           21         0.0.0.14           21         0.0.0.14           20         0.0.0.14	255, 255, 255, 255, 255 Cisc_0.967; 21:00 255, 255, 255, 255, 255 255, 255, 255, 255 255, 255, 255, 255 CDP/VTP/0TP/PAgP/UDL0 Cisc_0.967; 21:00 255, 255, 255, 255 10, 0, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 13 255, 255, 255 255, 255, 255, 255, 255 255, 255, 255, 255 255, 255, 255, 255, 255 255, 255, 255, 255, 255 255, 255, 255, 255, 255 255, 255, 255, 255, 255, 255 255, 255, 255, 255, 255, 255 255, 255, 255, 255, 255, 255, 255, 255,	LOOP Rep DNS Star LOOP Rep DNS Star DNS Star DNS Star CDP Dev LOOP Rep DNS Star TCP 4500 BGP OPEN BGP OPEN BGP WEB BGP WEB	yga ∰ 0.1kbps
369       1826.153474 (risco_96:f2:c0       cisco_96:f2:c0       LOOP       Reply         370       1834.11866110.0,0.13       10.0,0.14       BGP       UPDATE Message, UPDATE Message         371       1834.218198       10.0,0.13       10.0,0.14       BGP       UPDATE Message         371       1834.218198       10.0,0.13       10.0,0.14       BGP       UPDATE Message         371       1834.318053       10.0,0.13       10.0,0.13       TCP       bgp > 45063       [ACK] Seq=302       Ack=260       win=16125       Len=0         374       1834.318053       10.0,0.13       10.0,0.14       BGP       VEEPALIVE Message       EEPALIVE Message         374       1834.319319       10.0,0.14       10.0,0.13       BGP       UPDATE Message         375       1834.517523       10.0,0.14       10.0,0.13       TCP       bgp > 45063       [ACK] Seq=329       Ack=298       win=16087       Len=0         376       1834.518014       10.0,0.14       TCP       45083       bgp > 45063       [ACK] Seq=298       Ack=298       win=16087       Len=0         376       1834.518014       10.0,0.14       TCP       45083       bgp > 45063       [ACK] Seq=329       Ack=329       win=16056       Len=0	350         17.84         .7292           351         17.86         .15.84           352         17.87         .7305           353         17.90         .7301           354         17.93         .7479           355         17.95         .7411           356         17.96         .7501           358         17.99         .7501           358         18.04         .9027           361         18.04         .9027           361         18.04         .9027           362         18.04         .9027           363         18.04         .9027           364         18.04         .9127           364         18.04         .9125           364         18.05         .2000           365         18.05         .2020	67         10.0.0         14           88         Cisco_96:f2:c0         99           97         10.0.0         14           80         10.0.0         14           91         10.0.0         14           91         10.0.0         14           93         10.0.0         14           95         Cisco_96:f2:c0         98           95         Cisco_96:f2:c0         98           95         Cisco_96:f2:c0         91           90         0.0.0         14           10         0.0         13           21         0.0         0.13           24         10.0         0.13           24         10.0         0.14           29         10.0         0.14           29         10.0         0.14           29         10.0         0.14           10         10.0         0.13	255, 255, 255, 255, 255 Cisco_96:F2:C0 255, 255, 255, 255, 255 255, 255, 255, 255, 255 CDP/VTP/0TP/PAgP/UDLD Cisco_96:F2:C0 255, 255, 255, 255 255, 255, 255, 255 255, 255, 255, 255 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 14 10, 0, 14 10, 0, 14 10,	LOOP Rep DNS Star DNS Star DNS Star DNS Star DNS Star CDP Dev' DNS Star CDP Dev' DNS Star TCP 4500 BGP OPEN BGP OPEN BGP UPDD/ TCP 4500 TCP 4500	ya 0.1kbps ↑ 0.0kbps 8.192.in-addr.arpa y tidard query PTR 1.4.168.192.in-addr.arpa tidard query PTR 1.4.168.192.in-addr.arpa tidard query PTR 2.0.0.10.in-addr.arpa tice ID: Router_A Port ID: FastEthernet0/0 y tidard query PTR 2.0.0.10.in-addr.arpa tidard query PTR 2.0.0.10.in-addr.arpa tidard query PTR 2.0.0.10.in-addr.arpa tidard query PTR 2.0.0.10.in-addr.arpa tidard state for the state of
370     1834.118661     10.0.0.13     10.0.0.14     BGP     UPDATE Message, uPDATE Message       371     1834.118661     10.0.0.13     10.0.0.14     BGP     UPDATE Message       371     1834.218198     10.0.0.13     10.0.0.14     BGP     UPDATE Message       372     1834.317486     10.0.0.14     10.0.0.13     TCP     bgp > 45063     [ACK] Seq=302     Ack=260     win=16125     Len=0       373     1834.318053     10.0.0.13     10.0.0.14     BGP     WEPATE Message       374     1834.3131919     10.0.0.14     BGP     UPDATE Message       375     1834.517523     10.0.0.14     10.0.0.13     TCP     bgp > 45063     [ACK] Seq=329     Ack=298     win=16057     Len=0       376     1834.517523     10.0.0.14     TCP     bgp > 45063     > bgq > 245063     Len=0       376     1834.51501     10.0.0.14     TCP     bgp > 64063 > bgp [ACK] Seq=329     Ack=328     win=16056     Len=0       377     1835.781501     10.0.0.14     TCP     45063     Solf     Seq=232     Ack=328     win=16056     Len=0       377     1835.781501     10.0.0.14     TCP     5000000000000000000000000000000000000	350         1748.7292           351         1766.1538           352         1777.7301           353         1790.7301           354         1793.7479           355         1795.7941           356         1796.7501           358         1799.7501           358         1796.7501           358         1796.7501           350         1804.9024           361         1804.9024           