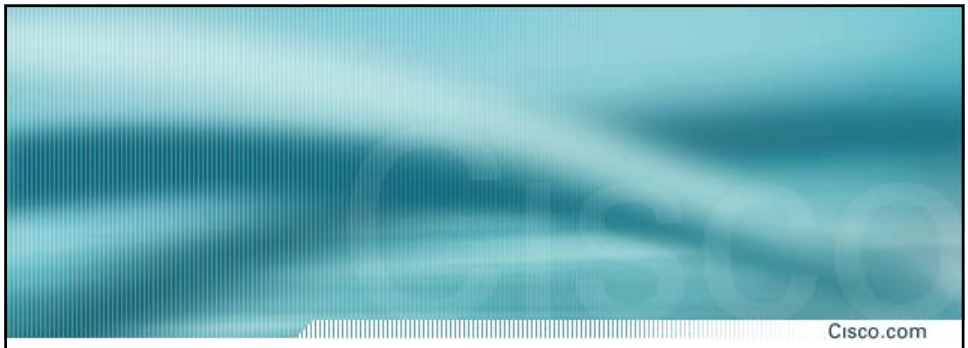


CCNP4
Layer 4 troubleshooting

Halmstad University

Olga Torstensson

035-167575 olga.torstensson@ide.hh.se

Transport-layer networking technologies

- Transport Control Protocol
- User Datagram Protocol
- NetBIOS
- Network Address Translation
- Extended Access Lists

User Datagram Protocol

Cisco.com

Characteristics of UDP

- Is connectionless
- Is unreliable (provides no software checking for message delivery)
- Transmits messages (called user datagrams)
- Does not reassemble incoming messages
- Does not use acknowledgments
- Does not provide flow control

UDP Packet Header

16 bits	16 bits	16 bits	16 bits	16 bits
Source Port	Destination Port	Length	Check Sum	Data...

UDP Header Fields

Field	Description
source port	Number of the calling port
destination port	Number of the called port
length	Length of the segment
checksum	Calculated checksum of the header and data fields
data	Upper-layer protocol data

UDP Communications

Look the curriculum, Animation

User Datagram Protocol

Cisco.com

- **Many higher-layer protocols and applications make use of UDP, including:**
  - **Trivial File Transfer Protocol (TFTP)**
  - **Domain Name Service (DNS)**
  - **NetBIOS Name Resolution (NetBIOS-NS)**
  - **Windows Internet Name Service (WINS)**
  - **Bootstrap Protocol (BootP)**
  - **Dynamic Host Configuration Protocol (DHCP)**
  - **Network Time Protocol (NTP)**
  - **Remote Authentication Dial-In User Service (RADIUS)**
  - **Terminal Access Control Access Control Server (TACACS)**

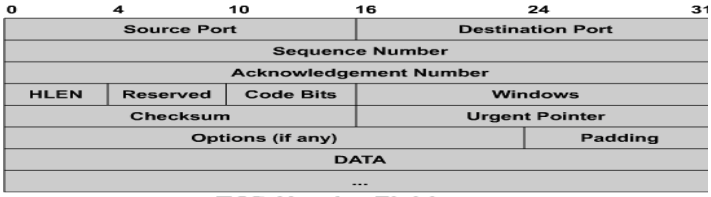
Transport Control Protocol

Cisco.com

Characteristics of TCP

- Is connection-oriented
- Is reliable
- Divides outgoing messages into segments
- Reassembles messages at the destination station
- Re-sends anything not received
- Reassembles messages from incoming segments

TCP Packet Header



TCP Header Fields

Field	Description
source port	Number of the calling port
destination port	Number of the called port
sequence number	Number used to ensure correct sequencing of the arriving data
acknowledgment number	Next expected TCP octet
HLEN	Number of 32-bit words in the header
reserved	Set to zero
code bits	Control functions (such as setup and termination of a session)
window	Number of octets that the sender is willing to accept
checksum	Calculated checksum of the header and data fields
urgent pointer	Indicates the end of the urgent data
option-one option	Maximum TCP segment size
data	Upper-layer protocol data

Standard access control lists

Cisco.com

Recall that access control lists (ACLs) can be implemented on routers to permit and deny traffic that matches predefined profiles. Traffic profiles can be configured to match individual hosts, parts of networks, or entire ranges of networks, and can apply to all IP traffic, or traffic using a specific source or destination port. Access lists can also be used to filter traffic for other operations on the network equipment, particularly network management traffic destined to a network switch or router.

Standard access lists examine only the source address of packets. This means they must be implemented at each ingress point for a protected destination. Implementing the standard access list as close to the protected destination as possible reduces the total number of access lists required.

Extended access control lists

Cisco.com

Extended access lists have more features and can be used to target very specific traffic based on any combination of the following:

- **Source address**
- **Destination address**
- **Source port**
- **Destination port**

Because extended access lists can filter on destination address, they should be implemented as close as possible to the source of the traffic being filtered, typically at the edge of an organization's network. This enables traffic to be examined and filtered before crossing expensive and congested WAN links within the organization.

