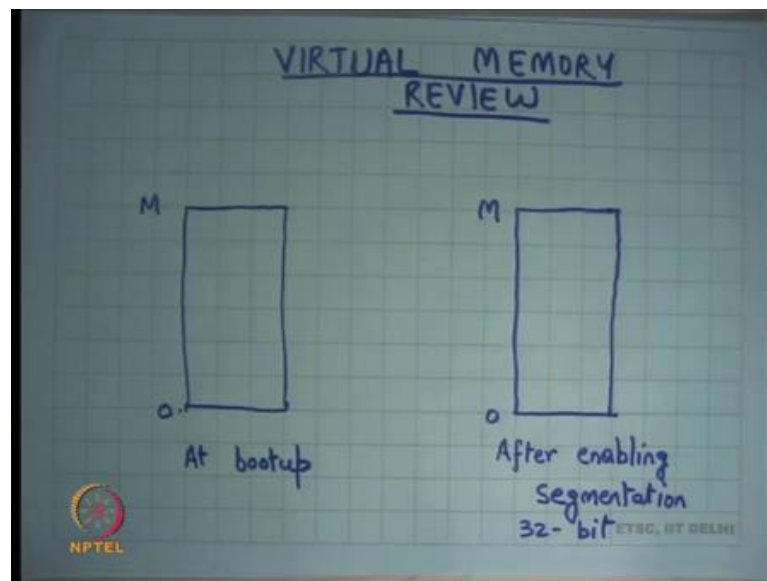


Operating Systems
Prof. Sorav Bansal
Department of Computer Science and Engineering
Indian Institute of Technology, Delhi

Lecture – 15
Setting up page tables for user processes

Welcome to Operating Systems lecture-15.

(Refer Slide Time: 00:30)



So, let us review the virtual memory subsystem as we have been looking at it. So, when you bootup the machine, we said that we start in the physical address space right. And so, if you use address x , then it just if x is less than M , then you had the physical memory at that address x right. You straight away hit the physical memory there is no translation involved. If you try to hit a physical memory address that is greater than the available memory let us say capital M is the amount of physical memory available in your system, then it will throw an error so that is not valid right.

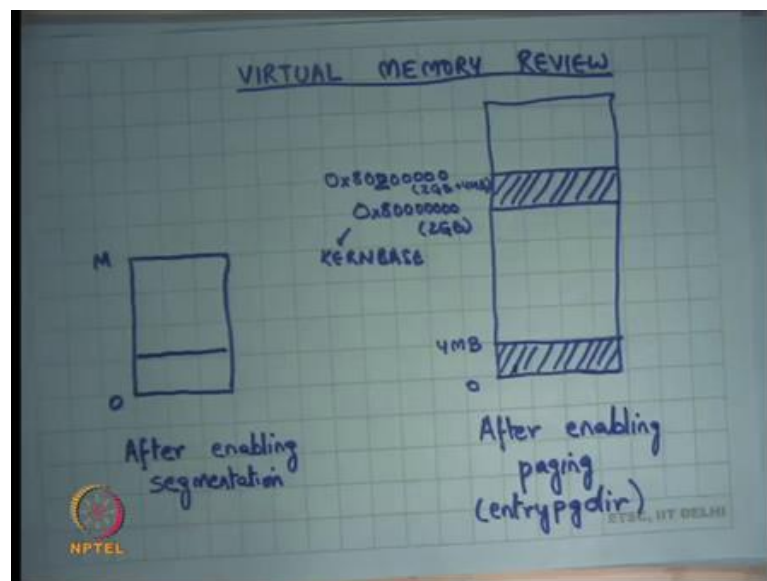
So, at bootup you have this simple system where there is almost no virtual memory subsystem and it is completely flat from 0 to M . Of course, recall that boot in 16-bit mode, so segmentation works in its primitive form, where you can add the segment register after multiplying it by 16 and all that. But for all practical purposes you know the kernel that we are studying sets all segment registers to 0, so you have a flat address space on 0 to M .

Then as soon as you enable segmentation in 32-bit mode, so you switch to you enable segmentation you initialize a global descriptor table and you switch 32-bit mode. The moment you do that you all your addresses are now getting translated through the segment hardware right. Each instruction has a default segment right. So, for example, if you are just making an access through some register, then it will the default segment is `ds` right. The instruction itself `eip` the instruction pointer itself always go through go through `cs` and all that.

So, in theory you could enable segmentation and you could use segmentation to segment your address space. But in the kernel that we are studying it just sets base and limit to 0, base to 0 and limit to $2^{32} - 1$. So, once again I have a completely flat address space right. So, if you would say I want to access address `x`, so let us say you fill in the value `x` into your `eip` register, it just goes into the physical memory at address `x`.

And as long as it is between 0 and `M`, you will see your valid byte; if it is greater than `M`, you will see an error right some kind of an exception will be thrown by the hardware. Similarly, `ESP` or any direct addressing, so these addresses can be generated in many ways through a register, through a direct addressing, through displaced addressing right all those things we have studied already right. In any case they all go through segmentation, and we saw that after enabling segmentation our address space is still the same 0 to `M` ok.

(Refer Slide Time: 03:12)



So, here is another figure. So, after enabling segmentation I had 0 to M, now the boot sector operates in this mode where only segmentation is enabled in 32-bit mode. And in that mode the boot sector, the boot sector was leaving in the first 512 bytes of the disk. So, the boot sector has code to load the kernel. The kernel lives from then sector number 1 till some value, and whatever that value is known to the boot sector the size of the kernel is known to the boot sector. And, so the boot sector loads that many sectors from the disk and puts them in memory.

While it is doing that, the address space is still 0 to M right. So, it picks up that kernel and sticks it somewhere here in this area right. We saw last time that it sticks the kernel at starting at address 1 MB right. So, it starts the it starts pasting the kernel starting at 1 MB and from there on it paste the kernel. And, recall that the size of the kernel was not very big either the size of the kernel was if I remember correctly definitely less than 1 MB right. So, you start you start the kernel from one M, you pick the kernel from that disk stick it at physical address 1 MB, and it will you know at most go till 2 MB right, all the kernel code and the kernel data.

Also recall that the kernel itself has been compiled with virtual addresses. So, all the symbols inside the kernel image have virtual addresses associated with them. So, if I say I want to branch to main, the address of main will be a virtual address right. It will be a virtual address in the sense that will be an address above this value 8 and seven 0s which is also called kern base. In our code, this called the kernel base right. So, all the symbols in our image have addresses above kern base, base or an above 2 GB.

So, all the symbols in that have addresses above 2 GB. So, anytime I dereference a symbol within my kernel code I am going to be trying to access a region above 2 GB. But in this address space, it is not possible right because assuming M is less than 2 GB, if I try to dereference a symbol in the kernel image, I will see an error, I will see an exception right, so not possible at this point.

So, the boot sector, so what the boot sector does it loads the kernel and it jumps to the first instruction of the kernel, and recall at the kernel was stored in elf format so the boot sector knows exactly where to start, and so the kernel the first instruction of the kernel get started. And the first instruction of the kernel leaves in this file called entry dot s

right. Now, the first few instructions of the kernel entry dot s are going to execute in this address space.

So, these instructions have to be very careful, they should not be dereferencing any kernel symbol, because all kernel symbols have addresses above 2 GB right. The moment it dereferences the kernel symbol, I will get an exception, not, it is not legal in this address space right. So, the first thing it does the entry dot s file does is it change changes this address space by enabling paging right. So, it enables paging and it uses a page directory called entry page directory right.

And we saw last time that this entry page directory implements an address space where the first 4 MB are mapped identically. So, if you access an address x within 0 to 4 MB, you will hit physical memory at address x right. On the other hand, it also maps this address kern base to kern base + 4 MB to the same location 0 to 4 MB right. So, if you access address kern base + x , and assuming x is less than 4 MB, then you will hit physical address x right, so that is how the entry page dir was configured.