362         1804.9024           363         1804.9024           364         1804.9035           365         1805.21800           365         1805.2000           366         1805.21800           367         1805.1365	67         10.0.0.14           86         152.0.6           97         10.0.0.14           80         10.0.0.14           910.0.0.0.14         10           95         10.0.0.14           95         10.0.0.14           95         10.0.0.14           97         10.0.0.14           97         10.0.0.14           97         10.0.0.14           97         10.0.0.14           97         10.0.0.14           97         10.0.0.13           21         10.0.0.13           23         10.0.0.13           23         10.0.0.13           23         10.0.0.13           20         10.0.0.14           91         0.0.0.14           91         0.0.0.13           24         10.0.0.13           30         10.0.0.14           10         10.0.0.14           10         10.0.0.14	255, 255, 255, 255 Cisc_0.967; 21:00 255, 255, 255, 255 255, 255, 255, 255 255, 255, 255, 255 255, 255, 255, 255 CDP/VTP/DTP/PAgP/UDLD Cisc_0.967; 21:00 255, 255, 255, 255 10, 0, 0, 0, 14 10, 0, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 15 10, 0, 0, 14 10, 0, 0, 15 10, 0, 0, 14 10, 0, 0, 15 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 15 10, 0, 0, 14 10, 0, 0, 15 10, 0, 0, 14 10, 0, 0, 15 10, 0, 0, 14 10, 0, 0, 15 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 15 10, 0, 0, 14 10, 0, 0, 15 10, 0, 15 10, 0, 15 10, 0, 15 10, 0, 15 10, 0, 15	LOOP Rep DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star TCP Dev LOOP Rep DNS Star TCP 4500 BGP OPEN BGP OPEN BGP OPEN BGP UPD/ TCP 4500 DNS Star TCP 4500 DNS Star DNS	ya ≜ 0.1kbpc ↑ 0.0kbpc 8,192.in-addr.arpa yada € 0.1kbpc ↑ 0.0kbpc 8,192.in-addr.arpa hdard query PTR 1.4.168.192.in-addr.arpa hdard query PTR 2.0.0.10.in-addr.arpa (ce ID: Router_A Port ID: FastEthernetO/0 y hdard query PTR 2.0.0.10.in-addr.arpa hdard query PTR 2.0.0.10.in-addr.arpa hdard query PTR 2.0.0.10.in-addr.arpa hdard query PTR 2.0.0.10.in-addr.arpa by (Stw) Seq=0 kin-16384 Len=0 MSS=1460 53 > bpg (Stw) Seq=0 Ack=1 win=16384 Len=0 MSS=1460 53 > bpg (Ack) Seq=1 Ack=1 win=16384 Len=0 Hessage Hessage, KEEPALIVE Message ALIVE Message, UPDATE Message, UPDATE Message, KEEPALIVE Message, KEEPALIVE Mess 33 > bpg (Ack) Seq=65 Ack=302 win=16083 Len=0 y
371     1834     21819     10.0.0.13     10.0.0.14     BGP     UPDATE Message       372     1834     218198     10.0.0.13     10.0.0.13     TCP     bgp > 45065     [AcK] Seq=302     Ack=260     win=16125     Len=0       373     1834     318053     10.0.0.13     10.0.0.14     BGP     KEEPALIVE     Message       374     1834     319319     10.0.0.14     10.0.0.13     BGP     VPDATE     Message       374     1834     319319     10.0.0.14     10.0.0.13     BGP     VPDATE     Message       375     1834     517523     10.0.0.14     10.0.0.13     TCP     bgp > 45065     [Ack] Seq=329     Ack=329     win=16087     Len=0       376     1834     51801     10.0.0.14     TCP     45083     bgp [Ack] Seq=298     win=16056     Len=0       377     1837     51501     10.0.0.14     TCP     45083     bgp [Ack] Seq=298     Ack=329     win=16056     Len=0       377     1834     51501     10.0.0.14     TCP     5105     bsc/>seq=298     Ack=329     win=16056     Len=0       377     1835     5150     10.0.0.14     TCP     5105     Destination port: 33448	350 1784,7292 351 1786,1538 352 1787,7305 353 1790,7301 354 1793,7479 355 1795,7941 356 1796,7501 358 1799,7501 358 1799,7501 358 1799,7501 358 1804,9027 361 1804,9077 361 1804,9077 363 1804,9073 364 1804,9053 364 1805,0200 365 1805,21803 367 1806,1335	67         10.0         14           88         Cisco_96:f2:c0         97         10.0         0.14           80         10.0         0.14         10         15:cc_96:f2:c0           80         10.0         0.14         10         15:cc_96:f2:c0           80         10.0         0.14         10         15:cc_96:f2:c0           80         10.0         0.14         10         10:c         11           10         0.0         0.14         10         10:c         11           10         0.0         0.14         10         10:c         11           10         0.0         0.13         10:c         10:c         11           10         0.0         0.13         10:c         10:d         10:d	255, 255, 255, 255, 255 Cisco_96:F2:C0 255, 255, 255, 255, 255 255, 255, 255, 255, 255 CDP/VTP/DTP/PAgP/VDLD Cisco_96:F2:C0 255, 255, 255, 255 255, 255, 255, 255 255, 255, 255, 255 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 Cisco_96:F2:C0 Cisco_96:F2:C0	LOOP Rep DNS Star LOOP Rep DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star TCP 4500 TCP 4500 BGP OPEN BGP CPEN BGP KEEF DGP KEEF DGP Rep DGP Rep	ya a 0.1kbos 1 0.0 kbos 0.1kbos 0.1kbos 0.1kbos 0.1kbos 1 0.0 kbos 0.1kbos 0.
