



Other Network Hardware

Understanding Networking Concepts

- » **Fundamental network knowledge needed to use Wireshark**
- » **How data traverses a network**
 - Traffic flow concepts from source to destination
- » **Other network hardware**
 - Other network connectivity devices
 - Network security devices

Wireshark & Firewalls

The screenshot shows the Wireshark 1.10.7 interface. The main window displays a packet capture on the 'Local Area Connection' interface. The packet list pane shows several packets, with packet 528 selected. The packet details pane shows the selected packet's structure. A 'Firewall ACL Rules' dialog box is open, displaying the configuration for a rule.

Firewall ACL Rules Dialog:

- Product: Cisco IOS (standard)
- Filter: 10.121.90.180
- Inbound
- Deny
- ! Cisco IOS (standard)
- access-list NUMBER deny host 10.121.90.180

Packet List (Selected Packet 528):

No.	Time	Source	Destination	Protocol	Length	Info
528	21.8707400	10.170.184.185	10.121.90.180	UDP	84	Source port: 62284 Destination port: 21328

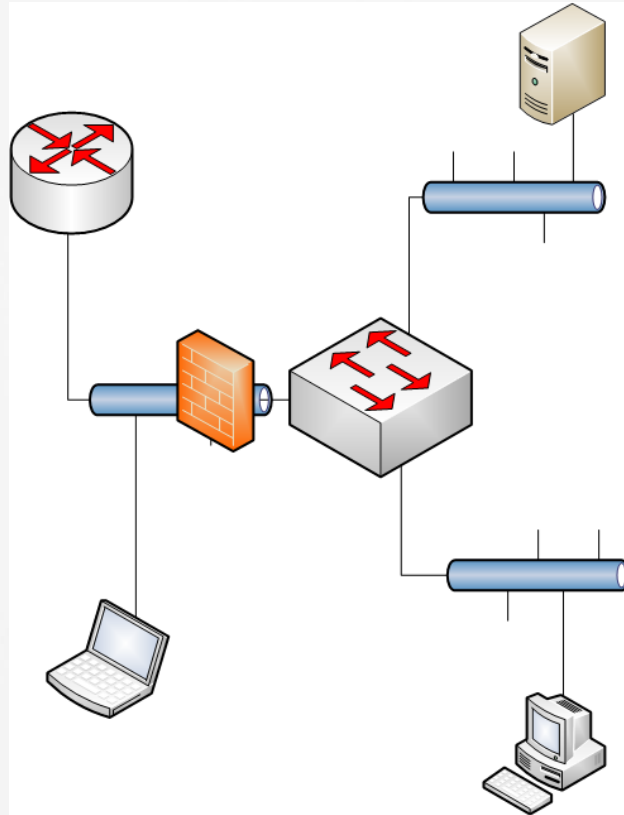
Packet Details (Selected Packet 528):

Layer	Protocol	Length	Info
2	Ethernet II	1440	Destination: 10.121.90.180
3	Internet Protocol Version 4	60	Source: 10.170.184.185 Destination: 10.121.90.180
4	TCP	60	Source port: 62284 Destination port: 21328
5	User Datagram Protocol	24	Destination port: 21328

Network Lab

- » Simple network with Layer 2 and Layer 3, multiple segments a firewall and common scenarios
- » How to create ACLs
 - Cisco ACL
 - Windows Firewall (netsh)
 - Linux (iptables) netfilter
 - Others
- » Troubleshooting problems
 - Use Wireshark to capture traffic
 - Review traffic to analyze network, protocols, and traffic flow

Network Lab



Firewall Concepts

» Firewalls block traffic

- When capturing data, you may not be able to troubleshoot source to destination without modification

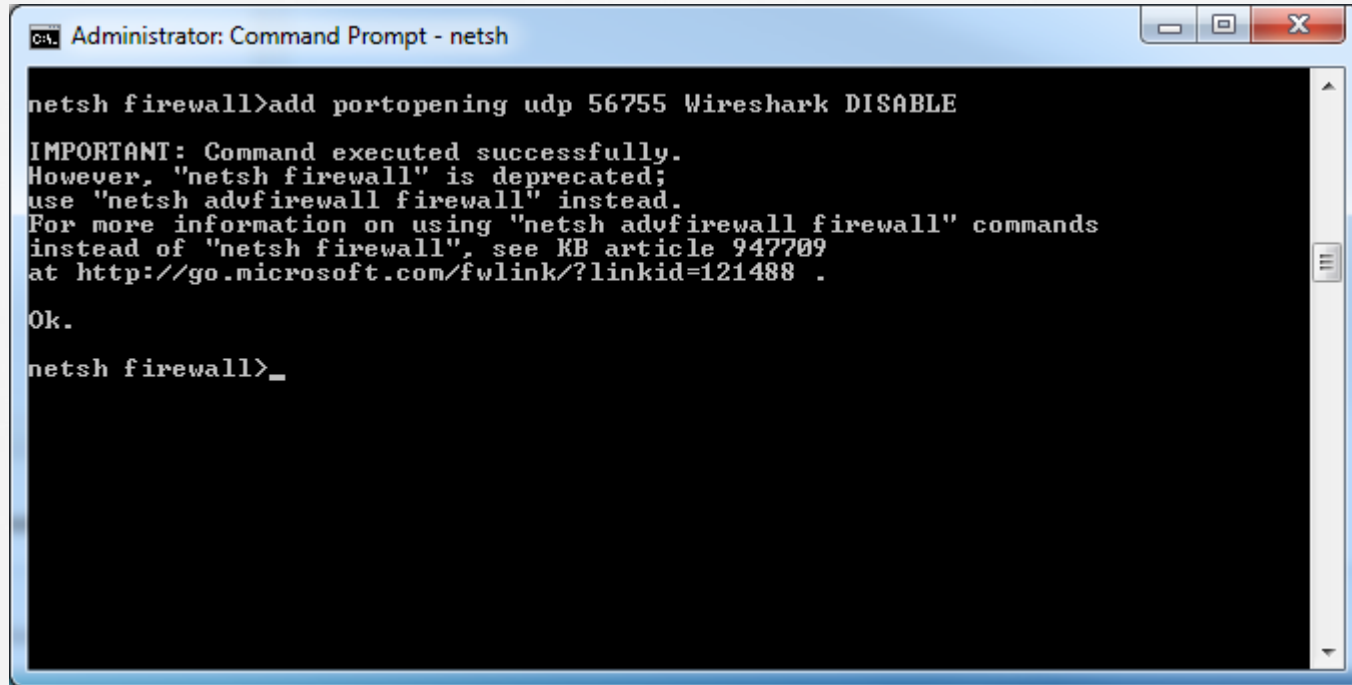
» Firewalls translate traffic

- When using Network Address Translation (NAT), you may confuse your capture data

» Ports and IP addresses

- Firewalls generally block by IP and port

Network Lab



```
Administrator: Command Prompt - netsh

netsh firewall>add portopening udp 56755 Wireshark DISABLE

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .

Ok.

netsh firewall>_
```

Other Hardware

» Hubs

- Create a broadcast domain; may confuse capture

» Load balancers

- Used to send traffic to multiple units to balance load; but rely on a single virtual IP

» Inspection units

- Used to inspect traffic

Capturing Protocol Data

- » Captures protocol data can be inspected for issues
- » Protocol analysis
 - Opens up the data for inspection
 - Helps find problems you cannot see without capturing data for inspection
- » Traffic analysis
 - Used to find bandwidth, latency, and other network issues