And, so the entry dot s code just switches from this address space to this address space as soon as it enables paging and check sub CR3 point to entry page dir right. So, it points CR3 point to entry page dir enables paging and suddenly I am running in this address space. Recall that because the kernel itself all the instructions the entry dot s file itself was living in you know less than 4 MB space, so we set from 1 MB to 2 MB let say all the addresses you know the eip and ESP still remain valid, because the addresses from here are identical here 0 to 4 MB right. So, those remain valid.

You do not know it is not like you know I am standing on the ground and the ground has been taken away from it is not true because this as long as the kernel is less than 4 MB, the kernel safely mapped right, so the next instruction can execute alright. So, you enable paging, but ensure you ensured that the ground that I am standing on still stays as soon as I switch the address space right ok. But in this new table, there is an extra mapping and this extra this new this table is going to be used to switch from here to here right.

Recall that the kernel all the symbols in the kernel have values which are in this range. So, I should not be dereferencing any symbol from here. The only thing I am going to do is I am going to look, so in this there are some symbols likes there is the region that is allocated as stack right. So, we saw so let us look at the entry dot s file on sheet 10.

(Refer Slide Time: 08:39)

```
Aug 28 14:35 2012 xv6/entry.S Page 2

1050 orl    $(CRO_PG|CRO_WP), %eax
1051 movl   %eax, %cr0
1052
1053 # Set up the stack pointer.
1054 movl   $(stack + KSTACKSIZE), %esp
1055
1056 # Jump to main(), and switch to executing at
1057 # high addresses. The indirect call is needed because
1058 # the assembler produces a PC-relative instruction
1059 # for a direct jump.
1060 movl   %main, %eax
1061 jmp    *%eax
1062
1063 .comm stack, KSTACKSIZE
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
```

And we will see there is this instruction which is loading this value stack plus KSTACKSIZE into esp. KSTACKSIZE is a constant. Stack is the symbol that has been declared here right. So, kstack is the symbol in the kernel and recall I am saying that all symbols in the kernel have been compiled to have addresses in the kernel virtual address space which is above kern base right. So, the stack the value of stack will be some you know kern based plus something above kern base and so that plus KSTACKSIZE, KSTACKSIZE is let say you know 4096 bytes, so that variable is loaded into esp.

Recall that at this point the paging is already been enabled, so this address should be a valid address. I should be able to dereference esp, because I am operating in this address space right. In this address space esp will be pointing somewhere here. And so, when I dereference it, I will get right value right. So, I was able, so notice that the I have I have only started reading the kernel symbols after I enabled paging.

(Refer Slide Time: 10:05)

```
1072 .text
1073 .globl multiboot_header
1074 multiboot_header:
1075     #define magic 0x1badb002
1076     #define flags 0
1077     .long magic
1078     .long flags
1079     .long (~magic-flags)
1080
1081 # By convention, the _start symbol specifies the ELF entry point.
1082 # Since we haven't set up virtual memory yet, our entry point is
1083 # the physical address of 'entry'.
1084 .globl _start
1085 _start = VZP_W0(entry)
1086
1087 # Entering xv6 on boot processor, with paging off.
1088 .globl entry
1089 entry:
1090     # Turn on page size extension for 4Mbyte pages
1091     movl    %cr4, %eax
1092     orl     $(CR4_PSE), %eax
1093     movl    %eax, %cr4
1094     # Set page directory
1095     movl    $(VZP_W0(entrypgdir)), %eax
1096     movl    %eax, %cr3
1097     # Turn on paging.
1098     movl    %cr0, %eax
1099     NPTEL
```

Before I enabled paging, this code did not read any kernel symbols except that one kernel symbol that was read was entry page dir, but it was converted to its physical address before it was loaded into CR3. In any case CR3 is going to take a physical address. So, it is ok, and physical address is already mapped right. So, this piece of code in entry dot s is very carefully written. There is some amount of tricks involved in this kind of code.

And, this kind of tricks you can only see if you are actually looking at some kind of you know real code right. So, if you know if you find this interesting, you should probably go and single step and see exactly what is happening you know as soon as you turn on paging what addresses become valid, what remain invalid, what were valid earlier and have become invalid now, what were invalid earlier have become valid now etcetera, etcetera right. So, it is interesting ok.

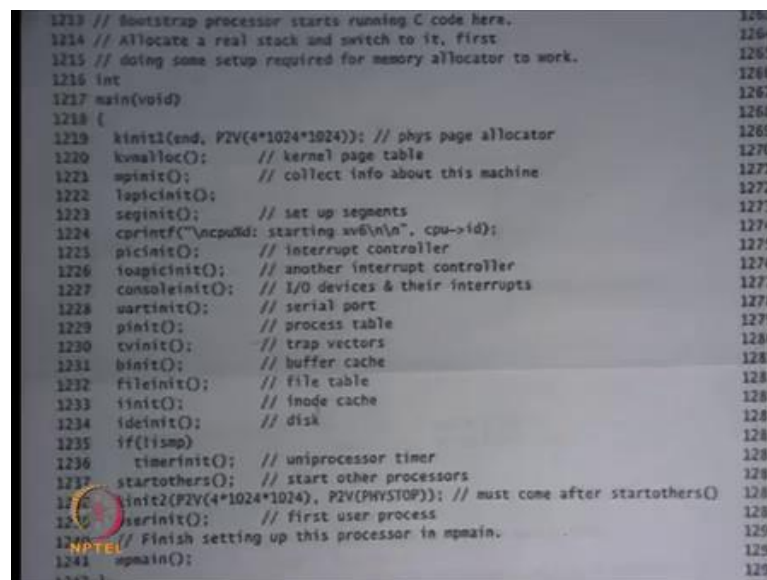
And then you basically, so at this point though you no need to any conversions from v to p right because stack having an address above 2 GB is a valid address, you already in the new address space. Similarly, main is a kernel symbol which will also have an address which is above kern base. And what you are going to do is you are going to move jump to main right. And the moment you do that, you have reloaded your eip with the kernel virtual address which is above kern base. So, you loaded esp with the kernel virtual

address here appropriately, and here you are going to load the eip with the kernel virtual address ok.

So, at this point, so far, my eip and esp were pointing somewhere here, I have reloaded esp to point here and it is standing on solid ground. And then I jump to main, and once again eip now points here. So, now both my esp and eip point here. And from now on I will basically be executing in this space completely because I have forgotten about all my addresses here; anything I dereference from the kernel will have addresses in this space.

So, from now on I just execute in the space right. So, from now on it is just normal plain c code that can execute you know just plain dereferencing should work right. But this kind of tricky code has to be written in assembly, because you know c does not understand this different address spaces and all that kind of stuff, it is very tricky the programmer has carefully done this very carefully done this alright. So, and so we said let us look at, so it is now going to jump to main.

(Refer Slide Time: 12:47)