372 1834.317486 10.0.0.14       10.0.0.13       TCP       bgp > 45063 [ACK] Seq=302 Ack=260 win=16125 Len=0         373 1834.318053 10.0.0.13       10.0.0.14       BGP       KEEPALTVE Message         374 1834.319319 10.0.0.14       10.0.0.13       BGP       VEEPALTVE Message         375 1834.517523 10.0.0.14       10.0.0.13       TCP       bgp Ack] Seq=329 Ack=298 win=16087 Len=0         376 1834.517523 10.0.0.14       10.0.0.13       TCP       bgp Ack] Seq=329 Ack=298 win=16087 Len=0         376 1834.517525 10.0.0.14       10.0.0.14       TCP       45063 > bgp [AcK] Seq=229 Ack=298 win=16056 Len=0         377 1835.781501 10.0.0.14       192.168.4.1       UDP       Source port: 3105 Destination port: 33448	350 1748.7292 351 1766.1538 352 1767.7305 353 1790.7301 354 1793.7479 355 1795.7411 356 1796.7501 358 1799.7501 358 1799.7501 358 1304.9024 361 804.9074 361 804.9074 363 804.9053 364 804.9153 365 805.0200 366 1805.2180 366 1805.2180 367 1806.1536 369 1826.1534	67         10.0.0.14           86         152.0.672.c0           97         10.0.0.14           80         10.0.0.14           910.0.0.14         10.0.0.14           92         10.0.0.14           95         01.0.0.14           92         10.0.0.14           97         10.0.0.14           97         10.0.0.14           97         10.0.0.13           92         10.0.0.13           93         10.0.0.13           91         10.0.0.13           91         10.0.0.13           92         10.0.0.13           91         10.0.0.13           91         10.0.0.13           91         10.0.0.14           91         10.0.0.13           91         10.0.0.13           91         10.0.0.13           91         10.0.0.13           91         10.0.0.14           91         0.0.0.14           91         0.0.0.14           91         0.0.0.12           91         0.0.0.14           91         0.0.0.12           91         0.0.0.13           92         0.0.0.14	255, 255, 255, 255, 255 Cisc_0ef; 72:00 255, 255, 255, 255, 255 255, 255, 255, 255 255, 255, 255, 255 255, 255, 255, 255 CDP/VTP/DTP/PAgP/UDLD Cisc_0ef; 72:00 255, 255, 255, 255 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 14 Cisc_0ef; 72:00 Cisc_0ef; 72:00	LOOP Rep DNS Star LOOP Rep DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star TCP Dev LOOP Rep DNS Star TCP 4500 BGP OPER BGP OPER BGP OPER BGP UPDV TCP 4500 TCP	y y dard query PTR 1.4.168.192.in-addr.arpa hdard query PTR 1.4.168.192.in-addr.arpa hdard query PTR 2.0.0.10.in-addr.arpa hdard query PTR 2.0.0.10.in-addr.arpa (ce ID: Router_A Port ID: FastEthernetO/0 y hdard query PTR 2.0.0.10.in-addr.arpa hdard query PTR 2.0.0.10.in-addr.arpa
373     1834     31804     310.0     0.1     BCP     KÉEPALIVE Message       374     1834     318013     10.0     0.14     10.0     0.13     BCP     UPDATE Message       375     1834     517523     10.0     0.14     10.0     0.13     TCP     bgp > 45063     [ACK]     Seq=329     Ack=298     win=16087     Len=0       376     1834     51804     10.0     0.14     TCP     45063     > bgp     [ACK]     Seq=298     Ack=329     win=16087     Len=0       376     1834     51804     10.0     0.14     TCP     45063     > bgp     [ACK]     Seq=298     Ack=329     win=16056     Len=0       377     1837     781501     10.0     0.14     TCP     5100     pact:     31448	350 1784.7292 351 1786.1538 352 1787.7305 353 1790.7301 354 1793.7479 355 1795.7941 355 1795.7941 355 1795.7941 359 1804.9026 360 1804.9077 362 1804.9077 362 1804.9077 363 1804.9153 364 1804.9153 364 1805.2180 365 1805.2180 366 1805.2180 366 1805.2180 366 1805.2180 367 1805.1335 368 1816.1335	67         10.0.0.14           88         Cisco_96:f2:c0           97         10.0.0.14           80         10.0.0.14           80         10.0.0.14           10         Cisco_96:f2:c0           80         Cisco_96:f2:c0           80         Cisco_96:f2:c0           90         0.0.0.14           77         10.0.0.14           79         10.0.0.13           24         10.0.0.13           24         10.0.0.13           29         10.0.0.14           79         10.0.0.13           29         10.0.0.13           20         10.0.0.14           93         10.0.0.13           93         10.0.0.14           93         10.0.0.13           93         10.0.0.14           103         10.0.0.13	255, 25, 255, 255, 255 Cisco_96:F2:C0 255, 255, 255, 255, 255 255, 255, 255, 255 255, 255, 255, 255 CDP/VTP/DTP/PAgP/VDLD Cisco_96:F2:C0 255, 255, 255, 255 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 Cisco_96:F2:C0 Cisco_	LOOP Rep DNS Star LOOP Rep DNS Star DNS Star DNS Star CDP Dev LOOP Rep DNS Star TCP 4500 BGP OPEN BGP CPE BGP KEE BGP KEE BGP KEE BGP Rep LOOP Rep LOOP Rep	yga ∰ 0.1kbpc
374         1834.319319         10.0.0.14         10.0.0.13         BGP         UPDATE Message           375         1834.517523         10.0.0.14         10.0.0.13         TCP         bgp > 45063         [AcK] Seq=329         Ack=298         win=16087         Len=0           376         1834.517523         10.0.0.14         TCP         45063 > bgp [AcK] Seq=228         Ack=29         win=16087         Len=0           377         1835.761501         10.0.0.14         TCP         45067         Source port: 35105         Destination port: 33448	350         1784.7292           351         1786.1538           353         1790.7301           353         1790.7301           355         1795.7941           355         1795.7941           356         1796.7501           358         1799.7501           358         1796.7501           358         1796.7501           358         1796.7501           358         1804.9024           361         1804.9074           361         1804.9074           361         1804.9074           361         1804.9074           361         1804.9074           361         1804.9074           361         1804.9074           361         1804.9074           361         1804.9074           361         1804.9074           361         1804.9074           361         1804.9074           361         1804.9074           361         1804.9074           361         1804.9074           361         1805.20200           366         1805.20200           366         1805.21804           369	67         10.0.0.14           86         152.0.672:c0           97         10.0.0.14           