Network Address Translation

Cisco.com

NAT can be configured in a number of ways:

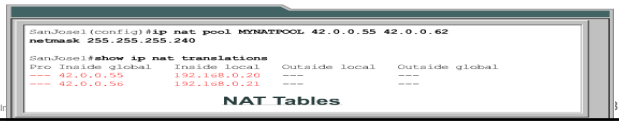
Static table entries

Static tables are manually defined by a network engineer and traditionally define a one-to-one mapping between inside and outside IP addresses so that only the IP address portion of the packet header is altered.

Static NAT has the benefit of offering both connectivity and security because hosts on either side of the NAT router cannot communicate if the administrator has not defined an appropriate NAT table entry.

Dynamic table entries

Dynamic NAT has neither of the problems associated with static NAT. Dynamic NAT creates entries in the NAT table as required and removes them after they have remained idle for a predefined period. Dynamic NAT allows a large number of inside hosts to share a small number of outside addresses. Dynamic NAT also offers greater security than static NAT, because unlike static NAT, entries in a dynamic NAT table are deleted after they have been idle for a short time.



NAT Tables

Dynamic IP Network Address Translation

Cisco.com

NAT with overload and Port Address Translation

- **Dynamic NAT also has a feature called overloading, or Port Address Translation. NAT without overloading operates at the network layer only, and only IP address information is substituted in packet headers. NAT with overloading extends the operation of NAT into the transport layer and UDP and TCP port numbers are included with entries in the NAT table.**
- **Recall from previous curriculum that UDP and TCP have roughly 65,535 associated ports each. It is highly unlikely that a single client host accessing network resources will legitimately need to use all of these ports at the same time.**
- **Because a single inside host does not require all of the ports available on an outside address, NAT overload allows multiple inside hosts to make use of the unused ports on a common outside address. It does this by including the port numbers for a given session in the translation table.**
- **Recall that a single entry in a normal static or dynamic NAT table represents a single host inside the network. In a table for NAT with overload, a single entry now represents a single transport-layer session.**

```
SanJose1(config)#ip nat inside source list 2 pool MYNATPOOL overload

SanJose1#show ip nat translations
Pro Inside global     Inside local       Outside local      Outside global
icmp 42.0.0.55:1536   192.168.0.21:1536  10.0.0.5:1536      10.0.0.5:1536
icmp 42.0.0.55:1536   192.168.0.21:1536  10.0.1.2:1536      10.0.1.2:1536
```

NAT with Overload Table

NetBIOS and NetBEUI

Cisco.com

- **NetBIOS and NetBEUI are a pair of protocols that work together to provide easily configured, broadcast-based networking service for computers running the Microsoft Windows family of operating systems. NetBIOS supports the following network services:**
  - Network name registration and verification
  - Session establishment, termination, and management
  - Reliable session data transfer (connection-oriented)
  - Unreliable datagram data transfer (connectionless)
  - Monitoring and management of network interfaces and lower-layer protocols
- **One of the main advantages of using NetBIOS and NetBEUI is that they are simple to configure. The main failing of NetBIOS is that it uses a broadcast-based non-hierarchical namespace, forcing it to rely on other network layer protocols if used over a routed network.**

NetBIOS Packet Format

Message Type	Flags	Datagram ID
Source IP		
Source Port		Datagram Length
Packet Offset		

Common issues with extended ACL's

Cisco.com

- **Recall that access lists are used to filter all traffic entering and leaving the router. Obviously, the most common issues with extended access lists will be the result of misconfiguration by the network engineer. There are eight areas where misconfigurations commonly occur:**
  - Selection of traffic flow
  - Order of access control elements
  - Implicit “deny any any”
  - Addresses and wildcard masks
  - Selection of transport layer protocol
  - Source and destination port(s)
  - Use of the ‘established’ keyword
  - Uncommon protocols

Gathering information on ACL operation

Cisco.com

- **The command** show ip access-list [*number* | *name*] **is particularly useful for troubleshooting IP access lists. This command displays the detailed elements of a specific access-list in the correct order and the number of packets that have been matched against each element. Alternatively, if no access list number is specified, details of all access lists are shown.**
- **Figure shows the typical output from the** show ip access-list **command.**

```
Router#show ip access-list
Extended IP access list 101
 deny udp any any eq ntp
 permit tcp any any
 permit udp any any eq tftp
 permit icmp any any
 permit udp any any eq domain
```

show ip access-lists

Gathering information on ACL operation

Cisco.com

When viewing the number of access list matches, the hit counters should sometimes be reset using the

clear ip access-list counter [*number* | *name*] **command. This command resets access list counters to zero, making it easier to spot changes in the counters and heavily-matched access list elements. Like the**

show ip access-list **command, this command can be used to clear the counters for only a specific access list by specifying its name or number. It will clear the counters for all IP access lists if no access list name or number is specified. An alternative command**

clear access-list counters [*number* | *name*] **can also be used to clear IP access list statistics.**

```
Router#clear access-list counters 101
```

clear access-list counters

Gathering information on ACL operation

Cisco.com

The command

show ip interface **shows information about the configuration of interfaces running the IP protocol, including information on any access lists configured for inbound and outbound traffic on the interface.**

show ip interface

```
Router#show ip interface fastethernet0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 1.1.1.2/8
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast
  Router Discovery is disabled
--MORE--
```