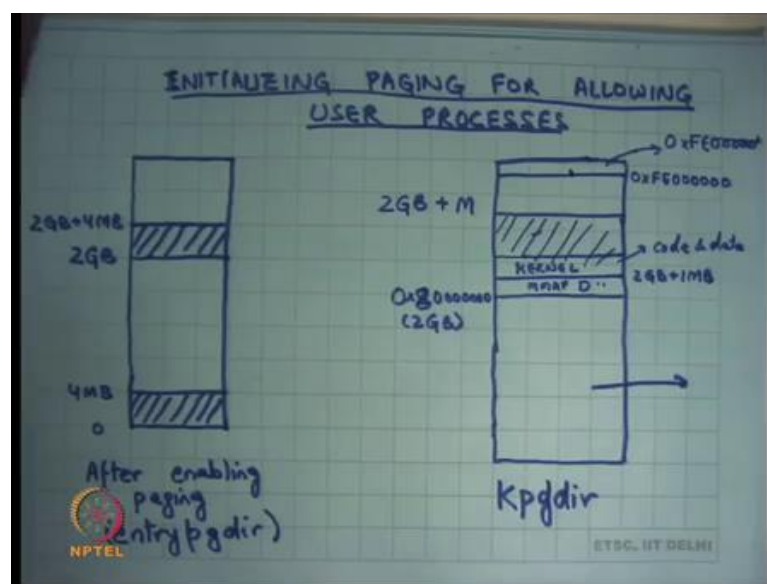
A screenshot of assembly code, likely from a debugger or a disassembler. The code is written in a mix of assembly and C-like syntax. It starts with a comment: "1213 // bootstrap processor starts running C code here." followed by "1214 // Allocate a real stack and switch to it, first". Then "1215 // doing some setup required for memory allocator to work." and "1216 int". The main function is defined as "1217 main(void)". The code then enters a block "1218 {" and contains several function calls: "1219 kinit1(end, P2V(4*1024*1024)); // phys page allocator", "1220 kmalloc(); // kernel page table", "1221 mpinit(); // collect info about this machine", "1222 lapicinit();", "1223 seginit(); // set up segments", "1224 cprintf("xcpuid: starting xv6\n\n", cpu->id);", "1225 picinit(); // interrupt controller", "1226 ioapicinit(); // another interrupt controller", "1227 consoleinit(); // I/O devices & their interrupts", "1228 uartinit(); // serial port", "1229 pinit(); // process table", "1230 tvinit(); // trap vectors", "1231 binit(); // buffer cache", "1232 fileinit(); // file table", "1233 iinit(); // inode cache", "1234 idinit(); // disk", "1235 if(tismp)", "1236 timerinit(); // uniprocessor timer", "1237 startothers(); // start other processors", "1238 init2(P2V(4*1024*1024), P2V(PHYSTOP)); // must come after startothers()", "1239 userinit(); // first user process", "1240 // Finish setting up this processor in mpmain.", "1241 mpmain();". The code ends with "1242 }". The line numbers on the right side of the code are 1260, 1261, 1262, 1263, 1264, 1265, 1266, 1267, 1268, 1269, 1270, 1271, 1272, 1273, 1274, 1275, 1276, 1277, 1278, 1279, 1280, 1281, 1282, 1283, 1284, 1285, 1286, 1287, 1288, 1289, 1290, 1291, 1292, 1293, 1294, 1295, 1296, 1297, 1298, 1299, 1300, 1301, 1302, 1303, 1304, 1305, 1306, 1307, 1308, 1309, 1310, 1311, 1312, 1313, 1314, 1315, 1316, 1317, 1318, 1319, 1320, 1321, 1322, 1323, 1324, 1325, 1326, 1327, 1328, 1329, 1330, 1331, 1332, 1333, 1334, 1335, 1336, 1337, 1338, 1339, 1340, 1341, 1342, 1343, 1344, 1345, 1346, 1347, 1348, 1349, 1350, 1351, 1352, 1353, 1354, 1355, 1356, 1357, 1358, 1359, 1360, 1361, 1362, 1363, 1364, 1365, 1366, 1367, 1368, 1369, 1370, 1371, 1372, 1373, 1374, 1375, 1376, 1377, 1378, 1379, 1380, 1381, 1382, 1383, 1384, 1385, 1386, 1387, 1388, 1389, 1390, 1391, 1392, 1393, 1394, 1395, 1396, 1397, 1398, 1399, 1400, 1401, 1402, 1403, 1404, 1405, 1406, 1407, 1408, 1409, 1410, 1411, 1412, 1413, 1414, 1415, 1416, 1417, 1418, 1419, 1420, 1421, 1422, 1423, 1424, 1425, 1426, 1427, 1428, 1429, 1430, 1431, 1432, 1433, 1434, 1435, 1436, 1437, 1438, 1439, 1440, 1441, 1442, 1443, 1444, 1445, 1446, 1447, 1448, 1449, 1450, 1451, 1452, 1453, 1454, 1455, 1456, 1457, 1458, 1459, 1460, 1461, 1462, 1463, 1464, 1465, 1466, 1467, 1468, 1469, 1470, 1471, 1472, 1473, 1474, 1475, 1476, 1477, 1478, 1479, 1480, 1481, 1482, 1483, 1484, 1485, 1486, 1487, 1488, 1489, 1490, 1491, 1492, 1493, 1494, 1495, 1496, 1497, 1498, 1499, 1500, 1501, 1502, 1503, 1504, 1505, 1506, 1507, 1508, 1509, 1510, 1511, 1512, 1513, 1514, 1515, 1516, 1517, 1518, 1519, 1520, 1521, 1522, 1523, 1524, 1525, 1526, 1527, 1528, 1529, 1530, 1531, 1532, 1533, 1534, 1535, 1536, 1537, 1538, 1539, 1540, 1541, 1542, 1543, 1544, 1545, 1546, 1547, 1548, 1549, 1550, 1551, 1552, 1553, 1554, 1555, 1556, 1557, 1558, 1559, 1560, 1561, 1562, 1563, 1564, 1565, 1566, 1567, 1568, 1569, 1570, 1571, 1572, 1573, 1574, 1575, 1576, 1577, 1578, 1579, 1580, 1581, 1582, 1583, 1584, 1585, 1586, 1587, 1588, 1589, 1590, 1591, 1592, 1593, 1594, 1595, 1596, 1597, 1598, 1599, 1600, 1601, 1602, 1603, 1604, 1605, 1606, 1607, 1608, 1609, 1610, 1611, 1612, 1613, 1614, 1615, 1616, 1617, 1618, 1619, 1620, 1621, 1622, 1623, 1624, 1625, 1626, 1627, 1628, 1629, 1630, 1631, 1632, 1633, 1634, 1635, 1636, 1637, 1638, 1639, 1640, 1641, 1642, 1643, 1644, 1645, 1646, 1647, 1648, 1649, 1650, 1651, 1652, 1653, 1654, 1655, 1656, 1657, 1658, 1659, 1660, 1661, 1662, 1663, 1664, 1665, 1666, 1667, 1668, 1669, 1670, 1671, 1672, 1673, 1674, 1675, 1676, 1677, 1678, 1679, 1680, 1681, 1682, 1683, 1684, 1685, 1686, 1687, 1688, 1689, 1690, 1691, 1692, 1693, 1694, 1695, 1696, 1697, 1698, 1699, 1700, 1701, 1702, 1703, 1704, 1705, 1706, 1707, 1708, 1709, 1710, 1711, 1712, 1713, 1714, 1715, 1716, 1717, 1718, 1719, 1720, 1721, 1722, 1723, 1724, 1725, 1726, 1727, 1728, 1729, 1730, 1731, 1732, 1733, 1734, 1735, 1736, 1737, 1738, 1739, 1740, 1741, 1742, 1743, 1744, 1745, 1746, 1747, 1748, 1749, 1750, 1751, 1752, 1753, 1754, 1755, 1756, 1757, 1758, 1759, 1760, 1761, 1762, 1763, 1764, 1765, 1766, 1767, 1768, 1769, 1770, 1771, 1772, 1773, 1774, 1775, 1776, 1777, 1778, 1779, 1780, 1781, 1782, 1783, 1784, 1785, 1786, 1787, 1788, 1789, 1790, 1791, 1792, 1793, 1794, 1795, 1796, 1797, 1798, 1799, 1800, 1801, 1802, 1803, 1804, 1805, 1806, 1807, 1808, 1809, 1810, 1811, 1812, 1813, 1814, 1815, 1816, 1817, 1818, 1819, 1820, 1821, 1822, 1823, 1824, 1825, 1826, 1827, 1828, 1829, 1830, 1831, 1832, 1833, 1834, 1835, 1836, 1837, 1838, 1839, 1840, 1841, 1842, 1843, 1844, 1845, 1846, 1847, 1848, 1849, 1850, 1851, 1852, 1853, 1854, 1855, 1856, 1857, 1858, 1859, 1860, 1861, 1862, 1863, 1864, 1865, 1866, 1867, 1868, 1869, 1870, 1871, 1872, 1873, 1874, 1875, 1876, 1877, 1878, 1879, 1880, 1881, 1882, 1883, 1884, 1885, 1886, 1887, 1888, 1889, 1890, 1891, 1892, 1893, 1894, 1895, 1896, 1897, 1898, 1899, 1900, 1901, 1902, 1903, 1904, 1905, 1906, 1907, 1908, 1909, 1910, 1911, 1912, 1913, 1914, 1915, 1916, 1917, 1918, 1919, 1920, 1921, 1922, 1923, 1924, 1925, 1926, 1927, 1928, 1929, 1930, 1931, 1932, 1933, 1934, 1935, 1936, 1937, 1938, 1939, 1940, 1941, 1942, 1943, 1944, 1945, 1946, 1947, 1948, 1949, 1950, 1951, 1952, 1953, 1954, 1955, 1956, 1957, 1958, 1959, 1960, 1961, 1962, 1963, 1964, 1965, 1966, 1967, 1968, 1969, 1970, 1971, 1972, 1973, 1974, 1975, 1976, 1977, 1978, 1979, 1980, 1981, 1982, 1983, 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 2680, 2681, 2682, 2683, 2684, 2685, 2686, 2687, 2688, 2689, 2690, 2691, 2692, 2693, 2694, 2695, 2696, 2697, 2698, 2699, 2700, 2701, 2702, 2703, 2704, 2705, 2706, 2707, 2708, 2709, 2710, 2711, 2712, 2713, 2714, 2715, 2716, 2717, 2718, 2719, 2720, 2721, 2722, 2723, 2724, 2725, 2726, 2727, 2728, 2729, 2730, 2731, 2732, 2733, 2734, 2735, 2736, 2737, 2738, 2739, 2740, 2741, 2742, 2743, 2744, 2745, 2746, 2747, 2748, 2749, 2750, 2751, 2752, 2753, 2754, 2755, 2756, 2757, 2758, 2759, 2760, 2761, 2762, 2763, 2764, 2765, 2766, 2767, 2768, 2769, 2770, 2771, 2772, 2773, 2774, 2775, 2776, 2777, 2778, 2779, 2780, 2781, 2782, 2783, 2784, 2785, 2786, 2787, 2788, 2789, 2790, 2791, 2792, 2793, 2794, 2795, 2796, 2797, 2798, 2799, 2800, 2801, 2802, 2803, 2804, 2805, 2806, 2807, 2808, 2809, 2810, 2811, 2812, 2813, 2814, 2815, 2816, 2817, 2818, 2819, 2820, 2821, 2822, 2823, 2824, 2825, 2826, 2827, 2828, 2829, 2830, 2831, 2832, 2833, 2834, 2835, 2836, 2837, 2838, 2839, 2840, 2841, 2842, 2843, 2844, 2845, 2846, 2847, 2848, 2849, 2850, 2851, 2852, 2853, 2854, 2855, 2856, 2857, 2858, 2859, 2860, 2861, 2862, 2863, 2864, 2865, 2866, 2867, 2868, 2869, 2870, 2871, 2872, 2873, 2874, 2875, 2876, 2877, 2878, 2879, 2880, 2881, 2882, 2883, 2884, 2885, 2886, 2887, 2888, 2889, 2890, 2891, 2892, 2893, 2894, 2895, 2896, 2897, 2898, 2899, 2900, 2901, 2902, 2903, 2904, 2905, 2906, 2907, 2908, 2909, 2910, 2911, 2912, 2913, 2914, 2915, 2916, 2917, 2918, 2919, 2920, 2921, 2922, 2923, 2924, 2925, 2926, 2927, 2928, 2929, 2930, 2931, 2932, 2933, 2934, 2935, 2936, 2937, 2938, 2939, 2940, 2941, 2942, 2943, 2944, 2945, 2946, 2947, 2948, 2949, 2950, 2951, 2952, 2953, 2954, 2955, 2956, 2957, 2958, 2959, 2960, 2961, 2962, 2963, 2964, 2965, 2966, 2967, 2968, 2969, 2970, 2971, 2972, 2973, 2974, 2975, 2976, 2977, 2978, 2979, 2980, 2981, 2982, 2983, 2984, 2985, 2986, 2987, 2988, 2989, 2990, 2991, 2992, 2993, 2994, 2995, 2996, 2997, 2998, 2999, 3000, 3001, 3002, 3003, 3004, 3005, 3006, 3007, 3008, 3009, 3010, 3011, 3012, 3013, 3014, 3015, 3016, 3017, 3018, 3019, 3020, 3021, 3022, 3023, 3024, 3025, 3026, 3027, 3028, 3029, 3030, 3031, 3032, 3033, 3034, 3035, 3036, 3037, 3038, 3039, 3040, 3041, 3042, 3043, 3044, 3045, 3046, 3047, 3048, 3049, 3050, 3051, 3052, 3053, 3054, 3055, 3056, 3057, 3058, 3059, 3060, 3061, 3062, 3063, 3064, 3065, 3066, 3067, 3068, 3069, 3070, 3071, 3072, 3073, 3074, 3075, 3076, 3077, 3078, 3079, 3080, 3081, 3082, 3083, 3084, 3085, 3086, 3087, 3088, 3089, 3090, 3091, 3092, 3093, 3094, 3095, 3096, 3097, 3098, 3099, 3100, 3101, 3102, 3103, 3104, 3105, 3106, 3107, 3108, 3109, 3110, 3111, 3112, 3113, 3114, 3115, 3116, 3117, 3118, 3119, 3120, 3121, 3122, 3123, 3124, 3125, 3126, 3127, 3128, 3129, 3130, 3131, 3132, 3133, 3134, 3135, 3136, 3137, 3138, 3139, 3140, 3141, 3142, 3143, 3144, 3145, 3146, 3147, 3148, 3149, 3150, 3151, 3152, 3153, 3154, 3155, 3156, 3157, 3158, 3159, 3160, 3161, 3162, 3163, 3164, 3165, 3166, 3167, 3168, 3169, 31