80         10.0.0.14           91         10.0.0.14           92         10.0.0.14           93         10.0.0.14           95         Cisco_96:f2:c0           93         Cisco_96:f2:c0           93         Cisco_96:12:c0           97         10.0.0.14           97         10.0.0.13           21         10.0.0.13           92         10.0.0.13           92         10.0.0.13           92         10.0.0.13           93         10.0.0.13           93         10.0.0.13           94         10.0.0.13           95         10.0.0.13           91         Cisco_96:f2:c0           93         Cisco_96:f2:c0           94         Cisco_96:f2:c0           95         10.0.0.13	255, 255, 255, 255, 255 Cisc_0ef; 72:00 255, 255, 255, 255, 255 255, 255, 255, 255 255, 255, 255, 255 CDP/VTP/DTP/PAgP/UDLD Cisc_0ef; 72:00 255, 255, 255, 255 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10,	LOOP Rep DNS Star DNS Star Star DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star Star DNS Star DNS Star DN	ya a 0.1kbpc 1 0.0kbpc 8,192.in-addr.arpa yada d query PTR 1.4.168.192.in-addr.arpa hdard query PTR 1.4.168.192.in-addr.arpa hdard query PTR 2.0.0.0.1n-addr.arpa totard query PTR 2.0.0.0.1n-addr.arpa totard query PTR 2.0.0.0.1n-addr.arpa hdard query PTR 2.0.0.1.1n-addr.arpa hdard query PTR 2.0.0.0.1.1n-addr.arpa hdard query PTR 2.0.0.1.1n-addr.arpa hdard query PTR 2.0.0.1.1n-addr.arpa hda
375         1834.51/523         10.0.0.14         10.0.0.13         TCP         bgp > 45063         [AcK]         Seq=329         Ack=329         Ack=298         win=16087         Len=0           376         1834.518014         10.0.0.13         10.0.0.14         TCP         45063 > bgp [AcK]         Seq=298         Ack=329         win=16056         Len=0           377         1835.781501         10.0.0.14         192.168.4.1         UDP         Source port: 35105         Destination port: 3448	350 1744.7292 351 1766.1538 352 1787.7305 353 1790.7301 354 1793.7479 355 1795.7941 355 1795.7941 356 1796.7501 359 1804.9074 360 1804.9074 361 1804.9074 361 1804.9074 363 1804.9153 364 1805.21800 365 1805.22800 365 1805.22800 367 1806.1336 369 1826.1534 369 1826.1534 369 1826.1534 369 1826.1534 370 1834.11866 371 1834.2181 372 1834.31747	67         10.0.0.14           86         cisc.06:f2:c0           97         10.0.0.14           80         10.0.0.14           10         cisc.06:f2:c0           98         cisc.06:f2:c0           98         cisc.06:f2:c0           90         co.0.14           97         10.0.0.14           97         10.0.0.13           22         10.0.0.13           24         10.0.0.13           24         10.0.0.13           29         10.0.0.14           97         10.0.0.13           20         10.0.0.13           21         10.0.0.13           20         10.0.0.14           10         10.0.0.13           10         10.0.0.13           10         10.0.0.14           10         10.0.0.13           10         10.0.0.13           10         15:c0.06:f2:c0           93         15:c0.01:3           10         12:c0.5:1           10         10.0.0:13           26         10.0.0:13           26         10.0.0:13           26         10.0.0:14	255, 255, 255, 255 Cisc_0, 96; 72:00 255, 255, 255, 255 255, 255, 255, 255 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 1	LOOP Rep DNS Star LOOP Rep DNS Star DNS Star DNS Star DNS Star DNS Star CDP Dev LOOP Rep DNS Star TCP 4500 BGP OPEN BGP CPE BGP KEE BGP WED TCP 4500 BGP MED TCP 4500 BGP OPEN BGP WED TCP 4500 COP Rep LOOP REP	yga ∰ 0.1kbpc ∰ 0.0kbpc ₿.192.in-addr.arpa y Haard query PTR 1.4.168.192.in-addr.arpa Haard query PTR 1.4.168.192.in-addr.arpa Haard query PTR 2.0.0.10.in-addr.arpa (cc ID: Router_A Port ID: FastEthernet0/0 y Haard query PTR 2.0.0.10.in-addr.arpa Haard query PTR 2.0.10.in-addr.arpa Haard query PTR 2.0.0.10.in-addr.arpa Haard query PTR 2.0.0.10.in-addr.arpa Haard query PTR 2.0.10.in-addr.arpa Haard query PTR 2.0.10.in-addr.arpa Haard query PTR 2.0.0.10.in-addr.arpa Haard query PTR 2.0.0.10.in-addr.arpa Haard query PTR 2.0.0.10.in-addr.arpa Haard query PTR 2.0.0.10.in-addr.arpa Ha
376         1834.518014         10.0.0.13         10.0.0.14         TCP         45063         > bgp         [Ack]         Seq=298         Ack=329         win=16056         Len=0           377         1835.781501         10.0.0.14         192.168.4.1         UDP         Source port:         35105         Destination port:         33448	350         17.84         .7292           351         17.86         .15.84           352         17.87         .7305           353         17.90         .7301           354         17.93         .7479           355         17.95         .7411           356         17.96         .7501           358         17.99         .7501           358         17.99         .7501           358         17.99         .7501           358         17.99         .7501           358         17.99         .7501           358         1.8049024         .9027           361         18.049027         .962           361         18.049024         .9036           361         18.049024         .9037           361         18.049155         .963           364         18.061535         .966           366         18.061535         .968           370         18.341186         .971           371         18.343143         .973	67         10.0.0         14           88         Cisco_96:f2:c0         97         10.0.0         14           88         Cisco_96:f2:c0         93         10.0.0         14           10         Cisco_96:f2:c0         93         10.0.0         14           