Common issues with IP NAT

Cisco.com

- **The biggest problem with all NAT technologies is interoperability with other network technologies, especially those that contain or derive information from host network addressing in the packet. Some of these technologies include:**

  BootP and DHCP

  DNS and WINS

  SNMP

  Tunneling and encryption protocols

- BootP and DHCP
  DHCP was developed from BootP. Both protocols are used to manage the automatic assignment of IP addresses to clients. Recall that the first packet that a new client sends is a DHCP-Request broadcast IP packet. The DHCP-Request packet has a source IP address of 0.0.0.0. Because NAT requires both a valid destination and source IP address, BootP and DHCP can have difficulty operating over a router running either static or dynamic NAT.

Common issues with IP NAT

Cisco.com

- **Common NAT misconfigurations**
  One of the more common misconfigurations of NAT is forgetting that it affects both inbound and outbound traffic. An inexperienced network administrator might pre-configure a static NAT entry to redirect inbound traffic to a specific inside 'backup' host. In the event of a failure on the primary system, traffic could be automatically re-directed to the backup system without the administrator having to do anything. This static NAT statement will also change the source address of traffic from that host, possibly resulting in an undesirable (and unexpected) set of behaviors. At best, this is likely to result in sub-optimal operation.

- **Misconfigured timers can also result in unexpected network behavior and suboptimal operation of dynamic NAT. If NAT timers are too short, entries in the NAT table may expire before replies are received and packets will be discarded. This means the intended traffic did not get through and the loss of the packets generates retransmissions, consuming more bandwidth. The NAT router log will also be filled with errors about closed ports.**

NAT Timers Too Long

- Outside host requests IP address for inside host from inside NS server
- Inside NS server returns inside address of inside host
- NAT router cannot alter data payload
- Outside receives inside address for inside host ? cannot route to inside host address

Gathering information on NAT configuration and operation

Cisco.com

show commands

There are two commands in the **show ip nat** group of commands. The **show ip nat statistics** command is used to display statistics on static and dynamic translations on the router, as shown in Figure 1.

The **show ip nat translations** command displays the NAT table currently in operation on the router, listing both static and dynamic NAT entries. (Fig. 2)

debug commands

There is a range of debug commands available for reporting on NAT traffic. A commonly used command is **debug ip nat**.

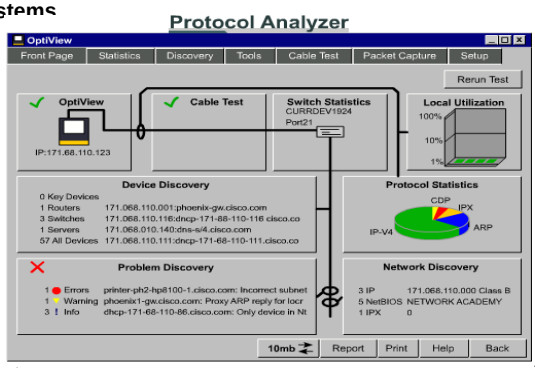
Other useful information

Cisco.com

There are a range of other tools that can be used to help troubleshoot transport layer problems on network devices. These include:

- Protocol analyzers
- Network device system logs
- Centralized logging system (using Syslog)
- Network Management systems

Protocol Analyzer



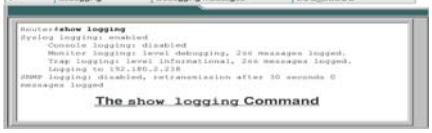
Other useful information

- Local system logging
  Configuring buffered local system logging can also provide a rich source of information when troubleshooting network problems.
- **A local system log can also provide historical information on past events. Logging on local systems is highly configurable and can be used to capture general router events as well as other information of interest, such as** debug **messages.**
- **To configure a router to keep its local log, use the following commands from global configuration mode:**

  Router(config)#logging on
  Router(config)#logging buffered [*buffer size*] [*logging level*]
- **There are seven levels of logging, from 0 for emergency messages (indicating that the router is unusable), to 7 for debugging messages generated by engineer-configured** debug **commands. These levels are summarized in Figure.**

Levels of System Logging

Level	Keyword	Description	Syslog Definition
0	emergencies	System is unusable	LOG_EMERG
1	alerts	Immediate action is needed	LOG_ALERT
2	critical	Critical conditions exist	LOG_CRIT
3	errors	Error conditions exist	LOG_ERR
4	warnings	Warning conditions exist	LOG_WARNING
5	notification	Normal, but significant, condition	LOG_NOTICE
6	informational	Informational messages only	LOG_INFO
7	debugging	Debugging messages	LOG_DEBUG



The show logging Command