For example, they do not the function called depth is not very large in the above, they do not allocate local variable that are too large or too many local variables that that stack should be sufficient to implement all these to execute all these functions alright. So, the first function it calls this kinit1 one. And so, this is a physical page allocator alright. So, it is going to it going to initialize functions called kalloc and kfree that allow you to take physical pages from the available address space. We are going to study this later. But let us just assume that this function works correctly.

And after this function has executed completely, the kernel can make calls to kalloc and kfree right. kalloc is just like malloc for kernel. So, just you can allocate memory, and you can free memory except that kalloc only works at page (Refer Time: 14:10). So, malloc can take any size, but kalloc can only kalloc one kalloc call will allocate one page and give it to you ok. And then there is this function k v malloc which will initialize the kernel page table and that is what I am going to discuss today right.

So, we said that this is the page table after the entry page dir and what the kernel wants to do is that it wants to remove this paging this space and map this space completely into physical map address space right. So, right now only 0 to 4 MB region is mapped, you want to map entire 0 to M in this area right. And you want to remove that, so that they can be used for user pages right. Recall that was what the xv6 paging configuration was ok.

(Refer Slide Time: 15:00)



So, in this page kernel page dir, so let me call it kpgdir. I want to switch from this address space to this address space, and so what I am going to do I am going to map right now it is just 2 GB plus 4 MB, I am going to map the entire physical memory from here right. So, I am going to say 2 GB plus M and this is entirely going to go to 0 to M in physical memory right, so that is what I want and how I going to do it we are going to look at the code later.

But let us just see what we want right, we want to map the entire physical memory here, also recall that the first 1 MB was reserved for memory map devices right. The first 1 MB of physical memory address space is actually not memory it is you know console and the other things. So, even that gets mapped, but that is just reserved for the memory map devices. Also recall that I loaded the kernel at 1 MB. So, so this is let us say M map let us say M map d memory map devices. Then there is some area which will be loaded for the kernel.

Recall that we had loaded the kernel starting at 1 MB of the physical address space. So, starting at 1 MB, you are going to have the kernel both code and data right. And all the other space I am going to call it free space right, and that is the space I am going to manage using kalloc and kfree that is a space I will say this is space that you can use for your heap right or this is the this is the vacant space.