10         Cisco_96:f2:c0         93         01.0.0         14           95         Cisco_96:f2:c0         93         10.0.0         14           97         10.0.0         14         10         11.0         11.1           92         10.0.0         13         10.0         13         10.0         13           21         10.0.0         13         10.0         14         10.1         10.0         14           29         10.0.0         13         10.0         14         10.0         10.0         13           30         10.0.0         14         10.0         14         10.0         14         10.0         10.0         14         10.0         10.0         13         10.0         11.1         10.0         14         10.0         11.0         10.0         11.1         10.0         10.0         11.1         10.0         11.1         10.0	255, 255, 255, 255, 255 Cisco_96:f2:C0 255, 255, 255, 255, 255 255, 255, 255, 255, 255 255, 255, 255, 255 CDP/VTP/0TP/PAgP/UDLD Cisco_96:f2:C0 255, 255, 255, 255 255, 255 255, 255, 255 255, 255, 255 255, 2	LOOP         Rep           DNS         Stain           LOOP         Rep           DNS         Stain           TCP         BgP           DPE         BGP           BGP         OPE           BGP         OPE           BGP         OPE           BGP         OPE           BGP         UPD/           COP         Rep           LOOP         Rep           LOOP         Rep           BGP         UPD/           GP         UPD/           GP         UPD/           TCP         BgP           BGP         UPL/           BGP         UPL/           BGP         UPL/           BGP         UPL/           BGP         UPL/           BGP         UPL/ <td>y ga → 0.1kbps ↑ 0.0 kbps ↑ 0.0 kbps ↓ 0.1 kbps ↓ 0.1 kbps ↑ 0.0 kbps ↓ 0.1 kbps ↑ 0.0 kbps ↓ 0.1 kbps ↓ 0.1</td>	y ga → 0.1kbps ↑ 0.0 kbps ↑ 0.0 kbps ↓ 0.1 kbps ↓ 0.1 kbps ↑ 0.0 kbps ↓ 0.1 kbps ↑ 0.0 kbps ↓ 0.1
377 1835.781501 10.0.0.14 192.168.4.1 UDP Source port: 35105 Destination port: 33448	350         1744.7292           351         1766.1538           352         1787.7305           353         1790.7301           354         1793.7479           355         1795.7941           356         1796.7501           358         1799.7301           358         1799.7501           358         1799.7501           358         1799.7501           358         1804.9024           361         1804.9077           362         1804.9074           361         1804.9077           362         1804.9074           361         1804.9077           362         1804.9153           364         1804.9153           365         1805.21800           365         1805.21800           366         1805.21800           370         1834.1186           371         1834.3184           372         1834.3147           373         1834.3143           374         1834.3143	710.0.0.14           86 clsc.06f2:c0           97 10.0.0.14           80 10.0.0.14           93 10.0.0.14           10 clsc.06f2:c0           98 clsc.06f2:c0           97 10.0.0.14           10 clsc.06f2:c0           93 clsc.06f2:c0           93 clsc.06f2:c0           93 clsc.06f2:c1           97 10.0.0.14           97 10.0.0.14           97 10.0.0.13           94 10.0.0.13           92 10.0.0.14           97 10.0.0.14           97 10.0.0.14           97 10.0.0.14           97 10.0.0.13           91 10.0.0.13           92 10.0.0.14           97 10.0.0.14           97 10.0.0.13           91 10.0.0.13           92 10.0.0.14           91 clsc.06f2:c0           93 clsc.06f2:c0           94 clsc.06f2:c0           95 10.0.0.13           98 10.0.0.13           98 10.0.0.14           91 0.0.0.14           91 0.0.0.14	$\begin{array}{c} 255, 255, 255, 255, 255\\ Clac_0, 96^+ f2: C0\\ 255, 255, 255, 255, 255\\ 255, 255, 255$	LOOP Rep DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star DNS Star TCP Dev LOOP Rep DNS Star TCP 4500 BGP OPEN BGP OPEN BGP UPD/ RGP UPD/ BGP	yga ∰ 0.1kbpc
	350         17.84         .7292           351         17.86         .15.84           352         17.87         .7305           352         17.87         .7305           353         17.90         .7301           354         17.93         .7479           355         17.96         .7501           356         17.96         .7501           358         17.99         .7501           358         17.99         .7501           358         17.90         .7501           358         17.90         .7501           358         17.90         .7501           358         17.90         .7501           358         17.90         .7501           358         17.90         .7501           359         18.04         .9073           363         18.05         .2000           367         18.06         .1305           368         18.16         .1335           370         18.34         .1186           371         18.34         .3101           373         18.34         .3103           374         18.34	67         10.0.0.14           88         Cisco_96:f2:c0           97         10.0.0.14           80         10.0.0.14           80         10.0.0.14           10         Cisco_96:f2:c0           80         Cisco_96:f2:c0           80         Cisco_96:f2:c0           80         Cisco_96:f2:c0           90         Cisco_96:f2:c0           91         Cisco_96:f2:c0           91         Cisco_96:f2:c0           91         Cisco_96:f2:c0           93         Cisco_96:f2:c0           91         Cisco_96:f2:c0           92         Cisco_96:f2:c0           93         Cisco_96:f2:c0      <	255, 25, 255, 255, 255 Cisco_96:F2:C0 255, 255, 255, 255, 255 255, 255, 255, 255, 255 255, 255, 255, 255 CDP/VTP/DTP/PAgp/VDLD Cisco_96:F2:C0 255, 255, 255, 255 255, 255, 255, 255 255, 255, 255, 255 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 13 10, 0, 0, 13 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 13 10, 0, 0, 13 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10,	LOOP Rep DNS Star DNS Star Star Star Star DNS Star DNS Star DNS Star Star Star Star DNS Star Star Star DNS Star Star Star Star Star DNS Star Star Star Star Star Star Star Star	y ga a 0.1kbpc ↑ 0.0kbpc 8.192.in-addr.arpa y dard query PTR 1.4.168.192.in-addr.arpa ddard query PTR 1.4.168.192.in-addr.arpa ddard query PTR 2.0.0.10.in-addr.arpa (ce ID: Router_A Port ID: FastEthernet0/0 y ddard query PTR 2.0.0.10.in-addr.arpa ddard query PTR 2.0.0.10.in-addr.a
378 1835 781914 10 0 0 1 3 10 0 0 14 TCMP Destination unreachable (Port unreachable)	350         1744.7292           351         1766.1538           352         1787.7305           353         1790.7301           354         1793.7479           355         1795.7941           356         1796.7501           358         1799.7501           358         1799.7501           358         1799.7501           358         1799.7501           358         1804.9026           361         1804.9047           361         1804.9047           361         1804.9045           361         1804.9045           361         1804.9045           361         1804.9045           361         1804.9045           361         1804.915           361         1804.915           361         1805.2180           361         1805.2180           371         1834.12681           371         1834.3141           373         1834.3144           374         1834.3143           376         1834.5180	67         10.0.0.14           86         152.0.672:c0           97         10.0.0.14           80         10.0.0.14           10         0.5cc_96:f2:c0           98         0:s0.0.14           10         0.5cc_96:f2:c0           98         0:s0.0.14           97         10.0.0.14           97         10.0.0.13           21         10.0.0.13           22         10.0.0.14           97         10.0.0.13           21         10.0.0.14           97         10.0.0.13           24         10.0.0.14           91         0:s0.0.14           91         0:s0.0.672:c0           92         (5:sc.96:f2:c0           92         10:s0.0.13           93         10:s0.0.13           93         10:s0.0.13           91         10:s0.0.14           91         10:s0.0.14           91	255, 255, 255, 255, 255 Cisc_0.967; 21:00 255, 255, 255, 255, 255 255, 255, 255, 255 255, 255, 255, 255 255, 255, 255, 255 CDP/VTP/0TP/PAgP/UDL Cisc_0.967; 21:00 255, 255, 255, 255 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0, 13 10, 0, 0, 14 10, 0, 0	LOOP         Rep           DNS         Star           LOOP         Rep           DNS         Star           DS         Star           DNS         Star           TCP         BgP           DPC         4500           LOOP         Rep           BGP         UPD/           TCP         BgP           BGP         UPD/           TCP         BgP           BGP         UPD/           TCP         BgP           BGP         UPD/	yga ∰ 0.1kbpc
	350         17.84         .7292           351         17.86         .1538           352         17.87         .7303           352         17.87         .7303           353         17.90         .7301           354         17.93         .7479           355         17.95         .7417           355         17.96         .7501           359         18.04         .9026           360         18.04         .9027           361         18.04         .9027           361         18.04         .9027           361         18.04         .9027           361         18.04         .9027           361         18.04         .9027           361         18.04         .9027           361         18.04         .9027           361         18.05         .100           361         18.05         .100           361         18.05         .100           361         18.05         .136           368         18.05         .136           368         18.05         .136           370         18.34<.1360	57         10.0.0.14           88         Cisco_96:f2:c0           97         10.0.0.14           80         10.0.0.14           80         10.0.0.14           10         Cisco_96:f2:c0           80         Cisco_96:f2:c0           80         Cisco_96:f2:c0           90         Cisco_96:f2:c0           91         Cisco_96:f2:c0           97         10.0.0.14           97         10.0.0.13           24         10.0.0.13           24         10.0.0.14           97         10.0.0.13           93         10.0.0.14           93         10.0.0.13           93         10.0.0.14           93         10.0.0.13           93         Cisco_96:f2:c0           93         Cisco_96:f2:c0           93         10.0.0.13           93         10.0.0.13           93         10.0.0.14           93         10.0.0.14           93         10.0.0.14           93         10.0.0.14           93         10.0.0.14           93         10.0.0.14	$\begin{array}{r} 255, 255, 255, 255, 255, 255, 255, 255$	LOOP         Rep           DNS         Star           LOOP         Rep           DNS         Star           BGP         OPEN           BGP         OPEN           LOOP         Rep           LOOP         Rep           LOOP         Rep           LOOP         Rep           BGP         UPD           BGP         UP           BGP         UP           BGP         UP           BGP         UP	y ga d 0.1kbpc ↑ 0.0kbpc ↑ 0.0kbpc ↓ 0.0kbpc