And this is the space that you can allocate for your data structures like the page directory right. So, where is the page directory can go to get allocated. Recall that the entry page directory was a global variable and so that was allocated in the data section of kernel. But all anything other than that, for example, per process page directories right, so all these things are going to be allocated from this extra space which is wherever the kernel ends and from there on till whatever capital M is the physical size of physical memory.

Also, this is the space allocate memory for data structures like process control box right. And most importantly this is the space from where you are going to allocate memory for the user processes themselves alright. So, what you are going to do is you are going to say kalloc going to get some page and you are going to create a mapping in this area for that. So, recall that is how it works basically allocate some pages here. Let us say a user says I want more page, or a user says I want to load a particular executable and that executable is larger than the current allocation of the process.

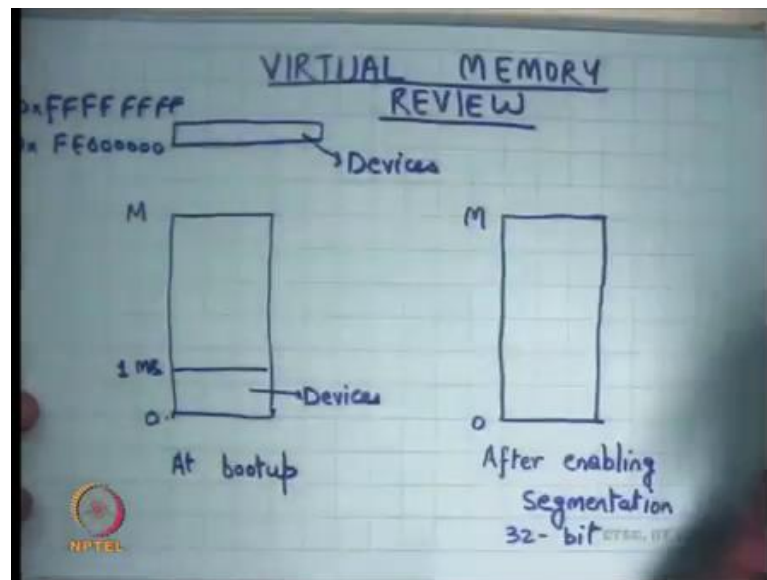
What is it going to do is, it is going to create mapping here it is going to allocate some space of here? Whatever space it allocates from here, it will have some backup in physical memory right some pointer into the physical memory. Some whatever pointer I get from allocation here I am going to convert it into its corresponding physical address, and then create a mapping from here to that physical address right, recall that the entire memory is been mapped here.

So, the entire memory has been mapped in my virtual address space, I allocate some area from that virtual address space, I get a page, I convert the address that I got to its physical address, and then I create a mapping in the user side of things to point to that right. So, these pages which are the mapped in the user side actually have two mappings in the page table: one on the kernel side and one on the user side right. So, if the two names for the same physical location, one name will be kern base plus something, and other name will be whatever the user want it to allocate it wherever it wanted to allocate it right, so.

So, I want to switch from this organization to this organization. Also point out that the top there is a slice of virtual address space on the top that starts at 0XFE and six zeros till 0XFF right. This slice of address space is actually used for memory map devices also. So, just like this area is used for memory map devices, this area is also used for memory map devices, and so this maps identically to the physical address space FE is same thing alright.

So, basically the physical address space in on a 32-bit X86 machine, the physical address 0XFE and six zeros is not actually pointing to memory, it is pointing to some memory map devices. And the kernel wants to retain that access. So, what it does is it just says the top virtual address space maps identically to its corresponding physical address space. So, if the kernel ever wants to access those devices, it can just access it using that address the same address right. So, basically, I am not going to use this top address space from FE000000 to FFFFFFFF for anything other than memory map devices right they map identically to physical address space right.

(Refer Slide Time: 20:59)



So, just to just to make this discussion more complete, at bootup the address space was not just this right. Actually at bootup the address space was 0 to 1 MB is devices, 1 MB to M is whatever your physical memory is, and also there is some chunk on the top FE e 2 3 4 5 6 to FF This area is can also be accessed. However, this will also point to devices right in the physical address space, so that was the original physical address space.

So, the amount of physical memory that you can have in your system is not really 2^{32} to the power 32 minus 1, it is 2^{32} minus 1 minus 1 MB minus whatever this is ok. And, so what the kernel wants to do is now retain this access and so it is going to map this identically to the corresponding physical address space right that is all. Anyways that is not really important, but when we are looking at code, it will help us in understanding what is going on ok.

(Refer Slide Time: 22:27)

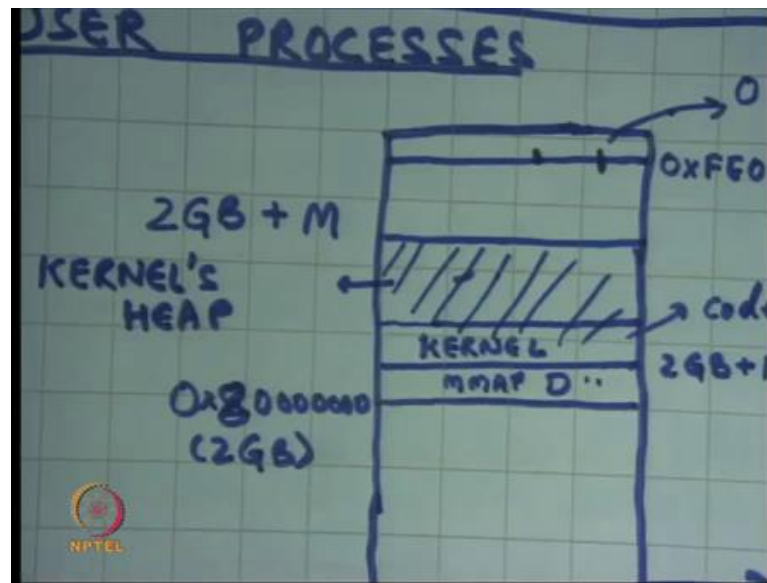
```
1753
1754 // Allocate one page table for the machine for the kernel address
1755 // space for scheduler processes.
1756 void
1757 kvmalloc(void)
1758 {
1759     kpgdir = setupkvm();
1760     switchkvm();
1761 }
1762
1763 // Switch h/w page table register to the kernel-only page table,
1764 // for when no process is running.
1765 void
1766 switchkvm(void)
1767 {
1768     lcr3(v2p(kpgdir)); // switch to the kernel page table
1769 }
1770
1771 // Switch TSS and h/w page table to correspond to process p.
1772 void
1773 switchvm(struct proc *p)
1774 {
1775     nptchcli();
1776     cpu->gdt[SEG_TSS] = SEG16(STS_T32A, &cpu->ts, sizeof(cpu->ts)-1);

```

So, let us look at what is kvmalloc doing on sheet 17. So, basically at the highest-level kvmalloc is going to initialize a new page table which is going to have this kind of mapping right, and it is going to switch to it. And it is going to forget about the old page table and that is it right. So, the kvmalloc function is just two lines. It calls the function called setupkvm; this is going to initialize a new page dir k page dir which will have this address spaces mapping.

And it is going to return a pointer k page dir to that particular page directory ok. So, it is going to initialize the page directory, where is it going to get the pages for to initialize for this page directory from its heap right from all this area that we discussed. This extra area: this is a kernels heap.

(Refer Slide Time: 23:24)



So, it is going to allocate a page directory from here, and it is going to initialize it, and it is going to return a pointer to the page directory ok. That that return pointer will be a virtual address in the kernel space right because everything in the kernel from now on is in the virtual address. When you allocate a page the return value that you get is also a virtual address. So, if you want to convert it to a physical address you need to subtract kernbase from it 2 GB from it right.

So, this function is going to allocate a page table and return a pointer to it this point is going to be a virtual address. And then I am going to call switch kvm. So, k page dir happens to be a global variable and. So, you just set up k page dir to this and switch kvm is just going to load cr3 with kpgdir except that it is going to call v 2 p on k page dir before it loads return cr3 perfect.