#### Analysis

The above traces demonstrate the operations of the BGP protocol. When a BGP router first comes up on the Internet, either for the first time or after being turned off, it establishes connections with the other BGP routers with which it directly communicates. The first thing it

does is download the entire routing table of each neighbouring router. After that it only exchanges much shorter update messages with other routers.

BGP routers send and receive update messages to indicate a change in the preferred path to reach a computer with a given IP address. If the router decides to update its own routing tables because this new path is better, then it will subsequently propagate this information to all of the other neighbouring BGP routers to which it is connected, and they will in turn decide whether to update their own tables and propagate the information further.

BGP uses the TCP/IP protocol on port 179 to establish connections. It has strong security features, including the incorporation of a digital signature in all communications between BGP routers.

Each BGP router contains a Routing Information Base (RIB) that contains the routing information maintained by that router. The RIB contains three types of information:

- Ad-RIBs-In. The unedited routing information sent by neighbouring routers.
- Loc-RIB. The actual routing information the router uses, developed from Adj-RIBs-In.
- Adj-RIBs-Out. The information the router chooses to send to neighbouring routers.
- BGP routers exchange information using four types of messages:
- Open. Used to open an initial connection with a neighbouring router.
- Update. These messages do most of the work, exchanging routing information between neighbouring routers, and contain one of the following pieces of information.
- Withdrawn routes. The IP addresses of computers that the router no longer can route messages to.
- Paths. A new preferred route for an IP address. This path consists of two pieces of information -- the IP address, and the address of the next router in the path that is used to route messages destined for that address.
- Notification. Used to indicate errors, such as an incorrect or unreadable message received, and are followed by an immediate close of the connection with the neighbouring router.
- Keepalive. Each BGP router sends a 19 byte Keepalive message to each neighboring router to let them know that it is still operational about every 30 seconds, and no more often than every three seconds. If any router does not receive a Keepalive message from a neighboring router within a set amount of time, it closes its connection with that router,

and removes it from its Routing Information Base, repairing what it perceives as damage to the network.

• Routing messages are the highest precedence traffic on the Internet, and each BGP router gives them first priority over all other traffic. This makes sense -- if routing information can't make it through, then nothing else will.

## Summary

The layered models of network architecture (both OSI and TCP/IP) make not only the communications process, which is a complicated processes when seen as one monolithic task, a simple, manageable task but also the process of troubleshooting the points of hiccups within the communication system. Looking at the whole issue of encapsulation and decapsulation, the hand-over of data from one layer to the next and back, and the overheads involved, it is perfectly reasonable to question the downside of the layered approach to data communications and networks in terms of the impact of this separation of tasks among the various layers on the performance of internetworking protocols and the overall system.

As a first step to look into the performance issues of the internetworking protocols, it is necessary to identify the metrics used, and evaluate the network performance against these metrics as criteria. This is difficult task in itself because:

- The layered approach to communications system design and internetworking models dictates that the function of each specific protocols span not all the layers of the model
- As a result, each protocol has a specific function and role in the communication process and/or system
- And because each protocol has a specific function and role, which will might call for a different set of algorithms and data structures, each protocol will probably have a different set of metrics that capture its performance criteria

To overcome this challenge, it was seen crucial that the sample set of protocols used in the study should be selected on the basis of their functions in the data communication process; and that each of the protocols be scrutinized separately. A lab environment, with the network diagram shown in the introduction, has been setup to try out and inspect the functions of and mechanisms used by each of the protocols that have been in this study, which included the following (grouped according to their functions and the layers of the OSI reference model they affect:

- Ping, traceroute, ICMP and DHCP
- TCP and UDP

- HTTP, SSH, Telnet and FTP
- ARP and RARP
- Unicast, Multicast and Ethernet
- RIP, OSPF, IS-IS, and BGP

Each of the protocols has been configured in the test-bed network, and the traces of the test runs have been captured using the Open Source Wireshark.

A revision of the generic findings of the study

#### The general performance metrics and their underlying assumptions

The purpose of this study was mainly to identify the various performance metrics of internetworking protocols using a select set of the most commonly used internetworking protocols as sample. If the internetworking model and the communication process is taken as one monolithic task, the performance metrics for the internetwork and data communication system would include the common metrics that have now become more or less marketing buzzwords such as throughput, delay and round-trip times. However, taken separately, and studied as individual autonomous systems, the internetwork protocols will have their own performance criteria and metrics depending on the underlying technologies and algorithms. An example of this would be the difference between the metrics of the different routing protocols (i.e. RIP and OSPF); although they both have the same functionality in the communications network, they have their own unique metrics.

The study also emphasizes that the overall performance of the internetwork communication is the 'sum' of the communications protocols that participate in the communication session. Since some protocols at a certain layer might use the services of another protocol in another layer, depending on the direction of this communication (read encapsulating or otherwise), the performance of the using protocol is also impacted by that of the protocols it depends to do its task or play its role in the communication process.

Next steps on how to improve this work: if there is anything this indicates, it is the need to build performance metrics identification and testing framework that encompasses all internetwork protocols. Most of the RFCs and papers that have been studied throughout this experiment either focused on service performance, and other general metrics such as throughput and delay; however, it appears that throughput and delay and the availability of services is not sufficient to measure the performance of all the protocols. There should be other criteria that can also equally apply to all the internetworking protocols either in use today or will be invented in the future. This is an area I would like to explore more, as it is, in my opinion, an interesting research area.

# Bibliography

- Ethernet Network Performance Differentiation , Ethernet Technology Summit, Session 202 on Broadband Networks, February 24, 2011 <u>http://www.ethernetsummit.com/English/Collaterals/Proceedings/2011/20110224\_S202\_Gum.p</u> df.
- 2. Address Resolution Protocol Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Address\_Resolution\_Protocol.
- 3. ARP and RARP Address Translation, Comptechdocs Repository, http://www.comptechdoc.org/independent/networking/guide/netarp.html.
- 4. Bandwidth, Packets Per Second, and Other Network Performance Metrics Cisco Systems, http://www.cisco.com/web/about/security/intelligence/network\_performance\_metrics.html.
- 5. BGP, Border Gateway Protocol, <u>http://www.livinginternet.com/i/iw\_route\_egp\_bgp.htm</u>.
- 6. Birds-Eye.Net Carrier-Class DHCP Testing Setup, <u>http://www.birds-</u> eye.net/technical archive/carrier class dhcp testing.htm.
- 7. Border Gateway Protocol Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Border\_Gateway\_Protocol.
- 8. Border Gateway Protocol Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Border\_Gateway\_Protocol.
- 9. Border Gateway Protocol: Conformance and Performance Testing :: White Papers :: Ixia -Enabling a Converged World, <u>http://www.ixiacom.com/library/white\_papers/display?skey=bgp</u>.
- 10. CLNS Wikipedia, the free encyclopedia, <u>http://en.wikipedia.org/wiki/CLNS</u>.
- 11. DHCP\_Overview.pdf, <u>http://www.cisco.com/en/US/docs/ios-</u> xml/ios/ipaddr\_dhcp/configuration/15-1mt/DHCP\_Overview.pdf.
- 12. <u>http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.3.540&rep=rep1&type=pdf</u>.
- 13. Ethernet Wikipedia, the free encyclopedia, <u>http://en.wikipedia.org/wiki/Ethernet</u>.
- 14. High Performance Enabled SSH/SCP [PSC], <u>http://www.psc.edu/networking/projects/hpn-ssh/</u>.
- 15. HTTP Compression, <u>http://www.http-compression.com/</u>.
- 16. HTTP Performance Overview, <u>http://www.w3.org/Protocols/HTTP/Performance/</u>.
- 17. IEEE 802.3 ETHERNET, http://www.ieee802.org/3/.
- 18. Intermediate System-to-Intermediate System Protocol [IP Routing] Cisco Systems, http://www.cisco.com/en/US/products/ps6599/products\_white\_paper09186a00800a3e6f.shtml.
- 19. Internet Control Message Protocol Wikipedia, the free encyclopedia, <u>http://en.wikipedia.org/wiki/Internet Control Message Protocol</u>.
- Investigations and Performance Evaluation of Dynamic Routing Protocol With New Proposed Protocol for WAN, from MAHARAJA AGRASEN INSTITUTE OF TECHNOLOGY - White Papers, Webcasts and Case Studies - ZDNet,
   http://whitepapers.zdnet.com/abstract.acpy2docid=2240867

http://whitepapers.zdnet.com/abstract.aspx?docid=3240867.

21. IS-IS - Wikipedia, the free encyclopedia, <u>http://en.wikipedia.org/wiki/IS-IS</u>.

- 22. Key features and algorithms of the BGP-4 protocol., <u>http://freesoft.org/CIE/RFC/1774/2.htm</u>.
- Measuring IP Network Performance The Internet Protocol Journal Volume 6, Number 1 -Cisco Systems, <u>http://www.cisco.com/web/about/ac123/ac147/archived\_issues/ipj\_6-</u> <u>1/measuring\_ip.html</u>.
- 24. OSPF Design Guide Cisco Systems, http://www.cisco.com/en/US/tech/tk365/technologies\_white\_paper09186a0080094e9e.shtml.
- 25. OSPF Packet Details, <u>http://cisco.iphelp.ru/faq/5/ch08lev1sec1.html</u>.
- 26. OSPF Packets, <u>http://www.juniper.net/techpubs/software/junos/junos74/swconfig74-</u> routing/html/ospf-overview7.html.
- 27. Reverse Address Resolution Protocol Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Reverse\_Address\_Resolution\_Protocol.
- 28. RFC 2131 Dynamic Host Configuration Protocol, <u>http://tools.ietf.org/html/rfc2131</u>.
- 29. RFC 4251, <u>http://www.ietf.org/rfc/rfc4251.txt</u>.
- 30. RFC 792 Internet Control Message Protocol (RFC792), <u>http://www.faqs.org/rfcs/rfc792.html</u>.
- 31. RFC 903 A Reverse Address Resolution Protocol (RFC903), http://www.faqs.org/rfcs/rfc903.html.
- 32. Routing protocol Wikipedia, the free encyclopedia, <u>http://en.wikipedia.org/wiki/Routing\_protocol</u>.
- 33. Satellite Internet access Wikipedia, the free encyclopedia, <u>http://en.wikipedia.org/wiki/Satellite\_Internet\_access</u>.
- 34. SSh A Telnet Replacement, <u>http://web.science.mq.edu.au/it/doc/services/ssh/</u>.
- 35. SSH Protocol Overview, <u>http://www.freesoft.org/CIE/Topics/139.htm</u>.
- 36. TCP and UDP performance tuning, <u>http://publib.boulder.ibm.com/infocenter/aix/v6r1/topic/com.ibm.aix.prftungd/doc/prftungd/tc</u> <u>p\_udp\_perf\_tuning.htm</u>.
- 37. TCP/IP Architecture, <u>http://technet.microsoft.com/en-us/library/cc751234.aspx</u>.
- 38. Telnet Wikipedia, the free encyclopedia, <u>http://en.wikipedia.org/wiki/Telnet</u>.
- 39. The Industrial Ethernet Book | Knowledge | Technical Articles | Performance metrics for Industrial Ethernet,

http://www.iebmedia.com/index.php?id=5430&parentid=63&themeid=255&hft=38&showdetail <a href="http://www.iebmedia.com/index.php?id=5430&parentid=63&themeid=255&hft=38&showdetail">http://www.iebmedia.com/index.php?id=5430&parentid=63&themeid=255&hft=38&showdetail</a>

- 40. The TCP/IP Guide Data Link Layer (Layer 2), http://www.tcpipguide.com/free/t\_DataLinkLayerLayer2.htm.
- 41. The TCP/IP Guide TCP and UDP Overview and Role In TCP/IP, <u>http://www.tcpipguide.com/free/t\_TCPandUDPOverviewandRoleInTCPIP.htm</u>.
- 42. Understanding OSPF Routing Webopedia.com, http://www.webopedia.com/DidYouKnow/Computer\_Science/2006/OSPF\_Routing.asp.
- 43. Understanding the Ping and Traceroute Commands Cisco Systems, <u>http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products\_tech\_note09186a00800a6</u> <u>057.shtml</u>.