You allocated k page dir in your virtual address space initialized it, you got a virtual pointer you converted into physical pointer and loaded into cr3, recall that cr3 takes only physical pointers ok, so that is very simple. What we are going to look at next is setup kvm how exactly this page table is getting initialized alright. So, what is the structure of the page table.

(Refer Slide Time: 24:59)

```
1727 int perm;
1728 } kmap[] = {
1729 { (void*)KERNBASE, 0,          EXTHIM, PTE_W}, // I/O space
1730 { (void*)KERNLINK, V2P(KERNLINK), V2P(data), 0}, // kern text
1731 { (void*)data,      V2P(data),    PHYSTOP, PTE_W}, // kern data
1732 { (void*)DEVSPACE, DEVSPACE,      0,      PTE_W}, // more dev
1733 };
1734
1735 // Set up kernel part of a page table.
1736 pde_t*
1737 setupkvm(void)
1738 {
1739     pde_t *pgdir;
1740     struct kmap *k;
1741
1742     if((pgdir = (pde_t*)kalloc()) == 0)
1743         return 0;
1744     memset(pgdir, 0, PGSIZE);
1745     if (p2v(PHYSTOP) > (void*)DEVSPACE)
1746         panic("PHYSTOP too high");
1747     for(k = kmap; k < &kmap[NELEM(kmap)]; k++)
1748         if(mappages(pgdir, k->virt, k->phys_end - k->phys_start,
1749             (uint)k->phys_start, k->perm) < 0)
```

So, on the same page at line 1737, here is the code for setup kvm alright. And what it is doing is it first calls kalloc function to get a page from the kernel heap right. So, let us just assume that kalloc just allocates a page from the kernels heap and returns the pointer to it right, just like malloc, and puts it into page dir. Just in case the malloc failed or kalloc failed, then it just says oh I cannot proceed, it will return 0 and ultimately it will return 0 and tell the user that you know something has failed. Why could kalloc fail, give me some reasons?

Student: (Refer Time: 25:48).

You have run out of memory. So, let us say the physical memory was very small and so the head room that you have above the kernel space is very small. So, when you call the first kalloc, the first page itself got failed right.

Student: Sir.

Yes, question?

Student: Sir, how is the kalloc for (Refer Time: 26:03), right now we do not have a page directory or anything. So, from where will it allocate the page?

So, there was one function called k init that I skipped alright. So, I am going to discuss the later, but let us just assume that this address space has already been so this right now

we are working in this address space right 2 GB to 2 GB plus 4 MB. So, that is a great question. Assuming that there is some headroom above the kernel in this first 4 MB, I should be able to allocate a page right. So, it is not really limited by the size of physical memory at this point, it is actually limited by 4 MB this artificial limit that we used right, because you have only mapped the first 4 MB.

So, assuming that if the kernel size was so large if the kernel was you know let us say 3.9 MB, then my kalloc would have failed right irrespective of how much physical memory I have. So, if my kernel was indeed that large, I should have mapped more area here in my entry page dir, but my kernel is small right not that large let us say less than 1 MB. So, I have enough space.

So, when you to call kalloc, you can actually allocating space from here ok, because yeah you right at this point I am I am not switched I do not have a heap, my heap is actually very small. So, what you have done is he is just initialized whatever space is here to a heap and that is from that is where he is going to serve his request for kalloc alright ok.

So, so he is going to get a get a pointer in that kernbase to kernbase plus 4 MB space and that is going to be stored in page dir. The next thing it does is it zeros out the page dir. So, the pointer that he gets has a one-page size memory area that can be used right. So, page size is 4096 bytes, and recall that a page directory structure itself was one-page rights 4096 bytes. And so, what it does is just zeros out, so memset page dir zero-page size means zero out the entire page.

Student: (Refer Time: 28:08).

What does it mean to zero out the entire page directory, basically means no mapping exist right, because recall that for a mapping to exist the present bit in an entry should be set right? So, if you zero out the entire thing, none of the present bits are set, and so there are no mappings in this page directory initially ok. We can ignore this, this is just an error check, but then it is going to say for k is equal to k map k is less than this map pages right.

So, it is going to so k map is an array of mappings. It is going to look at this array, and it will call the map pages function to create mappings in the page table for that array.

What this array is k map is basically telling you what the regions are, that need to be mapped. For example, so it basically so static struct k map, it says this is the virtual address at which you need to map a region. This is the corresponding start physical address at which this region should be mapped. This is the end physical address. So, it also tells you the size of the region that needs to be mapped, and these are the permissions with which you should map it right.

So, for example, what we want to do is we want to say 0x you know this kernbase 2 GB value. So, 2 GB value to this 2 GB plus 1 MB should be mapped to 2 GB plus 1 MB with all privileges read-write execute. Then 2 GB plus 1 MB to whatever the kernel code is and read only data is that should be mapped to 1 MB to 1 MB plus whatever kernel codes kernel sizes in read mode. You do not want that the code should be writeable, just a just a precaution measure.

So, you just basically map it in read only mode. And then for everything else which is kernels data, and all the other memory that should be mapped in read-write mode in this area to the corresponding physical address right. And finally, this address 0XFE00 should be mapped identically to the same address in physical memory. So, those are the four sort of regions that you need to map right, four contiguous regions that you need to specify and that is what this array is telling you right.

(Refer Slide Time: 30:31)

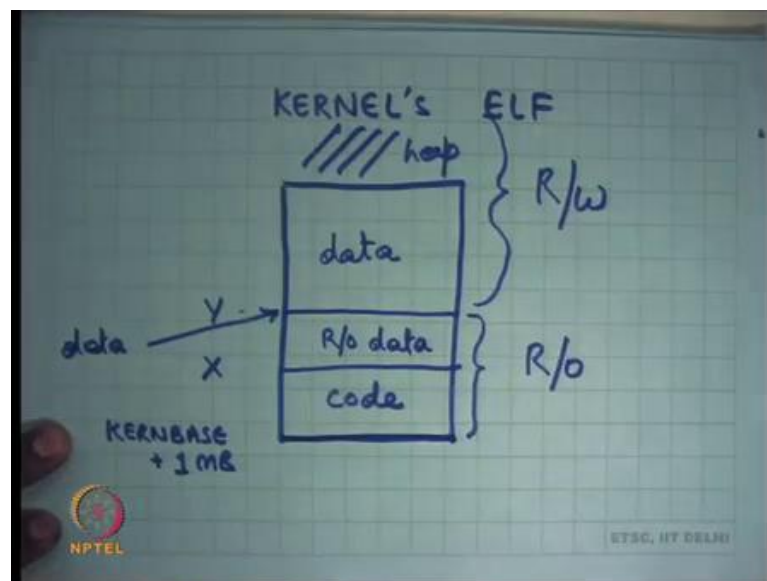
```
... // This table defines the kernel's mappings, which are present in
// every process's page table.
static struct kmap {
    void *virt;
    uint phys_start;
    uint phys_end;
    int perm;
} kmap[] = {
    { (void*)KERNBASE, 0,          EXTMEM,   PTE_W), // I/O space
    { (void*)KERNLINK, V2P(KERNLINK), V2P(data), 0), // kern text+rodata
    { (void*)data,     V2P(data),    PHYSTOP,  PTE_W), // kern data+mem
    { (void*)DEVSPACE, DEVSPACE,     0,       PTE_W), // more devices
};

// Set up kernel part of a page table.
pde_t*
setupkvm(void)
{
    pde_t *pgdir;
    struct kmap *k;
    if ((pgdir = (pde_t*)kalloc()) == 0)
        return 0;
}
```


So, the first mapping is saying start mapping at kernbase which is 2 GB. Physical address 0 to physical address 1 MB EXTMEM is 1 MB with write permissions alright. It is just initializing the IO space saying kernbase to kernbase + 1 MB map it to physical address 0 to 1 MB with write permissions, this is my IO this is my IO space memory map devices.

Then the next thing I have is starting at kernlink. So, kernlink is what, it is going to be the place at where you will start the kernel, it is 2 GB plus 1 MB ok, and V 2 P kernlink is 1 M b. So, recall that we have loaded the kern kernel starting at address 1 MB, the boot set at loaded the kernel starting at address 1 MB. So, we are going to load the kernel starting at 1 MB at address 2 GB plus 1 MB ok. The size the endpoint of this particular segment will be determined by where the data starts.

(Refer Slide Time: 31:49)



So, the kernel has been organized the kernels ELF has been organized in such a way that this is kern base plus 1 MB that is the start address. It will first have some code whatever the size of the code is and so somewhere the code will finish let us call that position X. Then there will be some area which will be called read only data ok. You can specify read only data. For example, in C, if you say const something then declared the global variable that gets allocated in the read only data right.

So, let us say you know data goes at Y, and then everything else is let us say data right. So, there are pointers in the kernel when you compile the kernel, there are symbols in the

kernel which tell you that here is the data, here is read only data and so on. So, this Y is pointing to so that is where the data point is pointing. So, what, what the loader is going to do is it is going to consider this as one segment and map it with read only permissions right. And it is going to map this and everything above it. So, above it is basically heap. After you load it above this is heap. So, everything above is going to be mapped with read-write privileges right ok. So, that is what that is what is happening here.

(Refer Slide Time: 33:25)

```

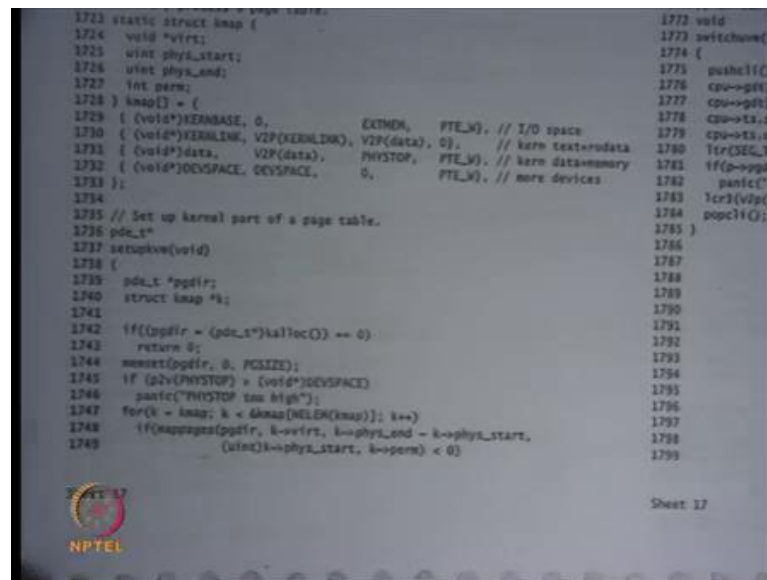
1713 // for the kernel's instructions and r/o data
1714 // data.KERNSPACE+PHYSTOP: mapped to V2P(data)..PHYSTOP,
1715 // r/w data = free physical memory
1716 // 0xf0000000..0: mapped direct (devices such as iocpts)
1717 // The kernel allocates physical memory for its heap and for user memory
1718 // between V2P(end) and the end of physical memory (PHYSTOP)
1719 // (directly addressable from end..P2V(PHYSTOP)).
1720
1721 // This table defines the kernel's mappings, which are present in
1722 // every process's page table.
1723 static struct kmap {
1724     void *virt;
1725     uint phys_start;
1726     uint phys_end;
1727     int perm;
1728 } kmap[] = {
1729     { (void*)KERNBASE, 0,          EXTHIGH, PTE_W, // I/O space
1730     { (void*)KERNLINK, V2P(KERNLINK), V2P(data), 0}, // kern text+rodata
1731     { (void*)data,      V2P(data),    PHYSTOP, PTE_W, // kern data+memory
1732     { (void*)DEVSPACE, DEVSPACE,     0,       PTE_W, // more devices
1733 };
1734
1735 // Set up kernel part of a page table.
1736 pde_t*
1737 setupkern(void)
1738 {
1739     pde_t *pgdir;
1740     struct kmap *k;
1741
1742     pgdir = (pde_t*)kalloc() -- 0;
1743     return 0;
1744     memset(pgdir, 0, PGSIZE);
1745     if (p2v(PHYSTOP) > (void*)DEVSPACE)
1746         panic("PHYSTOP too high");
1747     for (k = kmap; k < kmap+NMAP; k++)

```

Kernlink V2P kernlink which is 1 MB to V2P data right; so, wherever data starts till that point you map it with zero permissions 0 mean read only permissions in this case alright. If it is writeable, then you say PTE W, if 0 that means, read only. And then starting at data map it from at V2P data all the way till phystop, phystop is the size of the physical memory let us say alright or the maximum size of physical memory that you will support.

All that all the way up to phystop, you map it with writeable permissions, so that is kernel data plus all the other memory that will be used as a kernels heap right. And then you map devspace to devspace which is just FE00 identically right. So, that is what you are going to do, you are going to read this array which has these mappings contiguous mappings in a nice readable way.

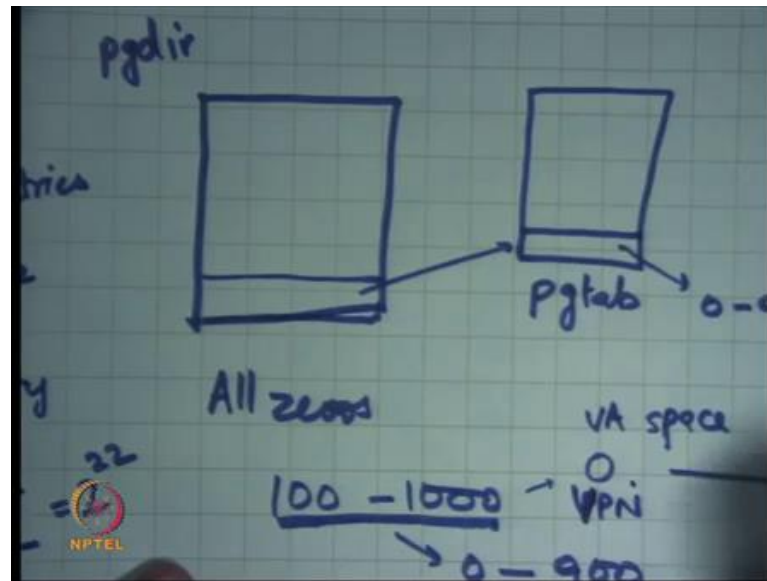
(Refer Slide Time: 34:27)



And for each of these mappings, you are going to call map pages right. So, what map pages is going to do is just going to create these mappings. Map pages takes an argument a virtual address, the corresponding size which is given by phys end minus phys start in the k map structure, the corresponding physical address at which it should be mapped and the permission with which it should be mapped alright.

So, it first takes the page directory in which it should create the mapping, it assumes that the page directory should already created, the virtual address, size, physical address permissions. And, if it succeeds and it will return a nonzero a positive value greater than equal to 0 value, otherwise return a negative value. What are some reasons for why it can fail? Recall that to map pages it may need to create allocate more pages right.

(Refer Slide Time: 35:31)



Right now, you are basically having a page dir. So, this is the page dir that is initially completely 0 doubt, all zeros. Now, let us say I want to say I want to map address 100 to 1000 to physical address 0 to 900. This type of the particular example right; so, I want to map virtual addresses 100 to thousand to physical addresses 0 to 900.

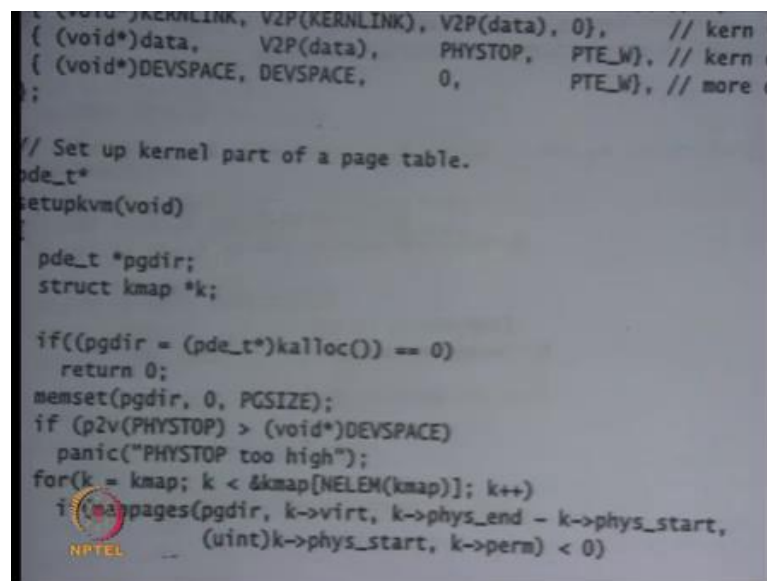
What do I need to do I will say address 100 is represented by entry number 0 right, each entry here represents a 4 MB region right because these are 2 to the power 10 entries mapping a space of 4 gigabytes right? So, each entry, 1 entry is mapping 2 to the power 32 divided by 2 to the power 10 which is 2 to the power 22 address space which is 4, 4 MB right.

And, recall that this 4 MB could be mapped using large pages or it could be mapped using another level of indirection using a page table right. So, in this case 100 is going to be this, the first entry within the first 4 MB. You are going to allocate another page table here; it is called as page table. And, in this you are going to say each entry going to allocate 4 kilo bytes.

So, here you going to create an entry saying map to 0 to 900 right. Clearly, I, I cannot just create this mapping, I need to say what is the corresponding page pages and so I can only do this at page (Refer Time: 37:22). So, instead of 0 to 100 to 1000, I will probably have to say map page 0 in VA space to map page 0 in PA space. So, this is just going to map to 0 in this case by the corresponding (Refer Time: 37:47).

So, to be able to do this, to be able to, so for this kind of mapping, I need to potentially allocate a new page to store this mapping right, and so this allocation could potentially fail. So, page directory is the top-level structure. Recall that a page table is a two-level structure. And so, whatever I want to map I may need to create allocate pages for the second level. And so, if that allocation fails, if I am running out of memory, I can probably I can probably fail so that is one reason for example, why map pages could fail ok.

(Refer Slide Time: 38:27)



```

// Set up kernel part of a page table.
pde_t*
setupkvm(void)
{
    pde_t *pgdir;
    struct kmap *k;

    if((pgdir = (pde_t*)kalloc()) == 0)
        return 0;
    memset(pgdir, 0, PGSIZE);
    if (p2v(PHYSTOP) > (void*)DEVSPACE)
        panic("PHYSTOP too high");
    for(k = kmap; k < &kmap[NELEM(kmap)]; k++)
        if (map_pages(pgdir, k->virt, k->phys_end - k->phys_start,
            (uint)k->phys_start, k->perm) < 0)

```

Yes. So, if I want to map let us say 0 to phystop in one go, I will divide it in two chunks and create entries in the page table, because recall that I cannot just the paging system does not allow me to map all at once. I have to you know divide it into either large pages or small pages, and then create appropriate entries in the page table to create that mapping ok.

Student: Already corrupt those pages.

So, the question is that let us say I want to map an entire region from data to phystop in the page table right. Question is how much space do I need to map this? The amount of space that I need to map this is basically whatever these spaces divided by

Student: 4 KB.

4 KB. If you are using small pages right, so that is not that much. So, let us say this space was, so the overhead is basically you know less than 1 percent, or less than 0.1 percent actually right. So, whatever this space was let say this space was x bytes, then the amount of space that your required to make that those x bytes is x divided by 4000 roughly right, so that is less than you know 0.1 percent of x .

Student: But when I map those in the page directory means that I have already also have a backup in my physical memory for those mapping.

Could you repeat?

Student: Like if I map it from my data to physical stop.

Ok.

Student: My in my page directory and it means that in my physical memory also I have allocated space for that particular memory only.

You have mapped that memory; you have mapped that memory. You are not, so there is a difference between mapping and allocation. You have just mapped that memory which means this name is going to refer to this location. You have not allocated that memory right. Allocation means you are going to you have basically committed to using it. You have just mapped it you are going to use it later on, ok. The memory that you have allocated is the kernels code, and kernels read only code and kernels data a kernel's read only data and kernels data.

All that has been already there are some contents into it which are useful which should not be overwritten. So, all that memories mapped, but that is a small piece. Everything above that you have mapped not necessarily used, you are going to use it later. And you are going to use it using `kalloc` and `kfree` functions, you are going to manage that using `kalloc` and `kfree` functions.

Student: Sir, so we do not need to store that mapping means that mapping will require some space.

Which mapping?

Student: What should do physical?

We do not need to store that. So, can you say your question fully?

Student: I am saying that we need some space to store that mapping that this space number in virtual will point to this page number in physical

Sure.

Student: So, how do we do that?

So, how do we say that this page number in virtual space maps to this page number in physical space. We say that using a page table entry right. So, one entry in the page table basically says that this page maps to this page right. And so, an entry of 4 bytes gives you information about mapping for a region of 4 KB. So, it is you know point one percent overhead or space in that sense alright.

So, what map pages is going to do is, it is going to fill in the structure called page dir such that this area in virtual address space gets mapped to this area in physical address space ok. And it is going to do it using small pages alright. So, recall that I had said that you know one common optimization used in mainstream kernels is that you use large pages to map the entire kernel right that save space, but xv 6 does not do that I mean it is not so xv6 just to make thing simple uses small pages to even map the kernel address space. So, all these regions are going to be mapped using small pages right.

(Refer Slide Time: 42:53)

```
// (directly addressable from end..P2V(PHYSTOP)).  
  
// This table defines the kernel's mappings, which are present  
// every process's page table.  
static struct kmap {  
    void *virt;  
    uint phys_start;  
    uint phys_end;  
    int perm;  
} kmap[] = {  
    { (void*)KERNBASE, 0,          EXTMEM,  PTE_W}, // I/O s  
    { (void*)KERNLINK, V2P(KERNLINK), V2P(data), 0}, // kern  
    { (void*)data,     V2P(data),    PHYSTOP, PTE_W}, // kern  
    { (void*)DEVSPACE, DEVSPACE,    0,       PTE_W}, // more  
};  
  
// Set up kernel part of a page table.  
pde_t*  
setu (void)  
{  
    pde_t *pgdir;
```

0xE0000000
224MB

In this case for example, if I wanted to be smart about it, I could have probably said look this area is 1 MB, so I am going to use small pages to map this area because you know 4 MB pages are too big to map. This area, this area from kernlink to V2P data, this is also very small I said it is less than 1 MB. So, even this is it does not make sense to use large pages. I am going to use small pages for this, but this area from V2P data to phystop and assuming my phystop is very large right like you know 100 MB or 200 MB.

Then this area is for potentially mapable using large pages right, but we are going to forget about it, we can say we are going to map all these areas using small pages right. And finally, this area is also small, so large pages may or may not help yeah, I mean perhaps large pages will help here too, but in any case, we are going to use small pages to map all this.

Student: Sir, phystop maps the end of (Refer Time: 43:46).

Phystop is just a constant defined in the kernel which basically says what is the maximum amount size of physical memory, that xv6 supports alright. So, phystop is just setup to hexadecimal E 3, 4, 5, 6. I think E and six 0s which is 224 MB right. So, it just irrespective of the size of the physical memory it maps data to phystop identically ok.

So, if the physical memory was larger than phystop those that area is not accessible right, above phystop area in the physical memory will not be accessible. If the physical memory was less than phystop let us say the physical memory was only 100 MB, then you have just unnecessarily mapped extra area, but that is I mean if the user ever accesses that area is going to get some error right, some exception ok.

Let us stop here.